StoreFront 2.6

Mar 17, 2016

About StoreFront

Known issues

System requirements

Infrastructure requirements
User device requirements

Plan

User access options
User authentication
Optimize the user experience
StoreFront high availability and multi-site configuration

Install and set up

Install StoreFront
Configure StoreFront
Uninstall StoreFront

Upgrade

Secure

Troubleshoot

Manage

Configure server groups
Create and configure the authentication service
Create a store
Create an unauthenticated store
Configure stores
Create a Receiver for Web site
Configure Receiver for Web sites
Add a NetScaler Gateway connection
Configure NetScaler Gateway connection settings
Configure beacon points
Configure smart card authentication
Set up highly available multi-site store configurations
Configure StoreFront using the configuration files
Configure Receiver for Web sites using the configuration files
Disable workspace control reconnect for all Receivers
Configure Desktop Appliance sites
Configure authentication for XenApp Services URLs
Create a single FQDN to access a store internally and externally
Configure NetScaler and StoreFront for Delegated Forms Authentication (DFA)
Configure Resource Filtering
Configure special folder redirection
Manage subscription data

Citrix SCOM Management Pack for StoreFront
About StoreFront

Oct 03, 2014

StoreFront manages the delivery of desktops and applications from XenApp, XenDesktop, XenMobile, or VDI-in-a-Box servers in the datacenter to users' devices. StoreFront enumerates and aggregates available desktops and applications into stores. Users access StoreFront stores through Citrix Receiver directly or by browsing to a Receiver for Web or Desktop Appliance site. Users can also access StoreFront using thin clients and other end-user-compatible devices through XenApp Services site.

StoreFront keeps a record of each user's applications and automatically updates their devices, ensuring users have a consistent experience as they roam between their smartphones, tablets, laptops, and desktop computers. StoreFront is an integral component of XenApp 7.x and XenDesktop 7.x but can be used with several versions of XenApp and XenDesktop.

What's new

StoreFront 2.6 includes the following new features and enhancements.

**Simplified store configuration in the administration console.** The updated StoreFront console simplifies the StoreFront configuration for the following features:

- User subscriptions (mandatory store)
- Set session timeout for Receiver for Web
- Show domains list in logon page

  Learn More ▶ See "Manage user subscriptions."

  Learn More ▶ See the "Set session timeout" section.

  Learn More ▶ See the "Configure trusted user domains" section.

**Special folder redirection.** You can specify that special folders are redirected to the users' local devices.

  Learn More ▶ See "Configure special folder redirection."

**Unauthenticated (anonymous) users.** Unauthenticated users with XenApp 7.6 and XenDesktop 7.6 can access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. When unauthenticated users are enabled in XenApp or XenDesktop, you must have an unauthenticated StoreFront store to allow access for them.

  Learn More ▶ See "Create an unauthenticated store."
Receiver for Web My Apps Folder View. This new view displays the applications in a folder hierarchy and includes a breadcrumb path for unauthenticated and mandatory stores. This folder view can help your users move from Web Interface to Receiver for Web.

Learn More  See " Disable the My Apps Folder View."

Single Fully Qualified Domain Name (FQDN) access. This feature allows you to provide access to resources internally and externally using a single FQDN.

Learn More  See " Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally."

Kerberos-constrained delegation for XenApp 6.5. StoreFront with Kerberos-constrained delegation enables pass-through authentication, eliminating the need for the client and device to run Windows with Receiver.

Learn More  See " Configure Kerberos constrained delegation for XenApp 6.5."

XenApp Services Support smart card authentication. The StoreFront server authenticates using smart cards to XenApp Services Support sites and does not require specific versions of Receiver and operating systems.

Learn More  See the " Use smart cards with XenApp Services Support" section.

Receiver for Android, iOS, and Linux smart card authentication. New versions of Receiver support local and remote use of smart cards for accessing apps and desktops.

Learn More  See the " Use smart cards with XenApp Services Support" section.

Extensible authentication. Support for extensible authentication provides a single customization point for extension of StoreFront’s form-based authentication. Worx Home and Receiver for Web use it to authenticate with XenMobile and XenApp and XenDesktop for both internal (direct) and external (using NetScaler Gateway) access scenarios.

Learn More  See the "Configure NetScaler and StoreFront for Delegated Forms Authentication (DFA)" section.

XenApp 7.6 and XenDesktop 7.6 connection leasing. When connection leasing is enabled, the XenApp 7.6 and XenDesktop 7.6 Controllers cache information about recent user connections. If the database becomes unavailable, the Controller uses that cached information to continue supporting connections for applications and desktops that the user launched within the past two weeks.

Learn More  See "Connection leasing."
StoreFront Web API. Allows you to build custom web applications or portal integrations to access XenApp or XenDesktop apps and desktops.

See "StoreFront Web API"

Receiver for Web access from a mobile browser. Enables touch for tablet users to verify credentials, remove apps, and restart desktops.

Updated Zero-install Receiver for HTML5 engine. Adds productivity applications including audio-video playback in XenApp and XenDesktop, clipboard across remote applications and between local and remote applications, seamless keyboard support inside Microsoft applications and desktops, and direct SSL connection.
Known issues

Oct 06, 2014
The following issues are known to exist in this release.

Activate Citrix ICA Client link might not work in non-English versions of Firefox

Some non-English versions of Firefox install the Addons Manager by default. You might not receive a response when clicking Activate the Citrix Client on the Activate the Citrix plug-in screen. There are three workarounds (the first being the preferred method) [#494376]:

- Click the block-like icon ⫸ in the address bar and choose an option for Allow <server> to run Citrix ICA Client.
- Remove or disable the Addons Manager.
  1. Click the menu button ⫸ and choose Add-ons.
  2. The Addons Manager tab opens.
  3. In the Addons Manager tab, select Extensions and click Remove or Disable on the Addons Manager page.

Third-party ad blockers might prevent users of older versions of Chrome from seeing StoreFront logon dialog boxes

This prevents a store from being accessible to users. As a workaround, users can either disable ad-blocking software or add an exception for the desired service domain to the ad-blocking software's configuration. [#319305]

Receiver for Web sites may be slow to respond on Internet Explorer 8

Users running Internet Explorer 8 may find that Receiver for Web sites containing a large number of desktops and applications are slow to respond when browsing the store or entering search terms. [#274126]

StoreFront deployed on Windows Server 2012 R2 affected by Certified Trust List (CTL) changes

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.

Windows 2012 Server does not by default send a list of trusted CAs during the SSL handshake, resulting in the Linux client failing to provide a client certificate. The changes to Windows 2012 Server are documented at What's New in TLS/SSL (Schannel SSP).

Windows Receiver clients will work if a CTL list is not sent to the client. For the Linux Receiver client, it is necessary to enable the CTL list as described in the above link.

The following registry edit is required:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL

Value name: SendTrustedIssuerList
Value type: REG_DWORD
Value data: 1 (True)
[# 460064]

Fixed issues

For issues fixed in this release, see http://support.citrix.com/article/CTX138215.
System requirements

Dec 01, 2014

When planning your installation, Citrix recommends that you allow at least an additional 2 GB of RAM for StoreFront over and above the requirements of any other products installed on the 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.

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

- Windows Server 2012 R2 Datacenter and Standard editions
- Windows Server 2012 Datacenter and Standard editions
- Windows Server 2008 R2 Service Pack 1 Enterprise 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. While a server group can contain a maximum of five servers, from a capacity perspective based on simulations, there is no advantage of server groups containing more than three servers. All servers in a server group must reside in the same location.

Microsoft Internet Information Services (IIS) and Microsoft .NET Framework are required on the server. If either of these prerequisites is installed but not enabled, the StoreFront installer enables them before installing the product. Windows PowerShell and Microsoft Management Console, which are both default components of Windows Server, must be installed on the web server before you can install StoreFront. The relative path to StoreFront in IIS must be the same on all the servers in a group.

StoreFront uses the following ports for communications. 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 be accessible from inside the corporate network.
- 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 Receiver for HTML5, 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.
Infrastructure requirements

Jan 26, 2015
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.

- XenDesktop
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
  - XenDesktop 5.6 Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
- XenApp
  - XenApp 7.6
  - XenApp 7.5
  - XenApp 6.5 Feature Pack 2
  - XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2
  - XenApp 6.5 for Windows Server 2008 R2
  - XenApp 6.0 for Windows Server 2008 R2
  - XenApp 5.0 Feature Pack 3 for Windows Server 2008 x64 Edition
  - XenApp 5.0 Feature Pack 3 for Windows Server 2008
  - XenApp 5.0 Feature Pack 3 for Windows Server 2003 x64 Edition
  - XenApp 5.0 Feature Pack 3 for Windows Server 2003
  - XenApp 5.0 Feature Pack 2 for Windows Server 2008 x64 Edition
  - XenApp 5.0 Feature Pack 2 for Windows Server 2008
  - XenApp 5.0 Feature Pack 2 for Windows Server 2003 x64 Edition
  - XenApp 5.0 Feature Pack 2 for Windows Server 2003
  - XenApp 5.0 Feature Pack 1 for Windows Server 2003 x64 Edition
  - XenApp 5.0 Feature Pack 1 for Windows Server 2003
  - XenApp 5.0 for Windows Server 2008 x64 Edition
  - XenApp 5.0 for Windows Server 2008
  - XenApp 5.0 for Windows Server 2003 x64 Edition
  - XenApp 5.0 for Windows Server 2003
- VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2

For more information about requirements and limitations, see Use StoreFront with VDI-in-a-Box.

NetScaler Gateway requirements

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

- NetScaler Gateway 10.5
Receiver for HTML5 requirements

If you plan to enable users to access desktops and applications using Receiver for HTML5 running on Receiver for Web sites, the following additional requirements apply.

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

- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 7.6
- XenApp 7.5
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2 (requires Hotfix XA650R01W2K8R2X64051, which is available at http://support.citrix.com/article/CTX135757)

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

- NetScaler Gateway 10.1
- Access Gateway 10 Build 71.6014 (the version number is displayed at the top of the configuration utility)

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

- XenDesktop
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
  - XenDesktop 5.6
  - XenDesktop 5.5
- XenApp
  - XenApp 7.6
  - XenApp 7.5
  - XenApp 6.5 Feature Pack 2
  - XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2
  - XenApp 6.5 for Windows Server 2008 R2
  - XenApp 6.0 for Windows Server 2008 R2
  - XenApp 5.0 Feature Pack 3 for Windows Server 2008 x64 Edition
  - XenApp 5.0 Feature Pack 3 for Windows Server 2008
  - XenApp 5.0 Feature Pack 3 for Windows Server 2003 x64 Edition
  - XenApp 5.0 Feature Pack 3 for Windows Server 2003
- XenApp 5.0 Feature Pack 2 for Windows Server 2008 x64 Edition
- XenApp 5.0 Feature Pack 2 for Windows Server 2008
- XenApp 5.0 Feature Pack 2 for Windows Server 2003 x64 Edition
- XenApp 5.0 Feature Pack 2 for Windows Server 2003
- XenApp 5.0 Feature Pack 1 for Windows Server 2003 x64 Edition
- XenApp 5.0 Feature Pack 1 for Windows Server 2003
- XenApp 5.0 for Windows Server 2008 x64 Edition
- XenApp 5.0 for Windows Server 2008
- XenApp 5.0 for Windows Server 2003 x64 Edition
- XenApp 5.0 for Windows Server 2003
- VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
User device requirements

Feb 24, 2015

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

Users with non-domain-joined desktop appliances access their desktops through their web browsers, which are configured to access Desktop Appliance sites. In the case of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with older Citrix clients that cannot be upgraded, users must connect through the XenApp Services URL for the store.

If you plan to deliver offline applications to users, the Offline Plug-in is required in addition to Receiver for Windows. If you want to deliver Microsoft Application Virtualization (App-V) sequences to users, a supported version of the Microsoft Application Virtualization Desktop Client is also required. For more information, see Publishing Applications for Streaming and Publishing App-V Sequences in XenApp. Users cannot access offline applications or App-V sequences through Receiver for Web sites.

It is assumed that all user devices meet the minimum hardware requirements for the installed operating system.

Requirements for access to stores within Citrix Receiver

The following Citrix Receiver versions can be used to access StoreFront stores from both internal network connections and through NetScaler Gateway. Connections through NetScaler Gateway can be made using both the NetScaler Gateway Plug-in and/or clientless access.

- Citrix Receiver for Windows 8/RT
- Citrix Receiver for Windows 4.3
- Citrix Receiver for Windows 4.2
- Citrix Receiver for Windows 4.1
- Citrix Receiver for Windows 4.0
- Citrix Receiver for Windows 3.4
- Citrix Receiver for Mac
- Citrix Receiver for iOS
- Citrix Receiver for Android 3.6
- Citrix Receiver for Android 3.7
- Citrix Receiver for Linux

For lifecycle information for Citrix Receiver, see Lifecycle Milestones for Citrix Receiver.

Requirements for access to stores through Receiver for Web sites

The following Citrix Receiver, operating system, and web browser combinations are recommended for users to access Receiver for Web sites from both internal network connections and through NetScaler Gateway. Connections through NetScaler Gateway can be made using both the NetScaler Gateway Plug-in and clientless access.

- Citrix Receiver for Windows 4.1, 4.2 & 4.3
- Windows 8.1 (32-bit and 64-bit editions)
- Internet Explorer 11 (32-bit mode)
- Google Chrome 33
- Mozilla Firefox 32
- Mozilla Firefox 31
- Windows 8 (32-bit and 64-bit editions)
  - Internet Explorer 10 (32-bit mode)
  - Google Chrome 33
  - Google Chrome 32
  - Mozilla Firefox 32
  - Mozilla Firefox 31
- Windows 7 Service Pack 1 (32-bit and 64-bit editions)
  - Internet Explorer 10 (32-bit mode)
  - Internet Explorer 9 (32-bit mode)
  - Internet Explorer 8 (32-bit mode)
  - Google Chrome 33
  - Google Chrome 32
  - Mozilla Firefox 32
  - Mozilla Firefox 31
- Windows Embedded Standard 7 Service Pack 1 or Windows Thin PC
  - Internet Explorer 10 (32-bit mode)
  - Internet Explorer 9 (32-bit mode)
  - Internet Explorer 8 (32-bit mode)
- Windows Vista Service Pack 2 (32-bit and 64-bit editions), Windows Embedded XP
  - Internet Explorer 9 (32-bit mode)
  - Internet Explorer 8 (32-bit mode)
  - Google Chrome 33
  - Google Chrome 32
  - Mozilla Firefox 32
  - Mozilla Firefox 31
- Windows Embedded Standard 2009
  - Internet Explorer 8 (32-bit mode)
- Citrix Receiver for Windows 4.0 or Citrix Receiver for Windows 3.4
  - Windows 8 (32-bit and 64-bit editions)
    - Internet Explorer 10 (32-bit mode)
    - Google Chrome 33
    - Google Chrome 32
    - Mozilla Firefox 27
    - Mozilla Firefox 26
- Windows 7 Service Pack 1 (32-bit and 64-bit editions)
  - Internet Explorer 10 (32-bit mode)
  - Internet Explorer 9 (32-bit mode)
  - Internet Explorer 8 (32-bit mode)
  - Google Chrome 33
  - Google Chrome 32
  - Mozilla Firefox 27
  - Mozilla Firefox 26
- Windows Embedded Standard 7 Service Pack 1 or Windows Thin PC
  - Internet Explorer 10 (32-bit mode)
  - Internet Explorer 9 (32-bit mode)
  - Internet Explorer 8 (32-bit mode)
- Windows Vista Service Pack 2 (32-bit and 64-bit editions), Windows Embedded XP
  - Internet Explorer 9 (32-bit mode)
  - Internet Explorer 8 (32-bit mode)
  - Google Chrome 33
  - Google Chrome 32
  - Mozilla Firefox 27
  - Mozilla Firefox 26
- Windows Embedded Standard 2009
  - Internet Explorer 8 (32-bit mode)
- Citrix Receiver for Mac 11.8 or Citrix Receiver for Mac 11.7
  - Mac OS X 10.9 Mavericks
    - Safari 7
    - Google Chrome 33
    - Mozilla Firefox 27
  - Mac OS X 10.8 Mountain Lion
    - Safari 6
    - Google Chrome 33
    - Mozilla Firefox 27
  - Mac OS X 10.7 Lion
    - Safari 5.1
    - Google Chrome 33
    - Mozilla Firefox 27
  - Mac OS X 10.6 Snow Leopard
    - Safari 5.0
    - Google Chrome 33
    - Mozilla Firefox 27
- Citrix Receiver for Linux 12.1 or Citrix Receiver for Linux 13
  - Google Chrome 33
  - Mozilla Firefox 27
- Citrix Receiver for Android 3.6 - Note: Requires users to manually open ICA file.
  - Android 4.x and 5.0
    - Chrome for Android
    - The default browser on the device.
- Citrix Receiver for iOS 5.9 - Note: Requires users to manually open ICA file.
  - iOS 6.1.x, 7 and 8
  - Safari

Requirements for access to desktops and applications through Receiver for HTML5

The following operating systems and web browsers are recommended for users to access desktops and applications using Receiver for HTML5 running on Receiver for Web sites. Both internal network connections and connections through NetScaler Gateway are supported. However, for connections from the internal network, Receiver for HTML5 only enables access to resources provided by specific products. Additionally, specific versions of NetScaler Gateway are required to
enable connections from outside the corporate network. For more information, see Infrastructure requirements.

- **Browsers**
  - Internet Explorer 11 (HTTP connections only)
  - Internet Explorer 10 (HTTP connections only)
  - Safari 7
  - Google Chrome 33
  - Mozilla Firefox 27
- **Operating systems**
  - Windows RT
  - Windows 8.1 (32-bit and 64-bit editions)
  - Windows 8 (32-bit and 64-bit editions)
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions)
  - Windows Vista Service Pack 2 (32-bit and 64-bit editions)
  - Windows Embedded XP
  - Mac OS X 10.9 Mavericks
  - Mac OS X 10.8 Mountain Lion
  - Mac OS X 10.7 Lion
  - Mac OS X 10.6 Snow Leopard
  - Google Chrome OS 33
  - Ubuntu 12.04 (32-bit)

**Requirements for access to stores through Desktop Appliance sites**

The following Citrix Receiver, operating system, and web browser combinations are recommended for users to access Desktop Appliance sites from the internal network. Connections through NetScaler Gateway are not supported.

- **Citrix Receiver for Windows 4.1**
  - Windows 8.1 (32-bit and 64-bit editions)
    - Internet Explorer 11 (32-bit mode)
  - Windows 8 (32-bit and 64-bit editions)
    - Internet Explorer 10 (32-bit mode)
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions), Windows Embedded Standard 7 Service Pack 1, or Windows Thin PC
    - Internet Explorer 9 (32-bit mode)
    - Internet Explorer 8 (32-bit mode)
  - Windows Embedded XP
    - Internet Explorer 8 (32-bit mode)
- **Citrix Receiver for Windows 4.0 or Citrix Receiver for Windows 3.4**
  - Windows 8 (32-bit and 64-bit editions)
    - Internet Explorer 10 (32-bit mode)
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions), Windows Embedded Standard 7 Service Pack 1, or Windows Thin PC
    - Internet Explorer 9 (32-bit mode)
    - Internet Explorer 8 (32-bit mode)
  - Windows Embedded XP
    - Internet Explorer 8 (32-bit mode)
  - Citrix Receiver for Windows Enterprise 3.4
Requirements for access to stores through XenApp Services URLs

All the versions of Citrix Receiver listed above can be used to access StoreFront stores with reduced functionality through XenApp Services URLs. In addition, you can use the older client that does not support other access methods — Citrix Receiver for Linux 12.0 (internal network connections only) — to access stores through XenApp Services URLs. Connections through NetScaler Gateway, where supported, can be made using both the NetScaler Gateway Plug-in and clientless access.

Smart card requirements

**Requirement for using Receiver for Windows 4.X with smart cards**

Citrix tests for compatibility with the U.S. Government Common Access Card (CAC), U.S. National Institute of Standards and Technology Personal Identity Verification (NIST PIV) cards, and 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.

The following smart card and middleware combinations have been tested by Citrix as representative examples of their type. However, other smart cards and middleware can also be used. For more information about Citrix-compatible smart cards and middleware, see [http://www.citrix.com/ready](http://www.citrix.com/ready).

<table>
<thead>
<tr>
<th>Middleware implementation</th>
<th>Smart card</th>
</tr>
</thead>
<tbody>
<tr>
<td>HID Global ActivClient 7.0 in both GSC-IS and NIST PIV modes</td>
<td>CAC</td>
</tr>
<tr>
<td>HID Global ActivClient 6.2 CAC edition in GSC-IS mode</td>
<td>CAC</td>
</tr>
<tr>
<td>Gemalto Minidriver 8.3 for .NET Smart Card</td>
<td>Gemalto IDPrime .NET 510</td>
</tr>
<tr>
<td>SafeNet Authentication Client 8.0 for Windows</td>
<td>SafeNet eToken 5100</td>
</tr>
</tbody>
</table>
**Middleware implementation**
GSC-IS – (U.S.) Government Smart Card Interoperability Specifications

<table>
<thead>
<tr>
<th>Smart card</th>
<th></th>
</tr>
</thead>
</table>

**Requirements for using Desktop Appliance sites with smart cards**

For users with desktop appliances and repurposed PCs running the Citrix Desktop Lock, Citrix Receiver for Windows Enterprise 3.4 is required for smart card authentication. On all other Windows devices, Citrix Receiver for Windows 4.1 can be used.

**Requirements for using Receiver for Android with smart cards**

Smartcard authentication to NetScaler Gateway with StoreFront 2.x and XenDesktop 5.6 and above or XenApp 6.5 and above.

Supported smart card readers:
- BaiMobile 3000MP Bluetooth Smart Card Reader

Supported smart cards:
- PIV cards
- Common Access Card

**Requirements for using Receiver for iOS with smart cards**

Smartcard authentication to NetScaler Gateway with StoreFront 2.x and XenDesktop 5.6 and above or XenApp 6.5 and above.

Supported smart card readers:
- Precise Biometrics Tactivo for iPad Mini
- Precise Biometrics Tactivo for iPad (4th generation) and Tactivo for iPad (3rd generation) and iPad 2
- Thursby TSS-PK7 and PK8 Smart Card Readers
- BaiMobile 3000MP Bluetooth Smart Card Reader

Supported smart cards:
- PIV cards
- Common Access Card

**Requirements for using Receiver for Linux 13.1 with smart cards and XenApp Services Support**

The following smart cards and readers are supported:

Smart cards:
- Smart cards with PKCS#11 drivers for the appropriate Linux platform

Smart card readers:
- Readers that are CCID compliant
Requirements for authentication through NetScaler Gateway

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

- NetScaler Gateway 10.1
- Access Gateway 10 Build 69.4 (the version number is displayed at the top of the configuration utility)
Plan

Apr 17, 2015

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 XenDesktop, XenApp, and VDI-in-a-Box 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 XenDesktop, XenApp, and VDI-in-a-Box. Users access stores through Citrix Receiver, Receiver for Web sites, Desktop Appliance 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 synchronized 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.
Load balancing

For multiple server deployments, external load balancing through, for example, NetScaler 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 NetScaler, see Load Balancing. For more information about Windows Network Load Balancing, see http://technet.microsoft.com/en-us/library/hh831698.aspx.

Active load balancing of requests sent from StoreFront to XenDesktop sites and XenApp 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 NetScaler.

Citrix recommends that in a load balanced environment, you modify the hosts file to ensure that Receiver for Web always talks to the local StoreFront server instead of the load balancer. You can also achieve this by setting up the DNS server appropriately.

Active Directory considerations

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

**Scalability**

The number of Citrix Receiver 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 the minimum recommended specification of two virtual CPUs running on an underlying dual Intel Xeon L5520 2.27Ghz 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 server is 3GB. When using Receiver for Web, assign an additional 3KB per resource, per user in addition to the base memory allocation.

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

**Important:** All servers in a server group must reside in the same location. StoreFront server groups containing mixtures of operating system versions and locales are not supported.

**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.

Receiver for Web also has a timeout setting, which controls how long a 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 Configure store time-out duration and retry attempts and Configure communication time-out duration and retry attempts.
Four different methods are available for users to access StoreFront stores.

- **Citrix Receiver**—Users with compatible versions of Citrix Receiver can access StoreFront stores within the Citrix Receiver user interface. Accessing stores within Citrix Receiver provides the best user experience and the greatest functionality.

- **Receiver for Web sites**—Users with compatible web browsers can access StoreFront stores by browsing to Receiver for Web sites. By default, users also require a compatible version of Citrix Receiver to access their desktops and applications. However, you can configure your Receiver for Web sites to enable users with HTML5-compatible browsers to access their resources without installing Citrix Receiver. When you create a new store, a Receiver for Web site is created for the store by default.

- **Desktop Appliance sites**—Users with non-domain-joined desktop appliances can access their desktops through the web browsers on their appliances, which are configured to access Desktop Appliance sites in full-screen mode. When you create a new store for a XenDesktop deployment using Citrix Studio, a Desktop Appliance 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.

Accessing stores from within the Citrix Receiver user interface provides the best user experience and the greatest functionality. For the Citrix Receiver versions that can be used to access stores in this way, see System requirements for StoreFront 2.6.

Citrix Receiver uses internal and external URLs as beacon points. By attempting to contact these beacon points, Citrix Receiver 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 Receiver. This enables Citrix Receiver 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 Receiver 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 Receiver 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 Receiver for Windows using command-line parameters.

Provisioning files

You can provide users with provisioning files containing connection details for their stores. After installing Citrix Receiver, users open the .cr file to automatically configure accounts for the stores. By default, 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 Setup URL Generator to create a URL containing connection details for a store. After installing Citrix Receiver, 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. For more information, see To create and configure a setup URL.

Manual configuration

More advanced users can create new accounts by entering store URLs into Citrix Receiver. Remote users accessing StoreFront through NetScaler Gateway 10.1 and Access Gateway 10 enter the appliance URL. Citrix Receiver obtains the required account configuration information when the connection is first established. For connections through Access Gateway 9.3, users cannot set up accounts manually and must use one of the alternative methods above. For more information, see the Citrix Receiver documentation.

Email-based account discovery

Users who install Citrix Receiver on a device for the first time can set up accounts by entering their email addresses, provided that they download Citrix Receiver from the Citrix website or a Citrix Receiver download page hosted within your internal network. You configure Service Location (SRV) locator resource records for NetScaler 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 Receiver initial configuration process. Citrix Receiver 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 Receiver.

Configure email-based account discovery

Configure email-based account discovery to enable users who install Citrix Receiver on a device for the first time to set up their accounts by entering their email addresses. Provided that they download Citrix Receiver from the Citrix website or a Citrix Receiver 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 Receiver. Email-based account discovery is not available if Citrix Receiver is downloaded from any other location, such as a Receiver for Web site, and cannot be used with Citrix Receiver Updater.

During the initial configuration process, Citrix Receiver prompts users to enter either an email address or a store URL. When a user enters an email address, Citrix Receiver 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 Receiver to locate available stores on the basis of users’ email addresses, you configure Service Location (SRV) locator resource records for NetScaler 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 Receiver searches for a machine named “discoverReceiver” to identify a StoreFront server.

You must install a valid server certificate on the NetScaler 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 Receiver 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 NetScaler Gateway with the StoreFront connection details. For more information, see Connecting to StoreFront by Using Email-Based Discovery.

Add a 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.
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 NetScaler 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 NetScaler Gateway FQDN. With this configuration, local users are provided with the StoreFront details, while remote users receive NetScaler Gateway connection information.
7. If you configured a SRV record for your NetScaler Gateway appliance, add the StoreFront connection details to NetScaler Gateway in a session profile or global setting.

Receiver for Web sites

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

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 Receiver is installed on the user’s device. If Citrix Receiver cannot be detected, the user is prompted to download and install the appropriate Citrix Receiver 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 Receiver 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 Receiver for Windows and Receiver for Mac, see Configure Receiver for Web sites.

Receiver for HTML5

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

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

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

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

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

Resource shortcuts

You can generate URLs that provide access to desktops and applications available through 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 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 Receiver for Web sites.
As with all desktops and applications accessed from Receiver for Web sites, users must either have installed Citrix Receiver or be able to use Receiver for HTML5 to access resources through shortcuts. The method used by a Receiver for Web site depends on the site configuration, on whether Citrix Receiver 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 Receiver for Web sites through shortcuts.

When you create an application shortcut, ensure that no other applications available from the 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 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 NetScaler 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 NetScaler Gateway to restrict user access to only those specific sites. For more information, see http://support.citrix.com/article/CTX123610.

Customize your sites

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 Receiver for Web site benefit from many of the features available with store access within Citrix Receiver, such as application synchronization. When you decide whether to use 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 Receiver for Web site.
- Subscribed applications are not available on the Windows Start screen when accessing a store through a Receiver for Web site.
- File type association between local documents and hosted applications accessed through Receiver for Web sites is not available.
- Offline applications cannot be accessed through Receiver for Web sites.
- Receiver for Web sites do not support Citrix Online products integrated into stores.
- Receiver 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 NetScaler Gateway.
- To use Receiver 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.

Desktop Appliance sites

Users with non-domain-joined desktop appliances can access their desktops through Desktop Appliance sites. Non-domain-joined in this context means devices that are not joined to a domain within the Microsoft Active Directory forest containing the StoreFront servers.
When you create a new store for a XenDesktop deployment using Citrix Studio, a Desktop Appliance site is created for the store by default. Desktop Appliance sites are only created by default when StoreFront is installed and configured as part of a XenDesktop installation. You can create Desktop Appliance sites manually using Windows PowerShell commands. For more information, see Configure Desktop Appliance sites.

Desktop Appliance sites provide a user experience that is similar to logging on to a local desktop. The web browsers on desktop appliances are configured to start in full-screen mode displaying the logon screen for a Desktop Appliance site. When a user logs on to a site, by default, the first desktop (in alphabetical order) available to the user in the store for which the site is configured starts automatically. If you provide users with access to multiple desktops in a store, you can configure the Desktop Appliance site to display the available desktops so users can choose which one to access. For more information, see Configure Desktop Appliance sites.

When a user's desktop starts, it is displayed in full-screen mode, obscuring the web browser. The user is automatically logged out from the Desktop Appliance site. When the user logs off from the desktop, the web browser, displaying the Desktop Appliance site logon screen, is visible again. A message is displayed when a desktop is started, providing a link for the user to click to restart the desktop if it cannot be accessed. To enable this functionality, you must configure the Delivery Group to enable users to restart their desktops. For more information, see Manage application and desktop delivery.

To provide access to desktops, a compatible version of Citrix Receiver is required on the desktop appliance. Typically, XenDesktop-compatible appliance vendors integrate Citrix Receiver into their products. For Windows appliances, the Citrix Desktop Lock must also be installed and configured with the URL for your Desktop Appliance site. If Internet Explorer is used, the Desktop Appliance site must be added to the Local intranet or Trusted sites zones. For more information about the Citrix Desktop Lock, see Prevent user access to the local desktop.

Important considerations

Desktop Appliance sites are intended for local users on the internal network accessing desktops from non-domain-joined desktop appliances. When you decide whether to use Desktop Appliance sites to provide users with access to your stores, consider the following restrictions.

- If you plan to deploy domain-joined desktop appliances and repurposed PCs, do not configure them to access stores through Desktop Appliance sites. Instead, configure Citrix Receiver with the XenApp Services URL for the store. For more information, see XenApp Services URLs.
- Desktop Appliance sites do not support connections from remote users outside the corporate network. Users logging on to NetScaler Gateway cannot access Desktop Appliance sites.

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 Receiver to XenApp Services URLs. Citrix Ready partner products use the Citrix Fast Connect API to streamline user logons through Receiver 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 XenDesktop and XenApp. For more information, see Receiver for Windows 4.0.
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. 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 Receiver and for scenarios where alternative access methods are not available. When you decide whether to use XenApp Services URLs to provide users with access to your stores, consider the following restrictions.

- You cannot modify the XenApp Services URL for a store.
- You cannot modify XenApp Services URL settings by editing the configuration file, config.xml.
- XenApp Services URLs support explicit, domain pass-through, smart card authentication, and pass-through with smart card authentication. Explicit authentication is enabled by default. Only one authentication method can be configured for each XenApp Services URL and only one URL is available per store. If you need to enable multiple authentication methods, you must create separate stores, each with a XenApp Services URL, for each authentication method. Your users must then connect to the appropriate store for their method of authentication. For more information about configuring user authentication to XenApp Services URLs, see Configure authentication for XenApp Services URLs.
- 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 XenDesktop, XenApp, and VDI-in-a-Box servers providing desktops and applications for the store, bypassing the StoreFront authentication service.
User authentication

Jan 27, 2015

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 when you create your first store. All user access methods support explicit authentication.

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

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 and create your first store, domain pass-through authentication is disabled by default. Domain pass-through authentication can be enabled for users connecting to stores through Citrix Receiver and XenApp Services URLs. Receiver for Web sites support domain pass-through authentication for Internet Explorer only. Enable domain pass-through authentication in the Receiver for Web UI node in the administration console and requires you to configure SSON on Receiver for Windows. Receiver for HT ML5 does not support domain pass-through authentication. To use domain pass-through authentication, users require Receiver for Windows or the Online Plug-in for Windows. Pass-through authentication must be enabled when Receiver for Windows or the Online Plug-in for Windows are installed on users' devices.

Pass-through from NetScaler Gateway

Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores. Pass-through from NetScaler Gateway authentication is enabled by default when you first configure remote access to a store. Users can connect through NetScaler Gateway to stores using Citrix Receiver or Receiver for Web sites. Desktop Appliance sites do not support connections through NetScaler Gateway. For more information about configuring StoreFront for NetScaler Gateway, see Add a NetScaler Gateway connection. For more information about setting up NetScaler Gateway to connect to StoreFront, see Integrating NetScaler Gateway with XenMobile App Edition.

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

- **Security token.** Users log on to NetScaler 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 NetScaler Gateway are required to enter both their domain credentials and security token passcodes.
- **Client certificate.** Users log on to NetScaler Gateway and are authenticated based on the attributes of the client certificate presented to NetScaler Gateway. Configure client certificate authentication to enable users to log on to...
NetScaler Gateway using smart cards. Client certificate authentication can also be used with other authentication types to provide double-source authentication.

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

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

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

If you configure double-source authentication to NetScaler Gateway for remote users accessing stores from within Citrix Receiver, you must create two authentication policies on NetScaler 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 NetScaler 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 NetScaler Gateway to StoreFront, set SSO Name Attribute to userPrincipalName in the NetScaler Gateway LDAP authentication policy for each domain. You can require users to specify a domain on the NetScaler Gateway logon page so that the appropriate LDAP policy to use can be determined. When you configure the NetScaler 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 NetScaler Gateway deployment, you can use SmartAccess to control user access to XenDesktop and XenApp resources on the basis of NetScaler Gateway session policies. For more information about SmartAccess, see Configuring SmartAccess on NetScaler Gateway.

Smart cards

Users authenticate using smart cards and PINs when they access their stores. When you install StoreFront and create your first store, smart card authentication is disabled by default. Smart card authentication can be enabled for users connecting to stores through Citrix Receiver, Receiver for Web, Desktop Appliance sites, 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 XenDesktop.
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 one-way trust or trust relationships of different types, are not 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 Receiver for Windows

Users with devices running Receiver for Windows can authenticate using smart cards, either directly or through NetScaler 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 Receiver for Windows.

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 Receiver for Windows for pass-through authentication and enable domain pass-through authentication to StoreFront.

In the case of non-domain-joined devices on the local network, the minimum number of logon prompts that users can
receive is two. Users log on to their devices and then authenticate to Receiver for Windows using their smart cards and PINs. With the appropriate configuration in place, users are only 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 of non-domain-joined devices log on to Receiver 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 NetScaler 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 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 NetScaler Gateway authentication to StoreFront and delegate credential validation to NetScaler Gateway. Then, create an additional NetScaler Gateway virtual server through which you route user connections to resources. In the case of domain-joined devices, you must also configure Receiver for Windows for pass-through authentication.

Users can log on to NetScaler 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 NetScaler Gateway logons. Configure pass-through authentication from NetScaler Gateway to StoreFront and delegate credential validation to NetScaler Gateway for smart card users so that users are silently authenticated to StoreFront.

**Use smart cards with Desktop Appliance sites**

Non-domain-joined Windows desktop appliances can be configured to enable users to log on to their desktops using smart cards. The Citrix Desktop Lock is required on the appliance and Internet Explorer must be used to access the Desktop Appliance site.

The figure shows smart card authentication from a non-domain-joined desktop appliance.

When users access their desktop appliances, Internet Explorer starts in full-screen mode displaying the logon screen for a Desktop Appliance site. Users authenticate to the site using their smart cards and PINs. If the Desktop Appliance site is configured for pass-through authentication, users are automatically authenticated when they access their desktops and applications. Users are not prompted for their PINs again. Without pass-through authentication, users must enter their PINs a second time when they start a desktop or application.

You can enable users to fall back to explicit authentication if they experience any issues with their smart cards. To do this, you configure the Desktop Appliance site for both smart card and explicit authentication. In this configuration, smart card
authentication is considered to be primary access method so users are prompted for their PINs first. However, the site also provides a link that enables users to log on with explicit credentials instead.

**Use smart cards with XenApp Services URLs**

Users of domain-joined desktop appliances and repurposed 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 authenticated when they access their desktops and applications, and are not prompted for their PINs again.

**Use smart cards with Receiver for Web**

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

1. Select the 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 XenDesktop and XenApp for Receiver for Windows users with domain-joined devices who do not access stores through NetScaler 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 XenDesktop and XenApp for Receiver for Windows users with domain-joined devices accessing stores through NetScaler 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 Receiver for iOS and Android**
Users with devices running Receiver for iOS and Receiver for Android can authenticate using smart cards, either directly or through NetScaler 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 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 Receivers 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 NetScaler 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 NetScaler Gateway authentication to StoreFront and delegate credential validation to NetScaler Gateway. Then, create an additional NetScaler Gateway virtual server through which you route user connections to resources.

Users can log on to NetScaler 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 NetScaler Gateway to StoreFront and delegate credential validation to NetScaler 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 Receiver for Linux

Users with devices running Receiver 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, Receiver 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 Receiver for Windows. Refer to How To Configure StoreFront 2.x and Smart Card Authentication for Internal Users using Stores and for instructions on using smart cards, see Receiver for Linux in eDocs.

The minimum number of logon prompts that users can receive is one. Users log on to their devices and then authenticate to Receiver 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 Receiver 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 NetScaler 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, 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 NetScaler Gateway authentication to StoreFront and delegate credential validation to NetScaler Gateway. Then, create an additional NetScaler Gateway virtual server through which you route user connections to resources.

Users can log on to NetScaler 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 NetScaler Gateway logons. Configure pass-through authentication from NetScaler Gateway to StoreFront and delegate credential validation to NetScaler Gateway for smart card users so that users are silently authenticated to StoreFront.

Smart cards for Receiver for Linux are not supported with the XenApp Services Support sites. Once smart card support is enabled for both the server and Receiver, you can use smart cards for the following purposes:

- Smart card logon authentication. Use smart cards to authenticate users to Citrix XenApp and XenDesktop 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 launch applications and desktops can authenticate using smart cards without depending on specific hardware, operating systems, and Receivers. 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 and later and XenDesktop 7.0 and later. For earlier versions, see http://support.citrix.com/proddocs/topic/xenapp6-w2k8-admin/ps-sf-citrix-xml-service-port-set-v2.html and http://support.citrix.com/proddocs/topic/access-gateway-50/ag-50-integrate-wi-client-xd5-xml-trust-tsk.html.

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**

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

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 NetScaler 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 NetScaler 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. 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 XenDesktop and XenApp for Receiver for Windows users with domain-joined devices who do not access stores through NetScaler 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 XenDesktop and XenApp for Receiver for Windows users with domain-joined devices accessing stores through NetScaler Gateway, this setting applies to all users of the store. To enable pass-through authentication for some users and require others to log on to their desktops and applications, you must create separate stores for each group of users. Then, direct your users to the appropriate store for their method of authentication.
- Only one authentication method can be configured for each XenApp Services URL and only one URL is available per store. If you need to enable other types of authentication in addition to smart card authentication, you must create separate stores, each with a XenApp Services URL, for each authentication method. Then, direct your users to the appropriate store for their method of authentication.
- When StoreFront is installed, the default configuration in Microsoft Internet Information Services (IIS) only requires that client certificates are presented for HTTPS connections to the certificate authentication URL of the StoreFront authentication service. IIS does not request client certificates for any other StoreFront URLs. This configuration enables you to provide smart card users with the option to fall back to explicit authentication if they experience any issues with their smart cards. Subject to the appropriate Windows policy settings, users can also remove their smart cards without needing to reauthenticate.

If you decide to configure IIS to require client certificates for HTTPS connections to all StoreFront URLs, the authentication service and stores must be collocated 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 NetScaler 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

Jan 27, 2015

StoreFront includes features designed to enhance the user experience. These features are configured by default when you create new stores and their associated Receiver for Web sites, Desktop Appliance 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 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 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 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 Receiver for Web sites, see Configure workspace control.

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

- Workspace control is not available when Receiver for Web sites are accessed from hosted desktops and applications.
- For users accessing Receiver for Web sites from Windows devices, workspace control is only enabled if the site can detect that Citrix Receiver is installed on users' devices or if Receiver for HTML5 is used to access resources.
- To reconnect to disconnected applications, users accessing 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 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 Receiver cannot be disconnected or shut down by 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 XenDesktop or XenApp. File type association is enabled by default for new stores. For more information, see Disable file type association.

User change password

You can enable 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.

If you enable 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. By default, the notification period for a user is determined by the applicable Windows policy setting. Password expiry warnings are only displayed to users connecting from the internal network. For more information about enabling users to change their passwords, see Configure the authentication service.

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

Receiver for Web site desktop and application views

When both desktops and applications are available from a 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 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 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 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 XenDesktop 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, Receiver for Web sites differentiate the desktops for users by appending numerical suffixes to the desktop names.

For users connecting to stores within Citrix Receiver 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 XenDesktop and XenApp, 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.

- Organize applications into folders to make it easier for users to find what they need when browsing through the available resources. The folders you create in XenDesktop and XenApp appear as categories in Citrix Receiver. You could, for example, group applications according to type or, alternatively, create folders 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 Receiver.
- You can specify that all users have a core set of applications that cannot be removed from the Receiver home screen by appending the string KEYWORDS:Mandatory to the application 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.
- Advertise XenDesktop applications to users or make commonly used applications easier to find by listing them in the Featured list in Citrix Receiver. 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, XenDesktop and XenApp hosted shared desktops are treated like other desktops by 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 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 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 Receiver 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 Receiver subscribes the user to the delivered application, but does not create a shortcut. When the user starts the delivered application from Citrix Receiver, the locally installed instance runs instead. For more information, see Configure application delivery.
StoreFront high availability and multi-site configuration

Oct 10, 2013

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. StoreFront high availability and multi-site configurations are set up by editing the store configuration files. Highly available multi-site configurations cannot be set up or managed using the Citrix StoreFront management console. 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 XenDesktop, XenApp, and VDI-in-a-Box 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 XenDesktop, XenApp, and VDI-in-a-Box 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 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 XenDesktop and XenApp 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 or when the user already has an active session on a non-preferred deployment.

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 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.

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 collocated 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 NetScaler Gateway routing

If you have configured separate NetScaler 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 NetScaler 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 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 NetScaler 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 NetScaler Gateway routing can also be used in the special case where local users on the internal network are required to log on to NetScaler Gateway for endpoint analysis. With this configuration, users connect to the store through the NetScaler 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 NetScaler Gateway. Note that you must also configure a specific internal virtual server IP address for the NetScaler Gateway appliance. Additionally, specify an inaccessible internal beacon point so that Citrix Receiver is always prompted to connect to NetScaler Gateway, regardless of the user's network location.

NetScaler Gateway global server load balancing

StoreFront supports NetScaler 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 NetScaler Gateway virtual server.

Important considerations

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

- Deskspots 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 Receiver 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.
- Primary deployments in the same equivalent deployment set must be identical. StoreFront only enumerates and displays to users the resources from the first available primary deployment in a set, since it is assumed that each deployment provides exactly the same resources. Configure separate equivalent deployment sets for deployments that differ even slightly in the resources they provide.
- 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 and set up

Sep 12, 2014
To install and configure StoreFront, complete the following steps in order.

1. If you plan to use StoreFront to deliver XenDesktop, XenApp, or VDI-in-a-Box 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.

   Note: StoreFront cannot be installed on a domain controller.

2. If not already present, StoreFront requires Microsoft .NET 4.5 Framework, which can be downloaded from Microsoft. You must have Microsoft .NET 4.5 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 NetScaler for load balancing, you define a virtual server to proxy your StoreFront servers. For more information on configuring NetScaler for load balancing, see Load Balancing Traffic on a NetScaler.

   1. Ensure that load balancing is enabled on your NetScaler appliance.
   2. For each StoreFront server, create individual HTTP or SSL load balancing services, as appropriate, using the StoreFront monitor type.

      For more information, see Monitoring Citrix StoreFront Stores.

   3. 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. For more information, see Inserting the IP Address of the Client in the Request Header.

   4. Create a virtual server and bind the services to the virtual server.
   5. On the virtual server, configure persistence on the basis of source IP address.

      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. For more information, see Persistence Based on Source IP Address.

4. Optionally, enable the following features.

   - .NET Framework 4.5 Features > .NET Framework 4.5, ASP.NET 4.5
   - 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
     - On Windows Server 2012 servers:

        Web Server (IIS) > Web Server > Application Development > .NET Extensibility 4.5, Application Initialization, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters
On Windows Server 2008 R2 servers:

Web Server (IIS) > Web Server > Application Development > .NET Extensibility, Application Initialization, ASP.NET, ISAPI Extensions, ISAPI Filters

- Web Server (IIS) > Management Tools > IIS Management Console, IIS Management Scripts and Tools

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

5. **Install StoreFront.**

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 Receiver requires HTTPS connections to stores. You can change from HTTP to HTTPS at any time after installing StoreFront, provided the appropriate IIS configuration is in place.


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

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

8. Use the Citrix StoreFront management console to configure your server.
Install StoreFront

Feb 12, 2015

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

2. Ensure that the required Microsoft .NET 4.5 Framework is installed on the server. (In some environments, version 4.5.1 or 4.5.2 may be required.)

3. Browse your installation media or download package, locate CitrixStoreFront-x64.exe, and run the file as an administrator.
   Note: On Windows Server 2008 R2 servers, a message may be displayed indicating that the .NET feature will be enabled. If this message appears, click Yes.

4. Read and accept the license agreement, and click Next.

5. If the Review prerequisites page appears, click Next.

6. On the Ready to install page, check the prerequisites and StoreFront components that are listed for installation and click Install.

   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
   • Web Server (IIS) > Web Server > Security > Request Filtering, Windows Authentication
   • On Windows Server 2012 & 2012 R2 servers:
     Web Server (IIS) > Web Server > Application Development > .NET Extensibility 4.5, Application Initialization, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters
     On Windows Server 2008 R2 servers:
     Web Server (IIS) > Web Server > Application Development > .NET Extensibility 3.5.1, Application Initialization, ASP.NET 3.5.1, ISAPI Extensions, ISAPI Filters
   • On Windows Server 2012 and Windows Server 2012 R2, the following features are also enabled if they are not already configured.
     • .NET Framework 4.5 Features > .NET Framework 4.5, ASP.NET 4.5

7. When the installation is complete, click Finish.

   The Citrix StoreFront management console starts automatically so that you can configure your server.

To install StoreFront at a command prompt

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

2. Ensure that all of the requirements for installation of StoreFront are met before installing StoreFront. Refer to the installation overview 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]]
Use the `-silent` argument to perform a silent installation of StoreFront and all the prerequisites. By default, StoreFront is installed at `C:\Program Files\Citrix\Receiver StoreFront\`. However, you can specify a different installation location using the `-INSTALLDIR` argument, where `installationlocation` is the directory in which to install StoreFront.

By default, if a Receiver for Web site cannot detect Citrix Receiver on a Windows or Mac OS X device, the user is prompted to download and install the appropriate Citrix Receiver for their platform from the Citrix website. You can modify this behavior so that users download the Citrix Receiver installation files from the StoreFront server instead. For more information, see Make Citrix Receiver installation files available on the server.

If you plan to make this configuration change, specify the `-WINDOWS_CLIENT` and `-MAC_CLIENT` arguments to copy Receiver for Windows and Receiver 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 Citrix Receiver installation file. Receiver for Windows and Receiver for Mac installation files are included on your StoreFront installation media or download package.
Configure StoreFront

Oct 10, 2013
When the Citrix StoreFront management console first starts, two options are available.

- **Create a new 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 new server, you will need access to an existing server in the deployment.
Create a new deployment

Nov 03, 2014

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

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

3. 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. For more information, see Configure server groups.

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 Receiver 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.

5. On the Store Name page, specify a name for your store and click Next.
   StoreFront stores aggregate desktops and applications, making them available to users. Store names appear in Citrix Receiver 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 procedure below. You can configure stores to provide resources from any mixture of XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments. Repeat the procedures, as necessary, to add all the deployments providing resources for the store.
   - Add XenDesktop, XenApp, and VDI-in-a-Box resources to the store
   - Add App Controller applications to 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 store through NetScaler Gateway.
   - To make the store unavailable to users on public networks, select None. Only local users on the internal network will be able to access the store.
   - To make only resources delivered through the store available through NetScaler Gateway, select No VPN tunnel. Users log on directly to NetScaler Gateway and do not need to use the NetScaler Gateway Plug-in.
   - 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 Full VPN tunnel. Users require the NetScaler Gateway Plug-in to establish the VPN tunnel.

   If you configure remote access to the store through NetScaler Gateway, the pass-through from NetScaler Gateway authentication method is automatically enabled. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

9. If you enabled remote access, list the NetScaler Gateway deployments through which users can access the store. To add a NetScaler Gateway deployment, follow the appropriate procedure below. Repeat the procedures, as necessary, to
add further deployments.

- Provide remote access to the store through a NetScaler Gateway appliance
- Provide remote access to the store through an Access Gateway 5.0 cluster

10. When you have added all your NetScaler Gateway deployments, select from the NetScaler Gateway appliances list the deployments through which users can access the store. If you enable access through multiple deployments, specify the default deployment to be used to access the store.

11. On the Remote Access page, click Create. Once the store has been created, click Finish.

After creating the store, further options become available in the Citrix StoreFront management console. For more information, see Manage your StoreFront deployment.

Your store is now available for users to access with Citrix Receiver, 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 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.

You can quickly add more servers to your deployment by selecting the option to join an existing server group when installing further instances of StoreFront.

Add XenDesktop, XenApp, and VDI-in-a-Box resources to the store

Complete the following steps to make desktops and applications provided by XenDesktop, XenApp, and VDI-in-a-Box 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 of the Create Store wizard, click Add.
2. 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 XenDesktop, XenApp, or VDI-in-a-Box.
3. 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 XenDesktop sites, give details of Delivery Controllers. In the case of XenApp farms, list servers running the Citrix XML Service. To add VDI-in-a-Box grids, specify either the grid-wide virtual IP address, if configured, or list the IP addresses of your servers.
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 Secure Sockets Layer (SSL) or Transport Layer Security (TLS), select HTTPS. If you select this option for XenDesktop and XenApp 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 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 XenDesktop and XenApp servers, the specified port must be the port used by the Citrix XML Service.

6. If you are using the SSL Relay to secure connections between StoreFront and XenApp 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.

You can configure stores to provide resources from any mixture of XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments. To add further XenDesktop sites, XenApp farms, or VDI-in-a-Box grids, repeat the procedure above. To make applications managed by App Controller available in the store, follow the steps in Add App Controller applications to the store. 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.

Add App Controller applications to the store

Complete the following steps to make applications managed by App Controller 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 of the Create Store wizard, click Add.

2. In the Add Delivery Controller dialog box, specify a name that will help you to identify the App Controller virtual appliance managing the applications that you want to make available in the store. Ensure that the name does not contain any spaces. Select AppController.

3. Enter the name or IP address of the App Controller virtual appliance in the Server box and specify the port for StoreFront to use for connections to App Controller. The default port is 443.

You can configure stores to provide resources from any mixture of XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments. To add applications managed by other App Controller virtual appliances, repeat the procedure above. To make desktops and applications provided by XenDesktop, XenApp, and VDI-in-a-Box available in the store, follow the steps in Add XenDesktop, XenApp, and VDI-in-a-Box resources to the store. 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 NetScaler Gateway appliance

Complete the following steps to configure remote access through a NetScaler 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.


2. In the Add NetScaler Gateway Appliance dialog box, specify a name for the appliance 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 appliance. For example, you can include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.

3. Enter the URL of the virtual server or user logon point (for Access Gateway 5.0) for your appliance. Specify the product version used in your deployment.
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. If you are adding an Access Gateway 5.0 appliance, select from the Deployment mode list Appliance. Otherwise, specify the subnet IP address of the NetScaler 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 NetScaler 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 NetScaler Gateway appliance. Where specified, StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

5. If you are adding an appliance running NetScaler Gateway 10.1, Access Gateway 10, or Access Gateway 9.3, select from the Logon type list the authentication method you configured on the appliance for Citrix Receiver users. The information you provide about the configuration of your NetScaler Gateway appliance is added to the provisioning file for the store. This enables Citrix Receiver 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.

6. Complete the NetScaler Gateway authentication service URL in the Callback URL box. StoreFront automatically appends the standard portion of the URL. Click Next.

   Enter the internally accessible URL of the appliance. StoreFront contacts the NetScaler Gateway authentication service to verify that requests received from NetScaler Gateway originate from that appliance.

7. If you are making resources provided by XenDesktop, XenApp, or VDI-in-a-Box 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. If you configured a grid-wide virtual IP address for your VDI-in-a-Box deployment, you need only specify this address to enable fault tolerance.

   Important: VDI-in-a-Box STA URLs must be entered in the form https://serveraddress/dt/sta in the Add Secure Ticket Authority URL dialog box, where serveraddress is the FQDN or IP address of the VDI-in-a-Box server, or the grid-wide virtual IP address.

   The STA is hosted on XenDesktop, XenApp, and VDI-in-a-Box servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop, XenApp, and VDI-in-a-Box resources.

8. If you want XenDesktop, XenApp, and VDI-in-a-Box to keep disconnected sessions open while Citrix Receiver 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.
9. Click Create to add your NetScaler Gateway deployment to the list on the Remote Access page.

To add further deployments, repeat the procedure above. To configure remote access to the store through an Access Gateway 5.0 cluster, follow the steps in Provide remote access to the store through an Access Gateway 5.0 cluster. When you have added all your NetScaler Gateway deployments, return to Step 10 in the “Create a new deployment” procedure at the top of this article.

Provide remote access to the store through an Access Gateway 5.0 cluster

Complete the following steps to configure remote access through an Access Gateway 5.0 cluster 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.

2. In the Add NetScaler Gateway Appliance dialog box, specify a name for the cluster 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 cluster. For example, you can include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.
3. Enter the URL of the user logon point for your cluster and select from the Version list 5.x.
4. From the Deployment mode list, select Access Controller and click Next.
5. On the Appliances page, list the IP addresses or fully qualified domain names (FQDNs) of the appliances in the cluster and click Next.
6. 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.
7. If you are making resources provided by XenDesktop, XenApp, or VDI-in-a-Box 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. If you configured a grid-wide virtual IP address for your VDI-in-a-Box deployment, you need only specify this address to enable fault tolerance. Important: VDI-in-a-Box STA URLs must be entered in the form https://serveraddress/dt/sta in the Add Secure Ticket Authority URL dialog box, where serveraddress is the FQDN or IP address of the VDI-in-a-Box server, or the grid-wide virtual IP address. The STA is hosted on XenDesktop, XenApp, and VDI-in-a-Box servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop, XenApp, and VDI-in-a-Box resources.
8. If you want XenDesktop, XenApp, and VDI-in-a-Box to keep disconnected sessions open while Citrix Receiver 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.
9. Click Create to add your NetScaler Gateway deployment to the list on the Remote Access page.

To add further clusters, repeat the procedure above. To configure remote access to the store through NetScaler Gateway
10.1, Access Gateway 10, Access Gateway 9.3, or a single Access Gateway 5.0 appliance, follow the steps in **Provide remote access to the store through a NetScaler Gateway appliance**. When you have added all your NetScaler Gateway deployments, return to Step 10 in the “Create a new deployment” procedure at the top of this article.
Join an existing server group

Dec 01, 2014

Before installing StoreFront, ensure that the server you are adding to the group 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. While a server group can contain a maximum of five servers, from a capacity perspective based on simulations, there is no advantage of server groups containing more than three servers. In addition, ensure that the relative path to StoreFront in IIS on the server you are adding is the same as on the other servers in the group.

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 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.

Remove a server from an existing server group

If a StoreFront server was a member of a server group and has been removed, you must run the Clear-DSConfiguration PowerShell cmdlet to reset the StoreFront server to a factory default state. After you run the Clear-DSConfiguration cmdlet on the disconnected server, you can add the server back to an existing server group or to a different newly created server group.

1. Open the StoreFront administration console on the primary StoreFront server that you use to manage your entire server group.
2. Select the server group node on the left pane and choose another server to remove.
3. Remove the selected server from the server group.
4. In the Actions pane, propagate changes from the server you used to disconnect one of your server group members. Any other remaining server group members are now aware that a server has been removed from the group. Until you reset the disconnected server to a factory default state, it is not aware that it is no longer a member of the group.
5. Close the administration console on the disconnected server.
6. Open a PowerShell session on your disconnected server after it has been removed from the group and import the StoreFront PowerShell modules using: & "$Env:PROGRAMFILES\Citrix\Receiver..."
7. Run the `Clear-DSConfiguration` command, which resets the server to default settings.
8. Open the StoreFront administration console and the disconnected server is reset and ready to be added to another server group.
Uninstall StoreFront

Aug 04, 2014

In addition to the product itself, uninstalling StoreFront removes the authentication service, stores, Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs, and their associated configurations. The subscription store service containing users' application subscription data is also deleted. In single-server deployments, this means that details of users' application subscriptions are 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. On the Windows Start screen or Apps screen, locate the Citrix StoreFront tile. Right-click the tile and click Uninstall.
3. In the Programs and Features dialog box, select Citrix StoreFront and click Uninstall to remove all StoreFront components from the server.
4. In the Uninstall Citrix StoreFront dialog box, click Yes. When the uninstallation is complete, click OK.
Upgrade

Nov 18, 2014

To upgrade existing StoreFront 2.0 through 2.5.x deployments to StoreFront 2.6, run the StoreFront 2.6 installation file. Releases before StoreFront 2.0 cannot be upgraded to StoreFront 2.6 directly. Instead, you must first upgrade StoreFront 1.2 to StoreFront 2.0 before upgrading to StoreFront 2.6. Similarly, you cannot upgrade Receiver Storefront 1.1 to StoreFront 2.6 directly. You must upgrade Receiver Storefront 1.1 to StoreFront 1.2 and then again to StoreFront 2.0 before finally upgrading to StoreFront 2.6. For more information on upgrading from previous releases, see the StoreFront legacy product documentation.

Once the upgrade process is started, it cannot be rolled back. If the upgrade is interrupted or cannot be completed, the existing configuration is removed but StoreFront is not installed. Before starting to upgrade, you must disconnect users from the StoreFront deployment and prevent users 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 any files cannot be accessed by the installer, they cannot be replaced and so the upgrade will fail, resulting in the removal of the existing StoreFront configuration. StoreFront does not support multiple server deployments containing different product versions, so all servers in a group must be updated to the upgraded version before granting access to the deployment. Concurrent upgrade is not supported for multiple server deployments, servers must be upgraded sequentially. Citrix recommends that you back up your data before upgrading.

Uninstalling StoreFront removes the authentication service, stores, users' application subscriptions, Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs. This means that if you decide to uninstall StoreFront, you must manually recreate your services, stores, and sites when you reinstall StoreFront. Upgrading also enables you to preserve your StoreFront configuration and leaves users' application subscription data intact so that users do not need to resubscribe to all of their applications.

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.

To upgrade from StoreFront 2.1 to StoreFront 2.6

1. If you are upgrading a multiple server StoreFront deployment, disable access to the deployment through the load balancing environment.
   Disabling the load-balanced URL prevents users from connecting to the deployment during the upgrade. All servers in a multiple server deployment must be updated concurrently.

2. Restart the StoreFront server.
   Restarting the server ensures that any file locks are cleared and that there are no Windows updates pending.

3. Run the StoreFront installation file as an administrator.
   Important: Be sure that no other installations or updates are in effect while running the StoreFront upgrade.

4. Restart the StoreFront server and check that all the StoreFront services are running.
   Restarting the server ensures that all caches are cleared and the StoreFront services are restarted.

5. If you are upgrading a multiple server StoreFront deployment, repeat Steps 2 to 4 for each of the remaining servers in your deployment until you have upgraded them all.
   Important: Ensure you finish upgrading the current server before starting to upgrade the next. In multiple server StoreFront deployments, servers must be upgraded sequentially. Upgrading multiple servers in concurrently is not
supported and can cause configuration mismatches that lead to stores, sites, and services becoming unusable. When the upgrade process is complete on the final server in your deployment, StoreFront automatically updates the configuration of the other servers in the deployment to match that of the final server.

6. For multiple server StoreFront deployments, on each server in the deployment, open Event Viewer and, in the left pane, navigate to Applications and Services Logs > Citrix Delivery Services. Search for events logged by the Citrix Subscriptions Store Service with an Event ID of 3 and a Task Category of 2901. Ensure that an entry is logged for each store on every server in the deployment before continuing.

7. If you are upgrading a multiple server StoreFront deployment, restore access to your deployment through the load-balanced URL.
Manage

Aug 26, 2014

After initial configuration of StoreFront, further tasks that enable you to manage your deployment become available in the Citrix StoreFront management console. For certain advanced administration tasks, you must edit the StoreFront configuration files.

This section includes the following topics.

- Configure server groups
- Create and configure the authentication service
- Configure the authentication service
- Create or remove a store
- Create an unauthenticated store
- Configure stores
- Create a Receiver for Web site
- Configure Receiver for Web sites
- Add a NetScaler Gateway connection
- Configure NetScaler Gateway connection settings
- Configure beacon points
- Configure smart card authentication
- Set up highly available multi-site store configurations
- Configure StoreFront using the configuration files
- Configure Receiver for Web sites using the configuration files
- Disable workspace control reconnect for all Receivers
- Configure Desktop Appliance sites
- Configure authentication for XenApp Services URLs
- Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally
- Configure Resource Filtering
- Configure special folder redirection
- Manage subscription data
Configure server groups

Dec 01, 2014

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.

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.

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.

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. Any changes made on other servers in the group are discarded. While running this task, you cannot make any further changes until all the servers in the group have been updated.

Important: If you update the configuration of a server without propagating the changes to the other servers in the group, you might lose those updates if you later propagate changes from different server in the deployment.

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.

To configure IIS for HTTPS, use the Internet Information Services (IIS) Manager console on the StoreFront server to create a server certificate signed by your Microsoft Active Directory domain certification authority. Then add HTTPS binding to the default website. For more information about creating a server certificate in IIS, see http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate. For more information about adding HTTPS binding to an IIS site, see http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding.

Generate security keys for a server group

Use the Generate Security Keys task to generate new security keys for self-signed certificates used by a server group. When you generate new security keys, any users who are currently logged on will need to reauthenticate to their stores. As a result, this task is best carried out during periods of low user activity.
### mystore

<table>
<thead>
<tr>
<th>Overview</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated</td>
<td>No</td>
<td></td>
<td></td>
<td><a href="http://as-as-nest.un.com/CitrixStore">http://as-as-nest.un.com/CitrixStore</a></td>
<td></td>
</tr>
<tr>
<td>Advertised</td>
<td>Yes</td>
<td></td>
<td></td>
<td><a href="http://as-as-nest.un.com/CitrixStore">http://as-as-nest.un.com/CitrixStore</a></td>
<td></td>
</tr>
<tr>
<td>Subscription Enabled</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td><a href="http://as-as-nest.un.com/CitrixStore">http://as-as-nest.un.com/CitrixStore</a></td>
</tr>
<tr>
<td>URL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://as-as-nest.un.com/CitrixStore">http://as-as-nest.un.com/CitrixStore</a></td>
</tr>
</tbody>
</table>

#### Status

- **Warning:** StoreFront using HTTP not HTTPS.
Create Store for Unauthenticated Users

StoreFront

Storage

Information

Store Name

Delivery Controllers

Specify the delivery controllers and servers for this store.

Delivery controllers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Servers</th>
</tr>
</thead>
</table>

Add..  Edit..  Remove..
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<StoreName>" authenticationMode="windows" transferMode="Streamed">
  C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
</clientEndpoint>

<subscriptionsStoreClient enabled="true">
  <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_External" authenticationMode="windows" transferMode="Streamed">
    <clientCertificate thumbprint="0" />
  </clientEndpoint>
</subscriptionsStoreClient>

<subscriptionsStoreClient enabled="true">
  <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_Internal" authenticationMode="windows" transferMode="Streamed">
    <clientCertificate thumbprint="0" />
  </clientEndpoint>
</subscriptionsStoreClient>
mystore Receiver2

Overview
Website URL: https://us.ad-nest.us.com/Citrix/mystoreWeb
Store URL: mystore
Store Authenticated: No

Status
⚠️ StoreFront using HTTP not HTTPS.
DisableCtrlAltDel=Off

UseLocalUserAndPassword=On
Configure load balancing, failover, disaster recovery, and user mapping for a store

Jul 14, 2016

To set up load balancing, failover, disaster recovery, and user mapping, you edit the store configuration files. After configuring load balancing, failover, disaster recovery, and user mapping for a store, some tasks become unavailable in the Citrix StoreFront management console to prevent misconfiguration.

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. Ensure that you have configured the store with details of all the XenDesktop, XenApp, and VDI-in-a-Box 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 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.
   
   ```xml
   <resourcesWingConfigurations>
   <resourcesWingConfiguration name="Default" wingName="Default" />
   </resourcesWingConfigurations>
   ```

4. Specify your configuration as shown below.
   ```xml
   <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>
   ...
   </equivalentFarmSets>
   </userFarmMapping>
   ...
   </userFarmMappings>
   </resourcesWingConfiguration>
   </resourcesWingConfigurations>
   ```

---

https://docs.citrix.com  © 1999-2017 Citrix Systems, Inc. All rights reserved.  p.109
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 associated group of disaster recovery deployments. The **loadBalanceMode** 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. While deployments within an equivalent deployment set must be identical, deployments aggregated from different sets do not need to provide exactly the same resources. To specify that the deployments defined in a particular equivalent deployment set should not be aggregated with others, set the aggregation group name to **None**.

**primaryFarmRefs**
Specifies a set of equivalent XenDesktop, XenApp, or VDI-in-a-Box deployments providing identical resources. 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.

**optimalGatewayForFarms**
Specifies groups of deployments and defines the optimal NetScaler Gateway appliances for users to access resources provided by these deployments. Typically, the optimal appliance for a deployment is collocated in the same geographical location as that deployment. You only need to define optimal NetScaler Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal appliance.
Configure subscription synchronization

Sep 12, 2014
To configure periodic pull synchronization of users’ application 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.
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.

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.

1. Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, type the following commands to import the StoreFront modules.
   ```
   Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1"
   Import-Module "installationlocation\Management\Cmdlets\SubscriptionSyncModule.psm1"
   ```
   Where installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\.

2. To specify the remote StoreFront deployment containing the store to be synchronized, type the following command.
   ```
   Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname -clusterAddress deploymentaddress
   ```
   Where deploymentname is a name that helps you identify the remote deployment and deploymentaddress is the externally accessible address of the StoreFront server or load-balanced server group for the remote deployment.

3. To specify the remote store with which to synchronize users' application subscriptions, type the following command.
   ```
   Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname -storeName storename
   ```
   Where deploymentname is the name that you defined for the remote deployment in the previous step and storename is the name specified for both the local and remote stores when they were created. To synchronize application subscriptions between the stores, both stores must have the same name in their respective StoreFront deployments.

4. To configure synchronization to occur at a particular time every day, type the following command.
   ```
   Add-DSSubscriptionsSyncSchedule -scheduleName synchronizationname -startTime hh:mm
   ```
   Where synchronizationname is a name that helps you identify the schedule you are creating. Use the -startTime setting to specify a time of day at which you want to synchronize subscriptions between the stores. Configure further schedules to specify additional synchronization times throughout the day.

5. Alternatively, to configure regular synchronization at a specific interval, type the following command.
   ```
   Add-DSSubscriptionsSyncReoccurringSchedule -scheduleName synchronizationname -startTime hh:mm:ss -repeatMinutes interval
   ```
6. 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 will allow the servers in the remote deployment to access the subscription store service on the local deployment once you have configured a synchronization schedule on the remote deployment. The CitrixSubscriptionSyncUsers group is automatically created when you import the subscription synchronization module in Step 1. For more information about modifying local user groups, see http://technet.microsoft.com/en-us/library/cc772524.aspx.

7. If your local StoreFront deployment consists of multiple servers, use the Citrix StoreFront management console to propagate the configuration changes to the other servers in the group. For more information about propagating changes in a multiple server StoreFront deployment, see Configure server groups.

8. Repeat Steps 1 to 7 on the remote StoreFront deployment to configure a complementary subscription synchronization schedule from the remote deployment to the local deployment. When configuring the synchronization schedules for your StoreFront deployments, ensure that the schedules do not lead to a situation where the deployments are attempting to synchronize simultaneously.

9. To start synchronizing users' application subscriptions between the stores, restart the subscription store service on both the local and remote deployments. At a Windows PowerShell command prompt on a server in each deployment, type the following command.
   ```powershell
   Restart-DSSubscriptionsStoreSubscriptionService
   ```

10. To remove an existing subscription synchronization schedule, type the following command. Then, propagate the configuration change to the other StoreFront servers in the deployment and restart the subscription store service.
    ```powershell
    Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
    ```
    Where synchronizationname is the name that you specified for the schedule when you created it.

11. To list the subscription synchronization schedules currently configured for your StoreFront deployment, type the following command.
    ```powershell
    Get-DSSubscriptionsSyncScheduleSummary
    ```
Configure optimal NetScaler Gateway routing for a store

Nov 30, 2015

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 optimal NetScaler Gateway routing to optimize the handling of ICA connection routing from the HDX engine to published resources such as XenDesktop VDAs or XenApp or XenDesktop published applications using StoreFront. Typically, the optimal gateway for a site is collocated in the same geographical location.

You need only define optimal NetScaler 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.

Example scenario

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 UK 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 NetScaler Gateway defined and UK and US farms in its delivery controller list. UK users access remote resources through their geographically collocated 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 a single optimal gateway per site for each StoreFront store.

Figure 1. Suboptimal gateway routing
**Figure 2. Optimal gateway routing**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-SiteId (Int)</td>
<td>Site ID within IIS. This is typically 1 for the site in IIS where StoreFront is installed by default.</td>
</tr>
<tr>
<td>-ResourcesVirtualPath (String)</td>
<td>Path to the store that is to be configured to have a farm to optimal gateway mapping. Example: &quot;/Citrix/Store&quot;</td>
</tr>
<tr>
<td>-GatewayName (String)</td>
<td>Name given to identify the Netscaler Gateway within StoreFront. Example 1: ExternalGateway Example 2: InternalGateway</td>
</tr>
<tr>
<td>-Hostnames (String Array)</td>
<td>Specifies the fully qualified domain name (FQDN) and port of the optimal NetScaler Gateway appliance. Example1 for standard vServer port 443: gateway.example.com Example2 for nonstandard vServer port 500: gateway.example.com:500</td>
</tr>
</tbody>
</table>
### Farms (String Array)
Specifies a set of (typically collocated) XenDesktop, XenApp, and VDI-in-a-Box deployments that share a common optimal NetScaler Gateway appliance. A farm can contain just a single delivery controller or multiple delivery controller that provides published resources.

You can configure a XenDesktop 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

### staUrls (String Array)
Specifies the URLs for XenDesktop, XenApp, and VDI-in-a-Box servers running the Secure Ticket Authority (STA). If using multiple farms, list the STA servers on each using a comma separated list:


### 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 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: 00.02:00:00

### 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 NetScaler Gateway.

---

Note: When PowerShell scripts span multiple lines such as shown below, each line must end with the backtick control character (`). Copy the following code examples into the Windows PowerShell Integrated Scripting Environment (ISE) to validate the code using the dynamic compiler before you run it.

**Configure an optimal gateway for a farm**

Example:

Create or overwrite OptimalGatewayForFarms 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"
  -StaUris "https://xenapp.example.com\scripts\ctxsta.dll","https://xendesktop.example.com\scripts\ctxsta.dll"
  -StasUseLoadBalancing:$false
  -StasBypassDuration 00:02:00:00
  -EnableSessionReliability:$false
  -UseTwoTickets:$false
  -EnabledOnDirectAccess:$true

Example:

This script returns configured OptimalGatewayForFarms for the store called 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 a NULL gateway for a farm

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”

Determine if your OptimalGatewayForFarms 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

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.
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 gateway Gateway1 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.
To configure a store for NetScaler Gateway global server load balancing

Oct 21, 2013
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 the Enable Remote Access task to configure the store with details of your load-balanced NetScaler Gateway deployment. For more information, see Manage remote access to stores through NetScaler Gateway.
2. When prompted for the NetScaler Gateway URL, enter the load-balanced URL for the deployment. For the subnet IP address, specify the virtual server IP address for one of the appliances in your deployment.
3. Repeat the process using exactly the same settings except for the display name and the subnet IP address. For the subnet IP address, enter the virtual server IP address for another appliance in your deployment.
4. Continue until you have added entries for all the appliances in your load-balanced NetScaler Gateway deployment. Each entry should be identical except for the display name and the subnet IP address.
Examples of highly available multi-site store configurations

Oct 08, 2015

StoreFront enables you to configure load balancing and failover between the deployments providing resources for stores, map users to deployments, and designate specific disaster recovery deployments for increased resiliency. To illustrate how you can configure StoreFront deployments distributed over multiple sites to provide high availability for your stores, consider the example configuration below.

The figure shows an example highly available multi-site configuration.

The example consists of two main locations, each with separate, load-balanced groups of StoreFront servers, providing desktops and application for users. A third location provides disaster recovery resources that are only intended to be used in the event that all resources provided by both the other locations are unavailable. Location 1 contains a group of identical deployments (XenDesktop sites, XenApp farms, or VDI-in-a-Box grids) providing exactly the same desktops and applications. Location 2 consists of a similar group of identical deployments delivering largely the same resources provided in Location 1, but with a few differences. Some specific resources that are not available in Location 2 are provided by a separate unique deployment in Location 1.

In this example, you want users at both locations to be able to log on to their local StoreFront servers and access desktops and applications provided locally, where possible. In the event that local resources are not available, either due to a failure or capacity issues, users must be automatically and silently redirected to resources delivered from the other location. If all resources provided by both locations are unavailable, users must be able to continue working with a subset of the most
business-critical desktops and applications.

To achieve this user experience, you configure the store in Location 1 as shown below.

```
<resourcesWingConfigurations>
  <resourcesWingConfiguration name="Default" wingName="Default">
    <userFarmMappings>
      <clear />
      <userFarmMapping name="user_mapping">
        <groups>
          <group name="Everyone" sid="everyone" />
        </groups>
      </userFarmMapping>
      <equivalentFarmSets>
        <equivalentFarmSet name="Location1" loadBalanceMode="LoadBalanced" aggregationGroup="AggregationGroup1">
          <primaryFarmRefs>
            <farm name="Location1Deployment1" />
            <farm name="Location1Deployment2" />
            <farm name="Location1Deployment3" />
          </primaryFarmRefs>
          <backupFarmRefs>
            <farm name="DisasterRecoveryDeployment" />
          </backupFarmRefs>
        </equivalentFarmSet>
        <equivalentFarmSet name="Location2" loadBalanceMode="Failover" aggregationGroup="AggregationGroup1">
          <primaryFarmRefs>
            <farm name="Location2Deployment1" />
            <farm name="Location2Deployment2" />
            <farm name="Location2Deployment3" />
          </primaryFarmRefs>
          <backupFarmRefs>
            <farm name="DisasterRecoveryDeployment" />
          </backupFarmRefs>
        </equivalentFarmSet>
        <equivalentFarmSet name="Location1Unique" loadBalanceMode="LoadBalanced" aggregationGroup="">
          <primaryFarmRefs>
            <farm name="Location1UniqueDeployment" />
          </primaryFarmRefs>
          <backupFarmRefs>
          </backupFarmRefs>
        </equivalentFarmSet>
      </equivalentFarmSets>
    </userFarmMappings>
  </resourcesWingConfiguration>
</resourcesWingConfigurations>
```

There is a single mapping available to all users, listing the Location 1 deployments first and the Location 2 deployments second. In both cases, the disaster recovery deployment is configured as the backup and all the deployments are assigned to
the same aggregation group. The configuration of the store in Location 2 is almost identical, differing only in that the order in which the deployments are listed is reversed such that the Location 2 deployments are listed first. In both cases, the deployment providing the Location 1 unique resources is listed last with no backup deployment or aggregation group defined.

When users at Location 1 log on to their local store, StoreFront contacts a Location 1 deployment to enumerate the desktops and applications available. Because the loadBalanceMode attribute is set to LoadBalanced, the exact deployment contacted is selected randomly to evenly distribute requests across the available deployments. If the selected Location 1 deployment is unavailable, StoreFront randomly selects another Location 1 deployment to contact.

In the case of the Location 2 deployments, the loadBalanceMode attribute is set to Failover. This means that StoreFront always contacts the deployments in the specified order. As a result, resources are enumerated from Location 2 Deployment 1 for every user request until Deployment 1 stops responding. Subsequent requests are then routed to Deployment 2 until Deployment 1 becomes available again. This minimizes the number of deployments in use at Location 2 at any given time.

When a response is received from a Location 1 deployment, StoreFront does not contact any further Location 1 deployments. Including all the Location 1 deployments in a single <equivalentFarmSet> element specifies that these deployments provide exactly the same resources. Similar behavior also occurs during enumeration of the Location 2 resources. Finally, the Location 1 unique deployment is contacted, although since there is no alternative in this case, the unique resources are not enumerated if the deployment is unavailable.

Where a desktop or application with the same name and path on the server is available from both Location 1 and Location 2, StoreFront aggregates these resources and presents users with a single icon. This behavior is a result of setting the aggregationGroup attribute to AggregationGroup1 for both the Location 1 and Location 2 deployments. Users clicking on an aggregated icon are typically connected to the resource in their location, where available. However, if a user already has an active session on another deployment that supports session reuse, the user is preferentially connected to the resource on that deployment to minimize the number of sessions used.

Because an aggregation group is not specified for the Location 1 unique resources, users see separate icons for each of the unique resources. In this example, none of the unique resources are available on the other deployments. However, if a desktop or application with the same name and path on the server were available from another deployment, users would see two icons with the same name.

Only when resources cannot be enumerated from any of the Location 1 or Location 2 deployments does StoreFront contact the disaster recovery deployment. Because the same disaster recovery deployment is configured for both Location 1 and Location 2, all of these deployments must be unavailable before StoreFront will attempt to enumerate the disaster recovery resources. In this example, a disaster recovery alternative is not configured for the Location 1 unique deployment, so the availability of the unique deployment does not affect this determination.

In this example, you want to provide different mixtures of resources for different users on the basis of their membership of Microsoft Active Directory user groups. Standard users in Location 1 and Location 2 only need access to the desktops and applications provided locally. These users do not need to access resources in the other locations. You also have a group of power users for whom you want to provide access to all the available resources, including the Location 1 unique resources, with high availability and disaster recovery. For this example, it is assumed that Location 1 and Location 2 share a common Active Directory domain.

To achieve this user experience, you configure the stores in both locations as shown below.

```xml
<resourcesWingConfigurations>
  <resourcesWingConfiguration name="Default" wingName="Default">
```
<userFarmMappings>
  <clear />
  <userFarmMapping name="UserMapping1">
    <groups>
      <group name="Location1Users"
          sid="S-1-5-21-1004336348-1177238915-682003330-1001" />
    </groups>
    <equivalentFarmSets>
      <equivalentFarmSet name="Location1" loadBalanceMode="LoadBalanced"
          aggregationGroup="AggregationGroup1">
        <primaryFarmRefs>
          <farm name="Location1Deployment1" />
          <farm name="Location1Deployment2" />
          <farm name="Location1Deployment3" />
        </primaryFarmRefs>
        <backupFarmRefs>
          <farm name="DisasterRecoveryDeployment" />
        </backupFarmRefs>
      </equivalentFarmSet>
      <equivalentFarmSets>
        <equivalentFarmSet name="Location2" loadBalanceMode="Failover"
          aggregationGroup="AggregationGroup1">
          <primaryFarmRefs>
            <farm name="Location2Deployment1" />
            <farm name="Location2Deployment2" />
            <farm name="Location2Deployment3" />
          </primaryFarmRefs>
          <backupFarmRefs>
            <farm name="DisasterRecoveryDeployment" />
          </backupFarmRefs>
        </equivalentFarmSet>
      </equivalentFarmSets>
    </userFarmMapping>
  <userFarmMapping name="UserMapping2">
    <groups>
      <group name="Location2Users"
          sid="S-1-5-21-1004336348-1177238915-682003330-1002" />
    </groups>
    <equivalentFarmSets>
      <equivalentFarmSet name="Location1Unique" aggregationGroup="AggregationGroup1">
        <primaryFarmRefs>
          <farm name="Location1Deployment1" />
          <farm name="Location1Deployment2" />
          <farm name="Location1Deployment3" />
        </primaryFarmRefs>
        <backupFarmRefs>
          <farm name="DisasterRecoveryDeployment" />
        </backupFarmRefs>
      </equivalentFarmSet>
    </equivalentFarmSets>
  </userFarmMapping>
</userFarmMappings>
Instead of creating a mapping that applies to all users, as in the load balancing and failover example, you create mappings for specific user groups. The main Location 1 deployments are mapped to the domain user group for Location 1 users. Similarly, the Location 2 deployments are mapped to the Location 2 user group. The mapping for the Location 1 unique resources specifies both user groups, which means that users must be members of both groups to access the unique resources.

Users who are members of the Location 1 user group see only resources from Location 1 when they log on to a store, even if that store is in Location 2. Likewise, Location 2 user group members are only presented with resources from Location 2. Neither group have access to the Location 1 unique resources. Domain users who are not members of either group can log on to the store, but do not see any desktops or applications.

To give your power users access to all the resources, including the unique resources, you add them to both user groups. When users who are members of both the Location 1 and Location 2 user groups log on to the store, they see an aggregate of the resources available from both locations, plus the Location 1 unique resources. As in the load balancing and failover example, the Location 1 and Location 2 deployments are assigned to the same aggregation group. The resource aggregation process functions in exactly the same way as described for the load balancing and failover example.

Disaster recovery also operates as described in the load balancing and failover example. Users only see the disaster recovery resources when all the Location 1 and Location 2 deployments are unavailable. Unfortunately, this means that there are some scenarios when standard users are not able to access any desktops or applications. For example, if all the deployments in Location 1 are unavailable, but the Location 2 deployments are still accessible, StoreFront does not enumerate the disaster recovery resources. So, users who are not members of the Location 2 user group do not see any resources in the store.

To resolve this issue, you would need to configure separate disaster recovery deployments for the Location 1 and Location 2 mappings. You would then add the disaster recovery deployments to the same aggregation group to aggregate the disaster recovery resources for your power users.

In the load balancing and failover and user mapping examples, users moving between Location 1 and Location 2 would benefit from synchronization of their application subscriptions between the two deployments. For example, a user based in Location 1 could log on to the StoreFront deployment in Location 1, access the store, and subscribe to some applications. If the same user then traveled to Location 2 and accessed the similar store provided by the Location 2 StoreFront deployment, the user would need to resubscribe to all the applications again to access them from Location 2. By default, StoreFront deployments in each location maintain details of users' application subscriptions separately.

To ensure that users need to subscribe only to applications in one location, you can configure subscription synchronization between the stores of the two StoreFront deployments.

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 PowerShell before opening the StoreFront console.

Delivery Controller names are case sensitive. Failing to duplicate the Delivery Controller names exactly may lead to inaccurate resource IDs across subscription synchronization stores.

1. Both stores must have the same name in both deployment locations. For example GlobalStore in Location 1 – London and Location 2 – New York could be configured as:

<table>
<thead>
<tr>
<th>Name</th>
<th>Authenticated</th>
<th>Advertised</th>
<th>Store URL</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalStore</td>
<td>Yes</td>
<td>Yes</td>
<td><a href="http://london.citrix.com/Citrix/GlobalStore">http://london.citrix.com/Citrix/GlobalStore</a></td>
<td>Internal and external networks</td>
</tr>
<tr>
<td>LocalStore</td>
<td>Yes</td>
<td>Yes</td>
<td><a href="http://london.citrix.com/Citrix/LocalStore">http://london.citrix.com/Citrix/LocalStore</a></td>
<td>Internal network only</td>
</tr>
</tbody>
</table>

GlobalStore

Overview

- Authenticated: Yes
- Advertised: Yes
- URL: http://london.citrix.com/Citrix/GlobalStore

GlobalStore

Overview

- Authenticated: Yes
- Advertised: Yes
- URL: http://newyork.citrix.com/Citrix/GlobalStore

2. Ensure the Delivery Controllers configured within the “GlobalStore” store have the same names and are case sensitive.
3. Start a new PowerShell session on a StoreFront server in Location 1 – London and run these commands:

# Import the required StoreFront modules
Import-Module "C:\Program Files\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

# Add the New York cluster as one to synchronize from.
# The clusterName is used to identify the cluster.
# The clusterAddress is either the address of the single
# StoreFront server when not in a group or the loadbalanced address when it is.
# The storeFriendlyNames is the display name of the store.
Add-DSSubscriptionsRemoteSyncClusterAndStores -clusterName “NewYork”
-clusterAddress “newyork.citrix.com” -storeFriendlyNames @("GlobalStore")

# Add the servers from the New York deployment on the
# XenDesktop domain to the Windows permissions group on the
# London1 server.
Add-DSLocalGroupMember -GroupName “CitrixSubscriptionsSyncUsers”
-AccountName “my.xendesktop.com/newyork1$”
Add-DSLocalGroupMember -GroupName “CitrixSubscriptionsSyncUsers”
-AccountName “my.xendesktop.com/newyork2$”

# Add a schedule to pull subscription data from New York to London starting at 18:00
# repeating every 24 hours.
Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName “SyncFromNewYork” -startTime “18:00:00”
-repeatMinutes 1440

# Restart the synchronization service and propagate settings to the other servers in the
# London deployment.
Restart-Service "CitrixSubscriptionsStore"
Start-DSConfigurationReplicationClusterUpdate
Get-DSSubscriptionsRemoteClusterSyncSummary
Get-DSSubscriptionsSyncScheduleSummary

4. Close the PowerShell session.
5. Start a PowerShell session on a server in Location 2 – New York and run the following commands:
   # Import the required StoreFront modules
   Import-Module "C:\Program Files\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"

   # Add the London cluster as one to synchronize from.
   # The clusterName is used to identify the cluster.
   # The clusterAddress is either the address of the single
   # StoreFront server when not in a group or the loadbalanced address when it is.
   # The storeFriendlyNames is the display name of the store.
   Add-DSSubscriptionsRemoteSyncClusterAndStores -clusterName "London"
   -clusterAddress "london.citrix.com" -storeFriendlyNames @("GlobalStore")

   # Add the servers from the London deployment on the
   # XenDesktop domain to the Windows permissions group on the NewYork1 server.
   Add-DsLocalGroupMember -GroupName "CitrixSubscriptionsSyncUsers"
   -AccountName "my.xendesktop.com\london1$"
   Add-DsLocalGroupMember -GroupName "CitrixSubscriptionsSyncUsers"
   -AccountName "my.xendesktop.com\london2$"

   # Add a schedule to pull subscription data from London to New York starting at 20:00
   # repeating every 24 hours.
   Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName "SyncFromNewYork" -startTime "20:00:00"
   -repeatMinutes 1440

   # Restart the synchronization service and propagate settings to the other servers in
   # the New York deployment.
   Restart-Service "CitrixSubscriptionsStore"
   Start-DSConfigurationReplicationClusterUpdate
   Get-DSSubscriptionsRemoteClusterSyncSummary
   Get-DSSubscriptionsSyncScheduleSummary

In this example, you want to configure separate NetScaler Gateway appliances in Location 1 and Location 2. Because Location 1 resources are available to users in Location 2, you want to ensure that user connections to Location 1 resources are always routed through the NetScaler Gateway appliance in Location 1, regardless of the way in which users access the store. A similar configuration is required for Location 2.

In the case of the Location 1 unique resources, you have made these desktops and applications accessible only to local users on the internal network. However, you still require users to authenticate to NetScaler Gateway to access a store. So, you want to ensure that user connections to Location 1 unique resources are not routed through NetScaler Gateway, despite
the fact that users connect to the stores through NetScaler Gateway.

To achieve this user experience, you configure the stores in both locations as shown below.

```
<optimalGatewayForFarmsCollection>
  <optimalGatewayForFarms enabledOnDirectAccess="true">
    <farms>
      <farm name="Location1Deployment1" />
      <farm name="Location1Deployment2" />
      <farm name="Location1Deployment3" />
    </farms>
    <optimalGateway key="_" name="Location1Appliance" stasUseLoadBalancing="false"
                    stasBypassDuration="02:00:00" enableSessionReliability="true"
                    useTwoTickets="false">
      <hostnames>
        <add hostname="location1appliance.example.com" />
      </hostnames>
      <staUrls>
        <add staUrl="https://location1appliance.example.com\scripts/ctxsta.dll" />
      </staUrls>
    </optimalGateway>
  </optimalGatewayForFarms>
  <optimalGatewayForFarms enabledOnDirectAccess="true">
    <farms>
      <farm name="Location2Deployment1" />
      <farm name="Location2Deployment2" />
      <farm name="Location2Deployment3" />
    </farms>
    <optimalGateway key="_" name="Location2Appliance" stasUseLoadBalancing="false"
                    stasBypassDuration="02:00:00" enableSessionReliability="true"
                    useTwoTickets="false">
      <hostnames>
        <add hostname="location2appliance.example.com" />
      </hostnames>
      <staUrls>
        <add staUrl="https://location2appliance.example.com\scripts/ctxsta.dll" />
      </staUrls>
    </optimalGateway>
  </optimalGatewayForFarms>
  <optimalGatewayForFarms enabledOnDirectAccess="false">
    <farms>
      <farm name="Location1UniqueDeployment" />
    </farms>
  </optimalGatewayForFarms>
</optimalGatewayForFarmsCollection>
```

You map the main Location 1 deployments to the NetScaler Gateway appliance in Location 1. This configuration ensures that users always connect to Location 1 resources through the NetScaler Gateway appliance in that location, even for users that logged on to the store through the appliance in Location 2. A similar mapping is configured for Location 2. For both deployments, you set the value of the enabledOnDirectAccess attribute to true to route all connections to resources through the optimal appliance specified for the deployment, even for local users on the internal network who log on to
StoreFront directly. As a result, the responsiveness of remote desktops and applications is improved for local users because data do not traverse the corporate WAN.

For the Location 1 unique resources, you configure a mapping for the deployment but do not specify a NetScaler Gateway appliance. This configuration ensures that connections to Location 1 unique resources are not routed through NetScaler Gateway, even for users that logged on to the store through NetScaler Gateway. As a result, only local users on the internal network can access these desktops and applications.

You must also configure a specific internal virtual server IP address for the appliance and an inaccessible internal beacon point. Making the internal beacon point inaccessible to local users prompts Citrix Receiver to access stores through NetScaler Gateway from devices connected to the internal network. This enables you, for example, to apply NetScaler Gateway endpoint analysis to local users on the internal network without the overhead of routing all user connections to resources through the appliance.
Configure StoreFront using the configuration files

Aug 26, 2014
This section describes additional configuration tasks that cannot be carried out using the Citrix StoreFront management console.

- Enable ICA file signing
- Configure communication time-out duration and retry attempts
- Configure the password expiry notification period
- Disable file type association
- Enable socket pooling
- Customize the Citrix Receiver logon dialog box
- Prevent Receiver for Windows from caching passwords
- Configure server bypass behavior
Enable ICA file signing

Oct 31, 2016

StoreFront provides the option to digitally sign ICA files so that versions of Citrix Receiver 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 Receiver, 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. 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. Ensure that the certificate you want to use to sign ICA files is available in the Citrix Delivery Services certificate store on the StoreFront server and not the current user's certificate store.
2. 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.
   
   ```xml
   <certificateManager>
   <certificates>
   <clear />
   <add ... />
   ...
   </certificates>
   </certificateManager>
   ```

4. Include details of the certificate to be used for signing as shown below.
   
   ```xml
   <certificateManager>
   <certificates>
   <clear />
   <add id="certificateid" thumb="certificatethumbprint" />
   <add ... />
   ...
   </certificates>
   </certificateManager>
   ```

   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.

5. Locate the following element in the file.
   
   ```xml
   <icaFileSigning enabled="False" certificateid="" hashAlgorithm="sha1" />
   ```

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 hashAlgorithm 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.

```
$certificate = Get-DSCertificate "certificatethumbprint"
Add-DSCertificateKeyReadAccess -certificate $certificate[0] -accountName "IIS APPPOOL\Citrix Delivery Services Resources"
```

Where `certificatethumbprint` is the digest of the certificate data produced by the hash algorithm.
Configure communication time-out duration and retry attempts

Aug 26, 2014

By default, requests from StoreFront to a server providing resources for a store time out after 30 seconds. The server is considered unavailable after two unsuccessful communication attempts. To change these settings, you edit the configuration 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 web.config files for the store, which is typically located in the
   
C:\inetpub\wwwroot\Citrix\Authentication\ and C:\inetpub\wwwroot\Citrix\storename\ directories, respectively, where storename is the name specified for the store when it was created.

2. Locate the following element in the file.

   <farmset ... serverCommunicationAttempts="2" communicationTimeout="30"
   connectionTimeout="6" ... >

3. Change the value of the serverCommunicationAttempts attribute to the set the number of unsuccessful communication attempts before the server is considered to be unavailable. Use the communicationTimeout attribute to set the time limit in seconds for a response from the server. Set the time limit in seconds for StoreFront to resolve the address of the server by changing the value of the connectionTimeout attribute.
Configure the password expiry notification period

Aug 26, 2014

If you enable 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. 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 edit the configuration file for the authentication service.

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 web.config file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication directory.
2. Locate the following element in the file.

   <explicitBL ... allowUserPasswordChange="Always"
       showPasswordExpiryWarning="Windows" passwordExpiryWarningPeriod="10" ... >

3. Ensure that the allowUserPasswordChange attribute is set to Always to enable password expiry notifications. Change the value of the showPasswordExpiryWarning attribute to Custom to apply a specific password expiry notification period to all users. Use the passwordExpiryWarningPeriod attribute to set the password expiry notification period in days. Receiver for Web site users connecting from the local network whose passwords are due to expire within the specified time period are shown a warning when they log on.
Disable file type association

Aug 26, 2014

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.

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 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.
Enable socket pooling

Aug 26, 2014

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.

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 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 ... pooledSockets="off" ... >

3. Change the value of the pooledSockets attribute to on to enable socket pooling for the store.
Customize the Citrix Receiver logon dialog box

Sep 11, 2014

When Citrix Receiver 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 Citrix Receiver logon dialog box, you edit the files for the authentication service.

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

3. Uncomment the statement by removing the leading and trailing leading @* and trailing *@, as shown below.
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   Citrix Receiver 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 ExplicitAuth.resx file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\ directory.

5. Locate the following elements in the file. Edit the text enclosed within the <value> element to modify the title text that users see on the Citrix Receiver 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 Citrix Receiver logon dialog box title text for users in other locales, edit the localized files ExplicitAuth.languagecode.resx, where languagecode is the locale identifier.
Prevent Receiver for Windows from caching passwords and usernames

Nov 04, 2014

By default, Receiver for Windows stores users' passwords when they log on to StoreFront stores. To prevent Receiver for Windows, but not Receiver for Windows Enterprise, from caching users' passwords, you edit the files for the authentication service.

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 inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrm file.
2. Locate the following line in the file.
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))
3. Comment the statement as shown below.
   <!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials")) -->

Receiver for Windows users must enter their passwords every time they log on to stores that use this authentication service. This setting does not apply to 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, Receiver for Windows automatically populated the last username entered. To suppress 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 server bypass behavior

Mar 09, 2016

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:

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

**Considerations when specifying allFailedBypassDuration**

Setting a larger allFailedBypassDuration reduces the impact of unavailability of a particular Delivery Controller; however, it has the negative effect 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 allFailedBypassDuration values when many Delivery Controllers have been configured for a Store, particularly for nonbusiness-critical Delivery Controllers.

Setting a smaller allFailedBypassDuration 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. 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 for the Delivery Controller you want to configure:

   ```xml
   <farm name="deliverycontrollername" ... allFailedBypassDuration="0" ... >
   ```

3. Change the value of the **allFailedBypassDuration** attribute to the maximum number of minutes that StoreFront should allow all servers from the specified Delivery Controller to be bypassed.
4. If desired, add (or update if the attribute is already present) the **bypassDuration** attribute to specify the number of minutes an individual server should be bypassed when StoreFront fails to contact that server.
Configure Receiver for Web sites using the configuration files

Oct 21, 2013
This section describes additional configuration tasks for Receiver for Web sites that cannot be carried out using the Citrix StoreFront management console.

- Configure how resources are displayed for users
- Make Citrix Receiver installation files available on the server
- Disable detection and deployment of Citrix Receiver
- Configure workspace control
- Stop offering provisioning files to users
- Configure Receiver for HTML5 use of browser tabs
- Configure store time-out duration and retry attempts
- Configure session duration
Configure how resources are displayed for users

Sep 12, 2014
When both desktops and applications are available from a Receiver for Web site, separate desktop and application views are displayed by default. Users see the desktop view first when they log 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.

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 web.config file for the 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" />

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">

5. Change the value of the autoLaunchDesktop attribute to false to prevent 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 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

Jul 24, 2014

By default, Receiver for Web displays the My Apps Folder View for unauthenticated (access for unauthenticated users) and mandatory (all published applications are available in the Home screen without users subscribing to them) stores. This view displays applications in a folder hierarchy and includes a breadcrumb path.

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 web.config file for the 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.
   <userInterface enableAppsFolderView="true"/>
3. Change the value of the enableAppsFolderView attribute to false to disable Receiver for Web My Apps Folder View.
Make Citrix Receiver installation files available on the server

Dec 18, 2014
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 Receiver is installed on the user's device. If Citrix Receiver cannot be detected, the user is prompted to download and install the appropriate Citrix Receiver for their platform from the Citrix website.

If you copy Receiver for Windows and Receiver for Mac installation files to the StoreFront server, you can configure the site to provide users with these local files rather than redirecting them to the Citrix website. When Citrix Receiver installation files are available on the StoreFront server, you can also configure the site to offer users with older clients the option to upgrade to the version on the server. To configure deployment of Receiver for Windows and Receiver for Mac, you run Windows PowerShell scripts and edit the site configuration file.

Note: These changes cannot be reverted. If you are not changing other configuration settings, you may revert with the following workaround: Back up the web.config file under C:\inetpub\wwwroot\citrix\<storename> before you change the download link and restore the web.config file when you want to revert it back. Make a copy of the default setting to refer to. 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.

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. Copy the Receiver for Windows and Receiver for Mac installation files to \Receiver Clients\Windows\ and \Receiver Clients\Mac\ directories, respectively, in the StoreFront installation, which is typically located at C:\Program Files\Citrix\Receiver StoreFront\.
   You also have the option to copy Citrix Receiver installation files to the server when installing StoreFront at a command prompt. For more information, see To install StoreFront at a command prompt.

2. Using an account with local administrator permissions, start Windows PowerShell and, at a command prompt, type the following commands to update StoreFront with the Citrix Receiver installation file names.
   & "installationlocation\Scripts\UpdateWindowsReceiverLocation.ps1"
   -ClientLocation "Windows\filename.exe"
   & "installationlocation\Scripts\UpdateMacOSReceiverLocation.ps1"
   -ClientLocation "Mac\filename.dmg"
   Where installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\, and filename is the name of the Citrix Receiver installation file.

3. On the StoreFront server, use a text editor to open the web.config file for the 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.

4. Locate the following element in the file.
   <pluginAssistant ...
   upgradeAtLogin="false"/>

5. Set the value of the upgradeAtLogin attribute to true to offer users with older clients the option to upgrade to the versions available on the server.
Disable detection and deployment of Citrix Receiver

Sep 12, 2014

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 Receiver is installed on the user’s device. If Citrix Receiver cannot be detected, the user is prompted to download and install the appropriate Citrix Receiver for their platform from the Citrix website. To disable detection and deployment of Receiver for Windows and Receiver for Mac for the Receiver for Web site, 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. Use a text editor to open the web.config file for the 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.
   `<pluginAssistant enabled="true" ... >`
3. Change the value of the enabled attribute to false to disable detection and deployment of Citrix Receiver for the site.
Configure workspace control for Receiver for Web

Sep 12, 2014

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 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. Use a text editor to open the web.config file for the 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.
   <workspaceControl enabled="true" autoReconnectAtLogon="true"
   logoffAction="disconnect" showReconnectButton="false"
   showDisconnectButton="false" />

3. Change the value of the enabled attribute to false to disable workspace control for the site. Set the value of the autoReconnectAtLogon attribute to false to prevent automatic reconnection of users to any applications that they left running. To automatically shut down users' applications when they log off from the site, set the value of the logoffAction attribute to terminate. Set logoffAction to none to leave users' applications running and active when they log off from the site.

   By default, autoReconnectAtLogon is set to true and logoffAction is set to disconnect. This configuration enables a user to log on to a site, start their applications, then log on to the same site using a different device and have those resources automatically transferred to the new device. All the applications that the user starts from a particular site are left running but are automatically disconnected when the user logs off from that site, provided that the same browser instance is used to log on, start the resources, and log off. If there is only one desktop available for a user on a Receiver for Web site that is configured to start single desktops automatically when the user logs on, that user's applications are not reconnected, even if the autoReconnectAtLogon attribute is set to true.

   Disable automatic reconnection of applications at logon to enable users to choose whether they want their applications to follow them from device to device. If you disable automatic reconnection of applications at logon, ensure that the Connect link is enabled so that users can manually reconnect to applications that they left running.

4. Change the value of the showReconnectButton attribute to true to display on the site the Connect link, which enables users to manually reconnect to applications that they left running. Set the value of the showDisconnectButton attribute to true to display the Disconnect link, which enables users to manually disconnect from applications without shutting them down.

   By default, the Connect and Disconnect links do not appear on sites. Enable the links and disable automatic reconnection of applications at logon to enable users to choose whether they want their applications to follow them from device to device.
Stop offering provisioning files to users

Sep 12, 2014

By default, Receiver for Web sites offer provisioning files that enable users to configure Citrix Receiver 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 NetScaler Gateway deployments and beacons configured for the store. To stop offering Citrix Receiver provisioning files to users, 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. Use a text editor to open the web.config file for the 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.
   <receiverConfiguration enabled="true" ... />
3. Change the value of the enabled attribute to false to remove from the site the option for users to download a provisioning file.
Configure Receiver for HTML5 use of browser tabs

Sep 12, 2014

By default, Receiver for HTML5 starts desktops and applications in a new browser tab. However, when users start resources from shortcuts using Receiver for HTML5, the desktop or application replaces the Receiver for Web site in the existing browser tab rather than appearing in a new tab. To configure Receiver for HTML5 so that resources are always started in the same tab as the Receiver for Web site, 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. Use a text editor to open the web.config file for the 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.
   <html5 ... singleTabLaunch="false" />
3. Change the value of the singleTabLaunch attribute to true to start desktops and applications with Receiver for HTML5 in the same browser tab as the Receiver for Web site instead of opening a new tab.
Configure store time-out duration and retry attempts

Sep 12, 2014

By default, requests from a Receiver for Web site to the associated store time out after one minute. The store is considered unavailable after two unsuccessful communication attempts. To change these settings, 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. Use a text editor to open the web.config file for the 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.
   
   <communication attempts="2" timeout="00:01:00">
   
3. Change the value of the attempts attribute to set the number of unsuccessful communication attempts before the store is considered to be unavailable. Use the timeout attribute to set the time limit in hours, minutes, and seconds for a response from the store.
Configure session duration

Mar 09, 2016

Once authenticated, users can, by default, access XenDesktop, XenApp, or VDI-in-a-Box resources for up to eight hours without needing to log on again. By default, user sessions on Receiver for Web sites time out after 20 minutes of inactivity. When a session times out, users can continue to use any desktops or applications that are already running, but must log on again to access Receiver for Web site functions such as subscribing to applications. To change these settings, 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. Use a text editor to open the web.config file for the 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.
   
   `<authentication tokenLifeTime="08:00:00" ... />`

3. Change the value of the `tokenLifeTime` attribute to set the time in hours, minutes, and seconds for which users, once authenticated to XenDesktop, XenApp, or VDI-in-a-Box can continue to use resources provided by that deployment.

4. Locate the following element in the file.
   
   `<sessionState timeout="20" />`

5. Use the `timeout` attribute to set the time in minutes for which a Receiver for Web site session can remain idle before the user is required to log on again to access the site.

---

**Note**

The timeout of Receiver for Website is actually one minute before the value that is set. If the value is set to 1 the timeout will be at 30 seconds. Alerts will appear at the halfway point of the actual timeout for values set at 6 or less. For example, if the value is set at 4 the actual timeout will be 3 minutes and the alert will appear at 1 minute 30 seconds. For values 7 and higher, the alert will appear at 5 minutes.
Disable workspace control reconnect for all Receivers

May 04, 2017
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 all Receivers. Manage this feature by using PowerShell or by editing `web.config`.

Make sure that you close the Administration Console. Run the following code snippet to import the StoreFront PowerShell modules:

```powershell
$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

```powershell
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:

```powershell
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store -IsAllowed $false
```

Open `web.config` under the Store Service (for example, /Citrix/Store) in a text editor. Locate the lines similar to:

```xml
<resourcesService id="f01f7dc4-7f28-4bc1-b8fb-7c0db9570d20"
    storeLockedDown="false"
    anonymousStore="false" allowSessionReconnect="true" />
```

Change the value of `allowSessionReconnect` to `false` to disable workspace control reconnect or `true` to enable it.
Configure Desktop Appliance sites

May 21, 2014

The tasks below describe how to create, remove, and modify Desktop Appliance sites. To create or remove sites, you execute Windows PowerShell commands. Changes to Desktop Appliance site settings are made by editing the site 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.

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.

Only a single store can be accessed through each Desktop Appliance site. You can create a store containing all the resources you want to make available to users with non-domain-joined desktop appliances. Alternatively, create separate stores, each with a Desktop Appliance site, and configure your users' desktop appliances to connect to the appropriate site.

1. Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, type the following command to import the StoreFront modules.

   & "installationlocation\Scripts\ImportModules.ps1"

   Where installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\.

2. To create a new Desktop Appliance site, type the following command.

   Install-DSDesktopAppliance -FriendlyName sitename -SiteId iid -VirtualPath sitepath -UseHttps {$False | $True} -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}] [-EnableExplicit {$True | $False}] [-EnableSmartCard {$False | $True}] [-EnableEmbeddedSmartCardSSO {$False | $True}]

   Where sitename is a name that helps you to identify your Desktop Appliance site. For iid, specify the numerical ID of the Microsoft Internet Information Services (IIS) site hosting StoreFront, which can be obtained from the Internet Information Services (IIS) Manager console. Replace sitepath with the relative path at which the site should be created in IIS, for example, /Citrix/DesktopAppliance. Note that Desktop Appliance site URLs are case sensitive.

   Indicate whether StoreFront is configured for HTTPS by setting -UseHttps to the appropriate value.

To specify the absolute URL of the store service used by the Desktop Appliance Connector site, use StoreUrl storeaddress. This value is displayed for the Store summary in the administration console.

By default, when a user logs on to a Desktop Appliance site, the first desktop available to the user starts automatically. To configure your new Desktop Appliance site to enable users to choose between multiple desktops, if available, set -EnableMultiDesktop to $True.

Explicit authentication is enabled by default for new sites. You can disable explicit authentication by setting the -
EnableExplicit argument to $False. Enable smart card authentication by setting -EnableSmartCard to $True. To enable pass-through with smart card authentication, you must set both -EnableSmartCard and -EnableEmbeddedSmartCardSSO to $True. If you enable explicit and either smart card or pass-through with smart card authentication, users are initially prompted to log on with a smart card, but can fall back to explicit authentication if they experience any issues with their smart cards.

The optional arguments configure settings that can also be modified after the Desktop Appliance site has been created by editing the site configuration file.

**Example:**

Create a Desktop Appliance Connector site at virtual path /Citrix/DesktopAppliance1 in the default IIS web site.

```
Install-DSDesktopAppliance  
-FriendlyName DesktopAppliance1  
-SiteId 1  
-VirtualPath /Citrix/DesktopAppliance1  
-UseHttps $false  
-StoreUrl https://servername/Citrix/Store  
-EnableMultiDesktop $true  
-EnableExplicit $true  
-EnableSmartCard $true  
-EnableEmbeddedSmartCardSSO $false
```

3. To remove an existing Desktop Appliance site, type the following command.

```
Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
```

Where iisid is the numerical ID of the IIS site hosting StoreFront and sitepath is the relative path of the Desktop Appliance site in IIS, for example, /Citrix/DesktopAppliance.

4. To list the Desktop Appliance sites currently available from your StoreFront deployment, type the following command.

```
Get-DSDesktopAppliancesSummary
```

Desktop Appliance sites support explicit, smart card, and pass-through with smart card authentication. Explicit authentication is enabled by default. If you enable explicit and either smart card or pass-through with smart card authentication, the default behavior initially prompts users to log on with a smart card. Users who experience issues with their smart cards are given the option of entering explicit credentials. If you configure IIS to require client certificates for HTTPS connections to all StoreFront URLs, users cannot fall back to explicit authentication if they cannot use their smart cards. To configure the authentication methods for a Desktop Appliance site, you edit the site configuration file.

1. Use a text editor to open the web.config file for the Desktop Appliance site, which is typically located in the C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance directory, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.
   `<explicitForms enabled="true" />`
3. Change the value of the `enabled` attribute to `false` to disable explicit authentication for the site.
4. Locate the following element in the file.
   `<certificate enabled="false" useEmbeddedSmartcardSso="false" embeddedSmartcardSsoPinTimeout="00:00:20" />`
5. Set the value of the `enabled` attribute to `true` to enable smart card authentication. To enable pass-through with smart card authentication, you must also set the value of the `useEmbeddedSmartcardSso` attribute to `true`. Use the `embeddedSmartcardSsoPinTimeout` attribute to set the time in hours, minutes, and seconds for which the PIN entry screen is displayed before it times out. When the PIN entry screen times out, users are returned to the logon screen and must remove and reinsert their smart cards to access the PIN entry screen again. The time-out period is set to 20 seconds by default.

By default, when a user logs on to a Desktop Appliance site, the first desktop (in alphabetical order) available to the user in the store for which the site is configured starts automatically. If you provide users with access to multiple desktops in a store, you can configure the Desktop Appliance site to display the available desktops so users can choose which one to access. To change these settings, you edit the site configuration file.

1. Use a text editor to open the web.config file for the Desktop Appliance site, which is typically located in the `C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance` directory, where `storename` is the name specified for the store when it was created.
2. Locate the following element in the file.
   `<resources showMultiDesktop="false" />`
3. Change the value of the `showMultiDesktop` attribute to `true` to enable users to see and select from all the desktops available to them in the store when they log on to the Desktop Appliance site.
Configure authentication for XenApp Services URLs

Sep 29, 2014

XenApp Services URLs enable 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, to access stores. When you create a new store, the XenApp Services URL 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.

XenApp Services URLs support explicit, domain pass-through, and pass-through with smart card authentication. Explicit authentication is enabled by default. You can change the authentication method, but only one authentication method can be configured for each XenApp Services URL. To enable multiple authentication methods, create separate stores, each with a XenApp Services URL, for each authentication method. To change the authentication method for a XenApp Services URL, you run a Windows PowerShell script.

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.

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.

Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, enter one of the following commands to configure the user authentication method for users accessing the store through the XenApp Services URL.

```
& "installationlocation\Scripts\EnablePnaForStore.ps1" –SiteId iisid –ResourcesVirtualPath storepath –LogonMethod {prompt | sson | smartcard_sson | smartcard_prompt}
```

Where installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\. For iisid, specify the numerical ID of the Microsoft Internet Information Services (IIS) site hosting StoreFront, which can be obtained from the Internet Information Services (IIS) Manager console. Replace storepath with the relative path to the store in IIS, for example, /Citrix/Store. To enable explicit authentication, set the -LogonMethod argument to prompt. For domain pass-through, use sson and for pass-through with smart card authentication, set the argument to smartcard_sson.

**XenApp Services Support smart card authentication method**

```
& "installationlocation\Scripts\EnablePnaForStore.ps1" –SiteId iisid –ResourcesVirtualPath storepath –LogonMethod smartcard_prompt
```

The installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\.

Replace storepath with the relative path to the store in IIS, for example, /Citrix/Store.

For domain pass-through with smart card authentication, set the argument to smartcard_prompt.
Create a single FQDN to access a store internally and externally

Jan 15, 2015

Note: To use this feature with native desktop receivers, the following versions are required.
- Windows Receiver 4.2
- MAC Receiver 11.9

You can provide access to resources from within your corporate network and from the Internet through a NetScaler 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.

Citrix Receiver 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 Receiver. 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.

The shared FQDN resolves either to an external firewall router interface IP or NetScaler Gateway vServer 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 NetScaler 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.
NetScaler Gateway vServer 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 NetScaler 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)
accounts.example.com (mandatory)
storefrontserver1.example.com (optional)
storefrontserver2.example.com (optional)

Sign the NetScaler Gateway vServer 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 NetScaler Gateway vServer 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 NetScaler Gateway vServer.

- 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 NetScaler Gateway vServer 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.
- 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 NetScaler Gateway**

WinSCP is a useful and free third party tool to move files from a Windows machine to a NetScaler Gateway file system. Copy certificates for import to the /nsconfig/ssl/ folder within the NetScaler Gateway file system. You can use the OpenSSL tools on the NetScaler 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 NetScaler Gateway.

1. Copy the PFX file into /nsconfig/ssl on the NetScaler Gateway appliance or VPX.
2. Open the NetScaler Gateway command line interface.
3. To switch to the FreeBSD shell, type Shell to exit the NetScaler 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 NetScaler Gateway command line interface, type Exit.

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

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 NetScaler Gateway vServer properties page. Universal Licenses are required for every concurrent user who accesses remote resources.

**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.

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.

Receiver for Web profile

Note: cVPN mode is not supported with StoreFront (3 pane view) with Receiver for Web.

If you use ICA Proxy, enable basic mode on the NetScaler Gateway vServer properties page. Only a Netscaler platform license is required.
### Receiver profile

[Image of Configure NetScaler Gateway Session Profile for Receiver ICAProxy]

### Receiver for Web profile

[Image of Configure NetScaler Gateway Session Profile for WebReceiver ICAProxy]
The same shared FQDN that resolves to the NetScaler Gateway vServer 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 NetScaler Gateway vServer that you created earlier or use the same certificate bound to the NetScaler Gateway vServer.
3. Add the accounts 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 Netscaler Gateway Session Profile in the earlier procedure - Native Receiver Gateway session policy and profile.
4. Ensure that the private key is exportable so the certificate can be transferred to another server or to multiple StoreFront server group nodes.

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 Netscaler LB vServer, import the certificate there instead.
8. Create an HTTPS binding in IIS on the StoreFront server and bind the imported SSL certificate to it.

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
Configure the Gateway on the StoreFront server: storefront.example.com

1. Type the shared FQDN into the gateway configuration text box under Netscaler Gateway URL.
2. Type the callback FQDN into the gateway configuration dialogue under Callback URL.

   ![Gateway Configuration Screenshot]

3. Type a list of Secure Ticket Authority (STA) servers that matches the list of delivery controllers already configured within the store node.
4. Enable remote access for the store.
5. 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 NetScaler Gateway vServer (storefront.example.com). DO NOT use the shared FQDN, as this creates a situation where both the internal and external beacons are identical.

   ![Internal Beacon Configuration Screenshot]

6. Note that if you want to support discovery using FQDNs, follow these 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 the authentication web.config file. Only the first entry in the file for the Authentication Token Producer requires you to add an additional <allowedAudience>.

7. Perform a search for the <allowedAudiences> string. Locate the following entry below and add the line shown in bold, save, and close the web.config file.

   ```xml
   <allowedAudiences>
   <service id="abd6f54b-7d1c-4a1b-a8d7-14b04e6c8c64" displayName="Authentication Token Producer">
   ```

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved.
8. In C:\inetpub\wwwroot\Citrix\Roaming\web.config. Locate the following entry below and add the line shown in bold, save, and close the web.config file.

```xml
<allowedAudiences>
  <add name="https-storefront.example.com" audience="https://storefront.example.com/" />
  <add name="https-accounts.example.com" audience="https://accounts.example.com/" />
</allowedAudiences>
```

Alternatively, it is possible to export the native receiver .CR provisioning file for the store. This eliminates the need for First Time Use configuration of native Receivers. Distribute this file to all Windows and MAC Receiver clients.

![Export Provisioning File](image)

If a Receiver is installed on the client, the .CR file type is recognized and double clicking on the provisioning file triggers it to be automatically imported.
Configure NetScaler and StoreFront for Delegated Forms Authentication (DFA)

Sep 25, 2014

Extensible authentication provides a single customization point for extension of NetScaler'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 NetScaler 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, NetScaler delegates authentication to StoreFront, which then interacts with a third party authentication server or service.

- To ensure communication between NetScaler 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 Netscaler has the issuer of StoreFront's server certificate as a trusted certificate authority when HTTPS is configured in StoreFront.

- Install a third party authentication plugin on all the nodes prior to joining them up together.
- Configure all the Delegated Forms Authentication related settings on one node and propagate the changes to the others. See the "Enable Delegated Forms Authentication"

Because there is no GUI to setup 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:\Program Files\Citrix\Receiver StoreFront\Scripts> 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-bbba-c08b2682c1bc
ParentInstanceId : 8dd182c7-9f70-466c-ad4c-27a5980f716c
RootInstance : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId : 860e9401-39c8-4f2c-920d-34251102b840
Data : {}
ReadOnlyData : {
    [Name, DelegatedFormsServer],
    [Cmdlet, Add-DSWebFeature],
    [Snapin, Citrix.DeliveryServices.Web.Commands],
    [Tenant, 860e9401-39c8-4f2c-920d-34251102b840]
}
ParameterData : {
    [FeatureClassName, e1eb3668-9c1c-4ad8-bbba-c08b2682c1bc],
    [ParentInstanceId, 8dd182c7-9f70-466c-ad4c-27a5980f716c],
    [TenantId, 860e9401-39c8-4f2c-920d-34251102b840]
}
AdditionalInstanceDependencies : {
    b1e48ef0-b9e5-4697-af9b-0910062aa2a3
}
IsDeployed : True
```

2. Add Citrix Trusted Client. Configure the shared secret key (passphrase) between StoreFront and Netscaler. Your passphrase and client ID must be identical to what you configured in NetScaler.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
```

3. Set the Delegated Forms Authentication conversation factory to route all the traffic to the custom form. To find the conversation factory, look for ConversationFactory in C:\inetpub\wwwroot\Citrix\Authentication\web.config. This is an example of what you might see.

```
<example connectorURL="http://Example.connector.url:8080/adapters-sf-aaconnector-webapp" >
  <routeTable order="1000" >
    <routes>
      <route name="StartExampleAuthentication" url="Example-Bridge-Forms/Start" >
        <defaults>
          <add param="controller" value="ExplicitFormsAuthentication" />
        </defaults>
      </route>
    </routes>
  </routeTable>
```

<add param="action" value="AuthenticateStart" />
<add param="postbackAction" value="Authenticate" />
<add param="cancelAction" value="CancelAuthenticate" />
<add param="conversationFactory" value="ExampleBridgeAuthentication" />
<add param="changePasswordAction" value="StartChangePassword" />
<add param="changePasswordController" value="ChangePassword" />
<add param="protocol" value="CustomForms" />
</defaults>
</route>

4. In PowerShell, set the Delegated Forms Authentication conversation factory. In this example, to ExampleBridgeAuthentication.

    PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication

PowerShell's arguments are not case-sensitive: -ConversationFactory is identical to –conversationfactory.

Before you uninstall StoreFront, uninstall any third party authentication plugin, as it will impact the functionality of StoreFront.
Configure Resource Filtering

This topic explains how to filter enumeration resources based on resource type and keywords. You can use this type of filtering in conjunction 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 Store Customization SDK.

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 the filter using PowerShell cmdlets defined within the StoresModule. Use the following PowerShell snippet to load the required modules:

```powershell
$dsInstallProp = Get-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

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.

Use this to filter resources based on keywords, such as resources derived from XenApp, XenDesktop or VDI-in-a-Box. 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
This command will set filtering to exclude workflow resources from enumeration:

```powershell
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

This example will set allowed resource types to applications only:

```powershell
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -IncludeTypes @("Applications")
```
Configure special folder redirection

Jul 22, 2014

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.

Configure special folder redirection using PowerShell.

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.

Command

Set-DSClientSettings

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteId</td>
<td>long</td>
<td>IIS site ID of the store.</td>
</tr>
<tr>
<td>VirtualPath</td>
<td>string</td>
<td>Virtual path of the store.</td>
</tr>
<tr>
<td>SpecialFolderRedirectionAllowed</td>
<td>bool</td>
<td>true to enable special folder redirection; false to disable.</td>
</tr>
</tbody>
</table>

Example1:

Enable special folder redirection for a store named Store.

Set-DSClientSettings -SiteId 1 -VirtualPath /Citrix/Store - SpecialFolderRedirectionAllowed $true

Example2:

Disable special folder redirection for a store named Store.

Set-DSClientSettings -SiteId 1 -VirtualPath /Citrix/Store - SpecialFolderRedirectionAllowed $false
Manage subscription data

Dec 09, 2014

Manage subscription data for a store using PowerShell cmdlets.

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.

Export subscription data

You can create a snapshot of a store’s subscription data using the following PowerShell cmdlets to create a subscription data file:

```
Export-DSStoreSubscriptions -StoreName StoreName -FilePath DataFile
```

When managing a multiple-server deployment, you can run these PowerShell cmdlets on any server within the StoreFront server group.

Restore subscription data

You can restore a store’s subscription data to a previously saved snapshot using the following PowerShell cmdlets:

```
Restore-DSStoreSubscriptions -StoreName StoreName -FilePath DataFile
```

This command restores the subscription data to the state when the export data file was produced, and it removes any existing subscriptions before adding the subscription data found in the data file.

When managing a multiple-server deployment, you can run these PowerShell cmdlets on any server within the StoreFront server group.

Import subscription data

You can update a store’s subscription data from a previously exported data file using the following PowerShell cmdlets:

```
Import-DSStoreSubscriptions -StoreName StoreName -FilePath FilePath
```

This command allows subscription data to be transferred from one store to another, and it retains existing subscriptions before adding/updating subscription data from the imported data file.

When managing a multiple-server deployment, you can run these PowerShell cmdlets on any server within the StoreFront server group.

Purge subscription data for a store

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

1. Stop the Citrix Subscriptions Store service on the StoreFront server.
2. Locate subscription store database folder on each StoreFront server in the new location.
   C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
3. Delete the contents of this folder, but do not delete the folder.
4. Restart the Citrix Subscriptions Store service on all StoreFront servers in the deployment.

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 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>` and `<property-value>` values. These represent properties associated with the subscription by a StoreFront client (typically a Citrix Receiver). A property with multiple values that is represented by multiple name/value pairs with the same name (for example, "... MyProp A MyProp B ....") represents the property MyProp with values A, B).

Example:

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

Size of subscription data on the Storefront server's disk

<table>
<thead>
<tr>
<th>No. of Records</th>
<th>Size (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>6.02</td>
</tr>
<tr>
<td>1000</td>
<td>7.02</td>
</tr>
<tr>
<td>10000</td>
<td>40.00</td>
</tr>
<tr>
<td>100000</td>
<td>219.00</td>
</tr>
<tr>
<td>200000</td>
<td>358.00</td>
</tr>
<tr>
<td>500000</td>
<td>784.00</td>
</tr>
<tr>
<td>800000</td>
<td>1213.02</td>
</tr>
<tr>
<td>1000000</td>
<td>1497.15</td>
</tr>
<tr>
<td>1300000</td>
<td>1919.15</td>
</tr>
<tr>
<td>1500000</td>
<td>2205.15</td>
</tr>
<tr>
<td>1700000</td>
<td>2487.15</td>
</tr>
<tr>
<td>2000000</td>
<td>2915.15</td>
</tr>
</tbody>
</table>

Size of import and export .txt files
<table>
<thead>
<tr>
<th>No of Records</th>
<th>Size MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>1000</td>
<td>0.13</td>
</tr>
<tr>
<td>10000</td>
<td>1.30</td>
</tr>
<tr>
<td>100000</td>
<td>12.80</td>
</tr>
<tr>
<td>200000</td>
<td>25.60</td>
</tr>
<tr>
<td>500000</td>
<td>64.30</td>
</tr>
<tr>
<td>800000</td>
<td>102.00</td>
</tr>
<tr>
<td>1000000</td>
<td>128.00</td>
</tr>
<tr>
<td>1300000</td>
<td>166.00</td>
</tr>
<tr>
<td>1500000</td>
<td>192.00</td>
</tr>
<tr>
<td>1700000</td>
<td>218.00</td>
</tr>
<tr>
<td>2000000</td>
<td>256.00</td>
</tr>
</tbody>
</table>
Secure

Oct 21, 2013
This topic highlights areas that may have an impact on system security when deploying and configuring StoreFront.

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

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.

To enable email-based account discovery for users installing Citrix Receiver 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 Receiver 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 Receiver 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.

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 XenApp servers. The SSL Relay is a default component of XenApp that performs host authentication and data encryption.

Citrix recommends securing communications between StoreFront and users' devices using NetScaler 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.

Note: SSL 2.0 is enabled by default in IIS. As this protocol is now deprecated, Citrix recommends disabling SSL 2.0 on StoreFront servers. For more information about disabling protocols in IIS, see http://support.microsoft.com/kb/187498.
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.

StoreFront provides the option to digitally sign ICA files using a specified certificate on the server so that versions of Citrix Receiver 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.

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.
Troubleshoot

Aug 27, 2014

When StoreFront is installed or uninstalled, the following log files are created by the StoreFront installer in the C:\Windows\Temp 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.

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.

Caution: 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 before opening the StoreFront console.

1. Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, type the following commands and restart the server to enable tracing.

   ```powershell
   Set-DSTraceLevel -All -TraceLevel Verbose
   ``

   Allowed values for -TraceLevel are, in increasing levels of tracing detail: Off, Error, Warning, Info, Verbose.

   StoreFront automatically captures Error trace messages. Due to the large amount of data that can potentially be generated, tracing may significantly impact the performance of StoreFront, so it is recommended that the Info or Verbose levels are not used unless specifically required for troubleshooting.

2. To disable tracing, type the following commands and restart the server.

   ```powershell
   Set-DSTraceLevel -All -TraceLevel Off
   ``

   When tracing is enabled, tracing information is written in the \Admin\Trace\ directory of the StoreFront installation located at C:\Program Files\Citrix\Receiver\StoreFront\.