StoreFront 2.0

2013-06-30 15:47:53 UTC

Contents

StoreFront 2.0

Citrix StoreFront 2.0 enables you to create enterprise app stores that aggregate resources from XenDesktop, XenApp, XenMobile App Controller, and VDI-in-a-Box in one place. The stores you create provide your users with self-service access to their Windows desktops and applications, mobile applications, external software-as-a-service (SaaS) applications, and internal web applications through a single portal from all their devices. You get a single place to manage the provisioning of corporate desktops and applications to your users. Consolidating the delivery of resources through StoreFront means you no longer need to manage multiple delivery mechanisms for different applications or provide support for manual installations and updates.

The topics in this section provide information about deploying, configuring, and managing StoreFront 2.0. Readers are assumed to be familiar with Citrix Receiver, XenDesktop, XenApp, XenMobile App Controller, and VDI-in-a-Box.

About StoreFront	Plan your StoreFront deployment
Known issues in StoreFront 2.0	To install and set up StoreFront
System requirements for StoreFront 2.0	Manage your StoreFront deployment

About StoreFront

StoreFront is an integral component of any XenDesktop, XenApp, XenMobile, or VDI-in-a-Box implementation, authenticating users to Microsoft Active Directory and managing the delivery of desktops and applications from your servers in the datacenter to users' devices. Users access StoreFront stores through Citrix Receiver or by browsing to a Receiver for Web or Desktop Appliance site, which enable users to access stores through a webpage. Where none of these access methods can be used, such as on devices with older Citrix clients that cannot be upgraded, users can connect to stores through XenApp Services URLs. StoreFront keeps a record of each user's applications and automatically updates their devices, ensuring that users have a consistent experience as they roam between their smart phones, tablets, laptops, and desktop computers.

What's new

Separate database no longer required. The requirement for a separate database has been removed. Users' application subscription data are stored locally and automatically replicated between StoreFront servers. For more information, see Plan your StoreFront deployment.

High availability and multi-site configuration. To enable load balancing and failover between the deployments providing the desktops and applications, you can define groupings and hierarchies, including specific backup deployments. You can restrict user access to specific resources by mapping deployments to Active Directory user groups. For more information, see StoreFront high availability and multi-site configuration.

Smart card authentication. StoreFront supports smart card authentication through both Receiver for Windows and NetScaler Gateway. Smart card authentication from desktop appliances and repurposed PCs through Desktop Appliance sites and XenApp Services URLs is also supported. For more information, see Use smart cards with StoreFront.

Receiver for HTML5 integration. You can configure Receiver for Web sites to enable users who cannot install Citrix Receiver to access their desktops and applications directly within HTML5-compatible web browsers. For more information, see Receiver for Web sites.

Desktop Appliance sites. You can enable users to access their desktops from non-domain-joined desktop appliances. The web browser on the appliance is configured to access the Desktop Appliance site for a store in full-screen mode at startup. For more information, see Desktop Appliance sites.

Receiver for Web site shortcuts. You can embed on your websites links to desktops and applications available through Receiver for Web sites. For more information, see Receiver for Web sites.

XenMobile App Controller workflow integration. Receiver for Web site users can subscribe to applications to which you are managing access with App Controller user account management. For more information about App Controller user account management, see Configuring Applications for User Account Management.

Receiver for Web site user change password. You can enable Receiver for Web site users to change their Active Directory domain passwords and configure notifications for users whose passwords are about to expire. For more information, see Optimize the user experience.

Fast Connect support. StoreFront supports pass-through authentication with proximity cards through Fast Connect-compatible third-party products to XenApp Services URLs. For more information, see XenApp Services URLs.

IPv6 support. StoreFront supports communications with both servers and clients on IPv6 networks and on hybrid dual-stack IPv4/IPv6 networks.

Other features

Citrix Receiver integration. Citrix Receiver provides users with intuitive, self-service access to your StoreFront stores from any device, anywhere. For more information, see Citrix Receiver.

Email-based account discovery. You can enable users who install Citrix Receiver on a device for the first time to set up their accounts by entering their email addresses. For more information, see Configure email-based account discovery.

One-click configuration of Citrix Receiver. You can configure Citrix Receiver for your users by making provisioning files available. For more information, see To export store provisioning files for users.

Automatically provisioned applications. You can automatically subscribe all users to a core set of applications. For more information, see Optimize the user experience.

Application synchronization. Subscribed applications follow users from device to device. Users do not need to resubscribe to their applications each time they use a different device, ensuring that they enjoy a consistent experience across all their devices. For more information, see Plan your StoreFront deployment.

Receiver for Web sites. In addition to accessing StoreFront stores within Citrix Receiver, users can also access stores through web pages. For more information, see Receiver for Web sites.

Citrix Receiver detection and deployment. Receiver for Web sites prompt Windows and Mac OS X users who do not have Citrix Receiver installed to download the appropriate version from the Citrix website. For more information, see Receiver for Web sites.

NetScaler Gateway support. StoreFront integrates with NetScaler Gateway to secure connections from remote users over public networks. Both connections through the NetScaler Gateway Plug-in and clientless access are supported. You can use SmartAccess to control user access to resources on the basis of session policies. For more information, see User authentication.

Pass-through authentication. StoreFront supports pass-through of domain and smart card credentials from users' devices, and pass-through authentication from NetScaler Gateway. For more information, see User authentication.

Secure user connections. You can configure StoreFront to use HTTPS to secure communications with users' devices. For more information, see Secure your StoreFront

deployment.

ICA file signing. StoreFront can digitally sign ICA files so that versions of Citrix Receiver that support this feature can verify that the file originates from a trusted source. For more information, see Secure your StoreFront deployment.

Workspace control. You can configure applications to follow users as they move between devices so that they do not have to restart their applications on each device. For more information, see Optimize the user experience.

Legacy client support. When you create a new store, access for older clients that support Web Interface XenApp Services sites is enabled by default. For more information, see XenApp Services URLs.

Centralized server management. You can manage a group of StoreFront servers using the Citrix StoreFront management console on the primary server. For more information, see Configure server groups.

Known issues in StoreFront 2.0

The following is a list of known issues in this release. **Read it carefully before installing the product**.

StoreFront initial configuration cannot be completed when the Windows Firewall service is not running

When either creating a new deployment or joining an existing server group for a newly installed StoreFront server on which the Windows Firewall service is not running, the operation fails. To resolve this issue, start the Windows Firewall service and try again. Once initial configuration is complete, the Windows Firewall service can be stopped again, if required. [#401143]

StoreFront cannot be upgraded when the Windows Firewall service is not running

When upgrading from StoreFront 1.2 to StoreFront 2.0 for a server on which the Windows Firewall service is not running, the installation fails with the error message "An error occurred during installation. Please ensure that all the required prerequisites have been installed and run the installer again." To resolve this issue, start the Windows Firewall service and, in the Windows Firewall with Advanced Security console, delete the Citrix Credential Wallet Replication inbound rule, if it exists. Then, run the StoreFront 2.0 installation file to complete the upgrade. Once the upgrade is complete, the Windows Firewall service can be stopped again, if required. [#400876]

Pending updates might not complete during upgrades to Receiver for Windows 3.4 from citrix.com

During upgrades of Receiver for Windows 3.4 from the Citrix website, pending updates, such as to plug-ins, might not be completed. To work around this issue, Receiver for Windows 3.4 must be upgraded manually. [#396558]

Upgrading from Receiver Storefront 1.1 removes the existing configuration

Upgrading Receiver Storefront 1.1 to StoreFront 2.0 directly is not supported. However, if you attempt to do so, your existing Receiver Storefront configuration is removed and cannot be recovered. To avoid this issue, first upgrade Receiver Storefront 1.1 to StoreFront 1.2 before upgrading to StoreFront 2.0. [#395810]

Upgrades to Receiver for Windows 3.3 from citrix.com cannot be completed

When upgrading Receiver for Windows 3.3 from the Citrix website, users receive the error message "Cannot complete setup". To work around this issue, Receiver for Windows 3.3 must be upgraded manually. [#393294]

Users cannot access resources after disabling Pass-through from NetScaler Gateway authentication

If you disable the Pass-through from NetScaler Gateway authentication method, users cannot access their resources through NetScaler Gateway even if the store is configured for remote access. Instead, users receive the error message "Unable to launch your application.

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

Users running Internet Explorer 8 might 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]

Receiver for Web site Logon screen might not be localized for some users

When accessing Receiver for Web sites through Access Gateway 5.0.4, the Logon screen appears in English for Traditional Chinese, Korean, and Russian users. When accessing Receiver for Web sites through Access Gateway 9.3, Enterprise Edition, the Logon screen appears in English for Simplified Chinese, Traditional Chinese, Korean, and Russian users. [#267899]

System requirements for StoreFront 2.0

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

- Windows Server 2012 Datacenter and Standard editions
- Windows Server 2008 R2 Service Pack 1 Enterprise and Standard editions

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. All other hardware specifications must meet the minimum requirements for the installed operating system.

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.

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. In addition, 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.

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

Infrastructure requirements

Citrix has tested and provides support for StoreFront when used with the following Citrix product versions.

Citrix server requirements

StoreFront stores aggregate desktops and applications from the following products.

- XenDesktop
  - XenDesktop 7
  - XenDesktop 5.6 Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
- XenApp
  - 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
- XenMobile App Controller
    - AppController 2.6
    - AppController 2.5
    - AppController 2.0
    - AppController 1.1
    - AppController 1.0
- 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 10.1
- Access Gateway 10 Build 69.4 (the version number is displayed at the top of the configuration utility)
- Access Gateway 9.3, Enterprise Edition
- Access Gateway 5.0.4

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
- 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
  - XenDesktop 5.6
  - XenDesktop 5.5
- XenApp
  - 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

Merchandising Server requirements

If you plan to configure Merchandising Server to use the authentication service to identify users when delivering Citrix Receiver configurations, StoreFront can be used with the following versions of Merchandising Server.

- Merchandising Server 2.2
- Merchandising Server 2.1

For more information, see Configuring Authentication.

User device requirements

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 clientless access.

- Citrix Receiver for Windows 8/RT 1.3
- Citrix Receiver for Windows 4.0
- Citrix Receiver for Windows 3.4
- Citrix Receiver for Mac 11.8
- Citrix Receiver for Mac 11.7
- Citrix Receiver for iOS 5.7
- Citrix Receiver for iOS 5.6
- Citrix Receiver for Android 3.3

- Citrix Receiver for Android 3.2
- Citrix Receiver for Linux 12.1

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.

Client	Operating system	Browser

Citrix Receiver for Windows 4.0 Citrix Receiver for Windows 3.4	Windows 8 (32-bit and 64-bit editions)	Internet Explorer 10 (32-bit mode) Google Chrome 27 Google Chrome 26 Mozilla Firefox 21 Mozilla Firefox 20
	Windows 7 Service Pack 1 (32-bit and 64-bit editions)	Internet Explorer 9 (32-bit mode) Internet Explorer 8 (32-bit mode) Google Chrome 27 Google Chrome 26 Mozilla Firefox 21 Mozilla Firefox 20
	Windows Embedded Standard 7 Service Pack 1	Internet Explorer 9 (32-bit mode) Internet Explorer 8 (32-bit mode)
	Windows Vista Service Pack 2 (32-bit and 64-bit editions) Windows XP Professional x64 Edition Service Pack 2 Windows XP Professional Service Pack 3	Internet Explorer 8 (32-bit mode) Google Chrome 27 Google Chrome 26 Mozilla Firefox 21 Mozilla Firefox 20
	Windows Embedded Standard 2009	Internet Explorer 8 (32-bit mode)

Citrix Receiver for Mac 11.8 Citrix Receiver for Mac 11.7	Mac OS X 10.8 Mountain Lion	Safari 6 Google Chrome 27 Mozilla Firefox 21
	Mac OS X 10.7 Lion	Safari 5.1 Google Chrome 27 Mozilla Firefox 21
	Mac OS X 10.6 Snow Leopard	Safari 5.0 Google Chrome 27 Mozilla Firefox 21
Citrix Receiver for Linux 12.1	SuSE Linux Enterprise Desktop 12.1 Ubuntu 12.04 (32-bit)	Google Chrome 27 Mozilla Firefox 21

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 10 (HTTP connections only)
  - Safari 6
  - Google Chrome 27
  - Mozilla Firefox 21
- Operating systems
  - Windows RT
  - 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 XP Professional x64 Edition Service Pack 2

- Windows XP Professional Service Pack 3
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.7 Lion
- Mac OS X 10.6 Snow Leopard
- Google Chrome OS 27

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.

Client	Operating system	Browser
Citrix Receiver for Windows 4.0 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	Internet Explorer 9 (32-bit mode) Internet Explorer 8 (32-bit mode)
	Windows XP Professional x64 Edition Service Pack 2 Windows XP Professional Service Pack 3	Internet Explorer 8 (32-bit mode)
Citrix Receiver for Windows (Enterprise) 3.4	Windows 7 Service Pack 1 (32-bit and 64-bit editions) Windows Embedded Standard 7 Service Pack 1	Internet Explorer 9 (32-bit mode) Internet Explorer 8 (32-bit mode)
	Windows XP Professional x64 Edition Service Pack 2 Windows XP Professional Service Pack 3	Internet Explorer 8 (32-bit mode)
Citrix Receiver for Linux 12.1	Ubuntu 12.04 (32-bit)	Mozilla Firefox 21

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, the following older clients that do not support other access methods can be used 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.

Client	Connect from internal network	Connect through NetScaler Gateway
Online Plug-in for Windows 12.3	Yes	Yes
Online Plug-in for Macintosh 11.2	Yes	Yes
Citrix Receiver for Linux 12.0	Yes	No

Smart card requirements

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.

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

Citrix Receiver requirements

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 4.0 can be used.

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)
- Access Gateway 9.3, Enterprise Edition

Plan your StoreFront deployment

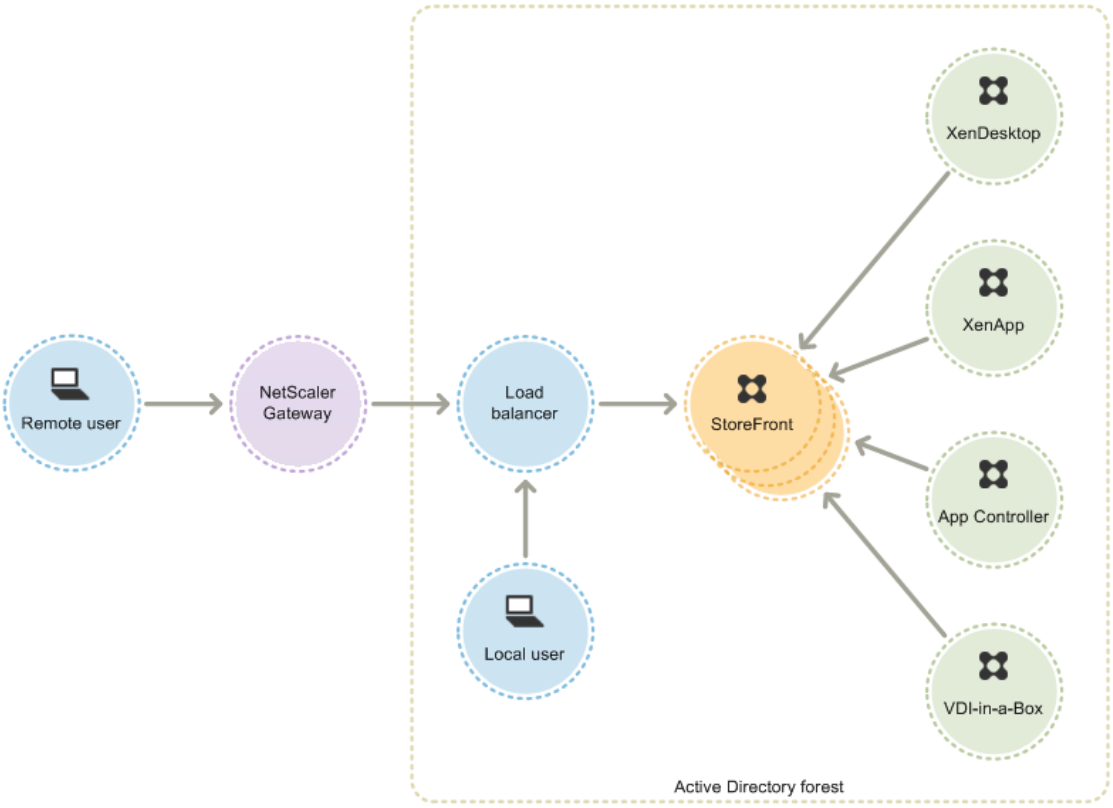
StoreFront employs Microsoft .NET technology running on Microsoft Internet Information Services (IIS) to provide enterprise app stores that aggregate resources and make them available to users. StoreFront integrates with your XenDesktop, XenApp, XenMobile App Controller, and VDI-in-a-Box deployments, 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, App Controller, 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.

Important: 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 providing the authentication service and associated stores is configured for HTTPS before the authentication service is created. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.

The figure shows a typical StoreFront deployment.



None

StoreFront can be configured either on a single server or as a multiple server deployment. 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.

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.

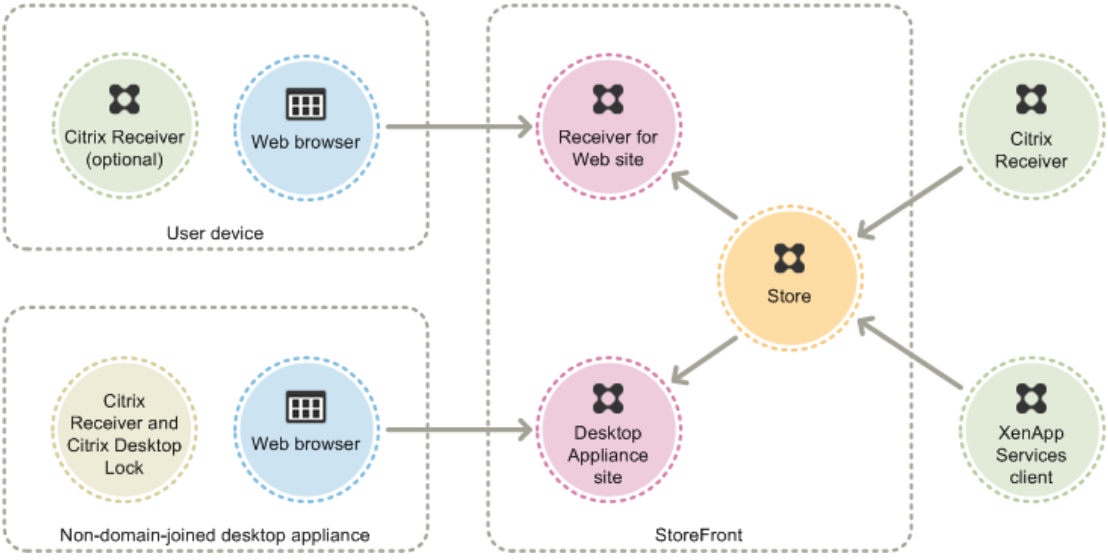
If you plan to enable access to StoreFront from outside the corporate network, NetScaler Gateway is required to provide secure connections for remote users. Deploy NetScaler Gateway outside the corporate network, with firewalls separating NetScaler Gateway from both the public and internal networks.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

User access options

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.



None

Citrix Receiver

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 2.0.

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 To 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.

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. For more information, see Configure email-based account discovery.

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 To 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 or Access Gateway 5.0, users cannot set up accounts manually and must use one of the alternative methods above. For more information, see the Citrix Receiver documentation.

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. For more information about creating your own Citrix Receiver download page, see http://www.citrix.com/downloads/citrix-receiver/administration/citrix-receiver-download-page-template.ht ml.

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 either a certificate with a Subject or Subject Alternative Name entry of **discoverReceiver.*domain***, or a wildcard certificate for the domain containing your users' email accounts. 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.

To add a SRV record to your DNS server

1. On the Windows Start screen, 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.

   Note: The FQDN for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN for StoreFront and the NetScaler Gateway virtual server is not supported. To use email-based account discovery, Citrix Receiver requires that the StoreFront FQDN is a unique address that is only resolvable from user devices connected to the internal network.
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

You can enable Receiver for HTML5 on your Receiver for Web sites so that users who cannot install Citrix Receiver can still access 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, but 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 port specified in the policy for use by Receiver for HTML5. 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 To 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 websites 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. For more information about customizing the appearance of Receiver for Web sites, see http://support.citrix.com/article/CTX134791.

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.
- Receiver for Web sites do not support domain pass-through or smart card authentication.
- Receiver for Web sites cannot initiate Secure Sockets Layer (SSL) virtual private network (VPN) connections. Users logging on through NetScaler Gateway without a VPN connection cannot access web applications for which App Controller requires that such a connection is used.
- Subscribed applications are not available on the Windows Start screen when accessing a store through a 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. Citrix Online products must be delivered with App Controller or made available as hosted applications to enable access through Receiver for Web sites.
- Receiver for HTML5 can only be used with Internet Explorer over HTTP connections.
- 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, 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 To 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

User authentication

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 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.

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 and Desktop Appliance sites do 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.

Smart card

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, Desktop Appliance sites, and XenApp Services URLs. Receiver for Web sites do not support smart card authentication. For more information about configuring StoreFront for use with smart cards, see Use smart cards with StoreFront.

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 To 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.
- **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 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. For more information about configuring NetScaler Gateway as a remote proxy, see Creating and Applying Web and File Share Links.

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

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 only. 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

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.

Use smart cards with StoreFront

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.

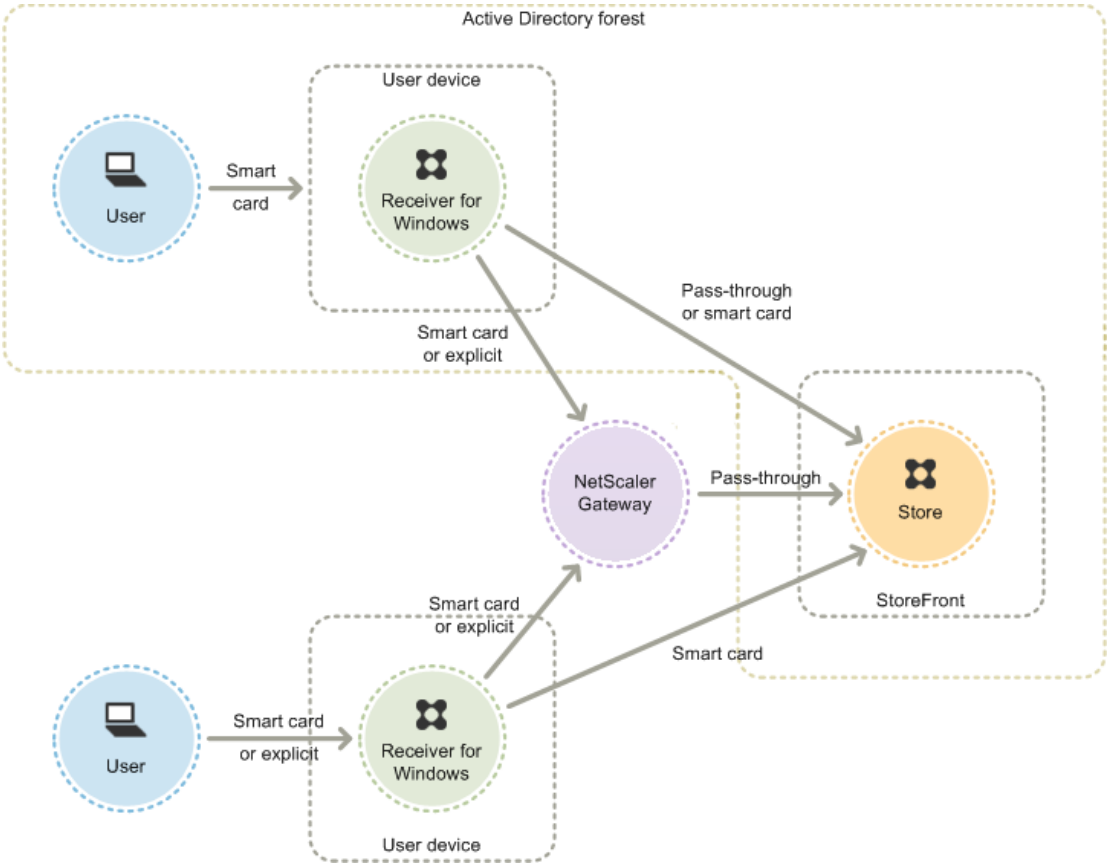
You can use smart cards for user authentication through StoreFront to desktops and applications provided by XenDesktop, XenApp. Smart card users logging on to StoreFront can also access applications provided by App Controller. However, users must authenticate again to access App Controller web applications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

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

Users of domain-joined devices log on to their devices using their smart cards and PINs. If Receiver for Windows is configured for pass-through authentication, users are silently authenticated to StoreFront and also when they access their desktops and applications. Users are not prompted for their PINs again. Without pass-through authentication, users are prompted to log on when they access their devices, when Receiver for Windows connects to Storefront, and when they access their desktops and applications.

In the case of non-domain-joined devices, users log on to their devices and then authenticate to Receiver for Windows using their smart cards and PINs. You can configure smart card authentication to the user devices as well, but this is not required because Receiver for Windows does not capture the device logon credentials. Users are prompted to authenticate again when Receiver for Windows connects to StoreFront and must also enter their PINs when they access their desktops and applications.

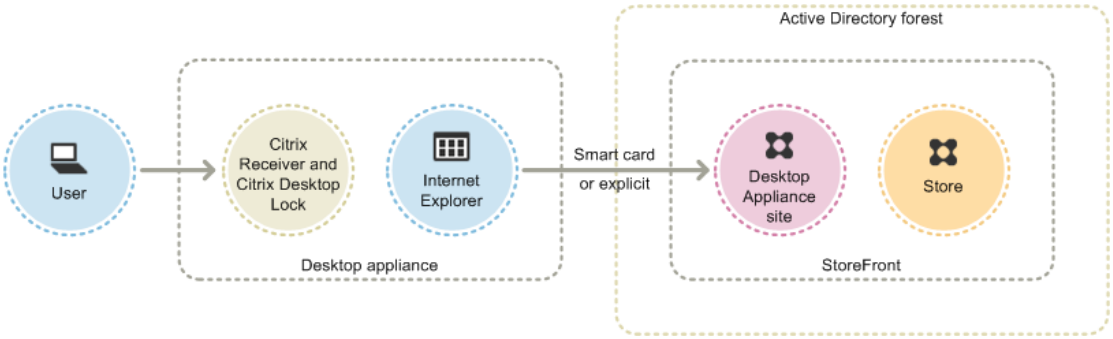
Because users of non-domain-joined devices log on to Receiver for Windows directly, you can enable users to fall back to explicit authentication. If you configure both smart card and explicit authentication, users are initially prompted to log on using their smart cards and PINs but have the option to select explicit authentication if they experience any issues with their smart cards.

If you decide to deploy NetScaler Gateway, users log on to their devices and are prompted by Receiver for Windows to authenticate to NetScaler Gateway. This applies to both domain-joined and non-domain-joined devices. 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

If Receiver for Windows is configured for pass-through authentication, users with domain-joined devices are automatically authenticated when they access their desktops and applications. Where pass-through authentication is not enabled, and for non-domain-joined devices, users must enter their PINs again when they access their desktops and applications.

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.



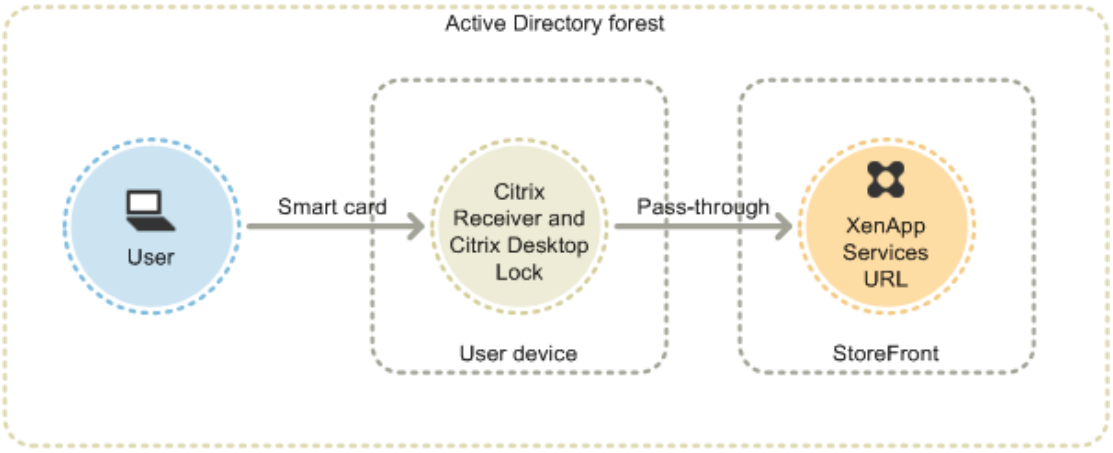
The figure shows smart card authentication from a non-domain-joined desktop appliance.

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. Smart card authentication without pass-through of smart card credentials is not available 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

- 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

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

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 To 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 automatically subscribe all users of a store to an application by appending the string KEYWORDS:Auto to the description you provide when you deliver the application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe.

- To automatically subscribe all users of a store to a web or software-as-a-service (SaaS) application managed by App Controller, select the App is available in Receiver to all users automatically check box when you configure the application settings.

- 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 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

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

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.

- Desktops and applications must have the same name and path on each server to be aggregated. In addition, the properties of aggregated resources, such as names and icons, must be the same. If this is not the case, users could see the properties of their resources change when Citrix Receiver enumerates the available resources.
- 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.

To install and set up StoreFront

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. 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.

   a. Ensure that load balancing is enabled on your NetScaler appliance.

   b. 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.

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

      StoreFront requires users' IP addresses to establish connections to their resources. For more information, see Inserting the IP Address of the Client in the Request Header.

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

   e. On the virtual server, configure persistence on the basis of HTTP cookies.

      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 HTTP Cookies.

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

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

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

Optionally, on Windows Server 2012 servers, enable the following features.

- .NET Framework 3.5 Features > .NET Framework 3.5

- .NET Framework 4.5 Features > .NET Framework 4.5, ASP.NET 4.5

Optionally, on Windows Server 2008 R2 servers, enable the following features.

- .NET Framework 3.5.1 Features > .NET Framework 3.5.1

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

4. Install StoreFront.

5. If you plan to use HTTPS to secure communications between StoreFront and users' devices, you must configure Microsoft Internet Information Services (IIS) for HTTPS before you configure StoreFront. HTTPS is required for smart card authentication. By default, Citrix Receiver requires HTTPS connections to stores. 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 domain certificate 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.

6. 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.

7. Ensure that the Windows Firewall service is running on the StoreFront server and then use the Citrix StoreFront management console to configure your server.

   StoreFront requires that the Windows Firewall service is running during initial configuration. Windows Firewall can be enabled or disabled, but the service must be running. Once initial configuration is complete, the Windows Firewall service can be stopped, if required.

To install StoreFront

1. Log on to the StoreFront server using an account with local administrator permissions.
2. Browse your installation media or download package, locate CitrixStoreFront-x64.exe, and run the file as an administrator.

   Note: On Windows Server 2008 R2 servers, a message may be displayed indicating that the .NET 3.5.1 feature will be enabled. If this message appears, click Yes.
3. Read and accept the license agreement, and click Next.
4. If the Review prerequisites page appears, click Next.
5. 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
   - 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

   On Windows Server 2012 servers, the following features are also enabled if they are not already configured.

   - .NET Framework 3.5 Features > .NET Framework 3.5
   - .NET Framework 4.5 Features > .NET Framework 4.5, ASP.NET 4.5

   On Windows Server 2008 R2 servers, the following features are also enabled if they are not already configured.

   - .NET Framework 3.5.1 Features > .NET Framework 3.5.1
6. 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. Browse your installation media or download package, locate CitrixStoreFront-x64.exe, and copy the file to a temporary location on the server.

3. At a command prompt, navigate to the folder containing the installation file and type the following command.

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

   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 To 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.

dws-first-auth-store

Due to technical difficulties, we are unable to display this topic. Citrix is currently fixing this problem. In the meantime, you can view this topic online:

http://support.citrix.com/proddocs/index.jsp?lang=en&topic=/dws-storefront-20/dws-first-auth-store.html

To create a new deployment

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

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.

   Important: If you plan to use HTTPS to secure communications between StoreFront and users' devices, you must configure Microsoft Internet Information Services (IIS) for HTTPS before you create the authentication service. 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.

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.

   - To add XenDesktop, XenApp, and VDI-in-a-Box resources to the store
   - To 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.

   - To provide remote access to the store through a NetScaler Gateway appliance

   - To 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. The Receiver for Web site 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.

To 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 To create a new deployment.

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 To add App Controller applications to the store. When you have added all the required resources to the store, return to Step 7 in To create a new deployment.

To 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 To create a new deployment.

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 providing 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.
4. Click OK to make the applications managed by your App Controller virtual appliance available in the store.

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 To 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 To create a new deployment.

To 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 To create a new deployment.

1. On the Remote Access page of the Create Store wizard, click Add.

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.

   The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN for StoreFront and the NetScaler Gateway virtual server is not supported.

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 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 To 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 To create a new deployment.

To 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 To create a new deployment.

1. On the Remote Access page of the Create Store wizard, click Add.
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 To 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 To create a new deployment.

To join an existing server group

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. 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.

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

2. In the results pane of the Citrix StoreFront management console, click Join existing server group.

3. Log on to the primary 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 primary 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 primary server. All the other servers in the group are updated with details of the new server.

To manage a multiple server deployment, use only the Citrix StoreFront management console on the primary server. Any configuration changes you make on the primary server must be propagated to the secondary servers to ensure a consistent configuration across the deployment.

To uninstall StoreFront

In addition to the product itself, uninstalling StoreFront removes the configurations of the authentication service, stores, Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs. In single-server deployments, users' application subscription data are also deleted from the subscription store service, whereas in multiple server deployments these data are retained on other servers in the deployment. 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, right-click the Citrix StoreFront tile and, in the app bar, click Uninstall.
3. In the Programs and Features dialog box, select Citrix StoreFront and click Uninstall to remove all StoreFront components from the server.

Upgrade StoreFront

To upgrade an existing StoreFront 1.2 deployment to StoreFront 2.0, you run the StoreFront 2.0 installation file. You cannot upgrade Receiver Storefront 1.1 to StoreFront 2.0 directly. Instead, you must first upgrade Receiver Storefront 1.1 to StoreFront 1.2 before upgrading to StoreFront 2.0.

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. Citrix recommends that you back up your data before upgrading.

Uninstalling StoreFront removes the authentication service, stores, 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 enables you to preserve your StoreFront configuration. In the case of single-server deployments, uninstalling StoreFront also deletes users' application subscription data from the database. Upgrading leaves the application subscription data intact so that you can migrate details of users' subscriptions from the database to the subscription store service on the upgraded server. Migrating existing application subscription data to an upgraded deployment ensures that users do not need to resubscribe to all of their applications.

1. If you are upgrading a multiple server StoreFront deployment, disable access to the deployment through the load balancing environment.

   StoreFront does not support multiple server deployments containing different product versions, so all servers must be updated concurrently. Disabling the load-balanced URL prevents users from connecting to the deployment during the upgrade.

2. Restart the primary StoreFront server in your deployment.

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

3. If Receiver for HTML5 is installed on the StoreFront server, use the Citrix HTML5 HDX Engine Configuration tool to remove Receiver for HTML5 from any Receiver for Web sites for which Receiver for HTML5 is configured. Uninstall Receiver for HTML5 from the Windows Programs and Features dialog box before continuing.

   Receiver for HTML5 does not support in-place upgrades so the StoreFront installation file cannot upgrade servers running Receiver for HTML5. For more information, see Receiver for HTML5.

   Once you have upgraded your StoreFront deployment, you must manually recreate the Receiver for HTML5 configuration for your Receiver for Web sites using the Citrix StoreFront management console. For more information about configuring Receiver for

4. Ensure that the Windows Firewall service is running on the StoreFront server and then run the StoreFront installation file as an administrator.

   StoreFront requires that the Windows Firewall service is running during the upgrade. Windows Firewall can be enabled or disabled, but the service must be running. Once initial configuration is complete, the Windows Firewall service can be stopped, if required. For more information about installing StoreFront, see To install and set up StoreFront.

5. For single-server StoreFront deployments only, in the dialog box that is displayed when installation is complete, specify when you want to migrate users' application subscription data from the old database to the new subscription store service.

   - Click Migrate Now to begin migrating users' application subscription data immediately. StoreFront starts a Windows PowerShell session and migrates users' application subscription data for all the upgraded stores.

   - Click Migrate Later to postpone this task if, for example, you do not want to migrate users' application subscription data for all the upgraded stores.

6. 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.

7. If you are upgrading a multiple server StoreFront deployment, repeat Steps 2, 3, 4, and 6 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 parallel 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.

8. 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.

9. If you are upgrading a multiple server StoreFront deployment, or if you postponed migration of application subscription data after upgrading a single-server deployment, on the Windows Start screen of the primary server in the deployment, click Citrix StoreFront.

   - To migrate users' application subscription data for all the stores in a deployment, select the Stores node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Migrate All Subscriptions.

   - To migrate users' application subscription data for an individual store, select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select the store. In the Actions pane, click Migrate Subscriptions.

StoreFront starts a Windows PowerShell session and migrates users' application subscription data from the old database to the subscription store service on the upgraded server.

10. For multiple server StoreFront deployments, restore access to your deployment through the load-balanced URL.

Manage your StoreFront deployment

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
- To create the authentication service
- Configure the authentication service
- Create a store
- Configure stores
- To create a Receiver for Web site
- Configure Receiver for Web sites
- To add a NetScaler Gateway connection
- Configure NetScaler Gateway connection settings
- To 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
- Configure Desktop Appliance sites
- To configure authentication for XenApp Services URLs

Configure server groups

The tasks described below enable you to modify settings for multiple server StoreFront deployments. To manage a multiple server deployment, use only the Citrix StoreFront management console on the primary server. Any configuration changes you make on the primary server must be propagated to the secondary servers 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 To 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 your updates if you subsequently propagate changes from another server in the deployment.

Change the base URL for a deployment

Use the Change Base URL task to modify the base URL used for stores and other StoreFront services hosted on a StoreFront deployment. For multiple server deployments, specify the load-balanced URL.

To create the authentication service

Use the Create Authentication Service task to configure the StoreFront authentication service. The authentication service authenticates users to Microsoft Active Directory, ensuring that users do not need to log on again to access their desktops and applications.

You can only configure one authentication service per StoreFront deployment. This task is only available when the authentication service has not yet been configured.

Important: If you plan to use HTTPS to secure communications between StoreFront and users' devices, you must configure Microsoft Internet Information Services (IIS) for HTTPS before you create the authentication service. 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.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Authentication node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Create Authentication Service.

3. Specify the access methods that you want to enable for your users and click Create.

   - Select the User name and password check box to enable explicit authentication. Users enter their credentials when they access their stores.

   - Select the Domain pass-through check box to enable pass-through of domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores. In order to use this option, pass-through authentication must be enabled when Receiver for Windows is installed on users' devices.

   - Select the Smart card check box to enable smart card authentication. Users authenticate using smart cards and PINs when they access their stores.

   - Select the Pass-through from NetScaler Gateway check box to enable pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

   To enable pass-through authentication for smart card users accessing stores through NetScaler Gateway, use the Configure Delegated Authentication task. For more information, see Configure the authentication service.

4. Once the authentication service has been created, click Finish.

   For more information about modifying settings for the authentication service, see Configure the authentication service.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure the authentication service

The authentication service authenticates users to Microsoft Active Directory, ensuring that users do not need to log on again to access their desktops and applications. You can only configure one authentication service per StoreFront deployment.

The tasks below describe how to modify settings for the StoreFront authentication service. Some advanced settings can only be changed by editing the authentication service configuration files. For more information, see Configure StoreFront using the configuration files.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To manage authentication methods

You can enable or disable user authentication methods set up when the authentication service was created by selecting an authentication method in the results pane of the Citrix StoreFront management console and, in the Actions pane, clicking Enable Method or Disable Method, as appropriate. To remove an authentication method from the authentication service or to add a new one, use the Add/Remove Methods task.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Authentication node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Add/Remove Methods.

3. Specify the access methods that you want to enable for your users.

   - Select the User name and password check box to enable explicit authentication. Users enter their credentials when they access their stores.

   - Select the Domain pass-through check box to enable pass-through of domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores. In order to use this option, pass-through authentication must be enabled when Receiver for Windows is installed on users' devices.

   - Select the Smart card check box to enable smart card authentication. Users authenticate using smart cards and PINs when they access their stores.

   - Select the Pass-through from NetScaler Gateway check box to enable pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

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

Generate security keys for the authentication service

Use the Generate Security Keys task to generate new security keys for self-signed certificates used by the authentication service. As part of security best practice, Citrix recommends that you periodically generate new security keys for self-signed certificates generated by StoreFront. When you generate new security keys, any users that 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.

To configure trusted user domains

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

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Authentication node in the left pane of the Citrix StoreFront management console and, in the results pane, select the appropriate authentication method. In the Actions pane, click Configure Trusted Domains.

3. Select Trusted domains only. Click Add to enter the name of a trusted domain. Users with accounts in that domain will be able to log on to all stores that use the authentication service. To modify a domain name, select the entry in the Trusted domains list and click Edit. Select a domain in the list and click Remove to discontinue access to stores for user accounts in that domain.

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

4. If you configure multiple trusted domains, select from the Default domain list the domain that is selected by default when users log on.

To enable users to change their passwords

Use the Manage Password Options task to enable Receiver for Web site users logging on with Active Directory domain credentials to change their passwords. 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. Enabling users to change their passwords exposes sensitive security functions to anyone who can access any of the stores that use the authentication service. If your organization has a security policy that reserves user password change functions for internal use only, ensure that none of the stores are accessible from outside your corporate network.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Authentication node in the left pane of the Citrix StoreFront management console and, in the results pane, select User name and password. In the Actions pane, click Manage Password Options.

3. Specify the circumstances under which Receiver for Web site users logging on with Active Directory domain credentials are able to change their passwords.

   - To enable users to change their passwords whenever they want, select At any time. Local users whose passwords are about to expire are shown a warning when they log on. Password expiry warnings are only displayed to users connecting from the internal network. By default, the notification period for a user is determined by the applicable Windows policy setting. For more information about setting custom notification periods, see To configure the password expiry notification period.

   - To enable users to change their passwords only when the passwords have already expired, select When expired. Users who cannot log on because their passwords have expired are redirected to the Change Password dialog box.

   - To prevent users from changing their passwords, select Never. If you select this option, you must make your own arrangements to support users who cannot access their desktops and applications because their passwords have expired.

   If you enable Receiver for Web site users to change their passwords at any time, ensure that there is sufficient disk space on your StoreFront servers to store profiles for all your users. To check whether a user's password is about to expire, StoreFront creates a local profile for that user on the server. StoreFront must be able to contact the domain controller to change users' passwords.

Delegate credential validation to NetScaler Gateway

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

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

Create a store

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

To create a store, you identify and configure communications with the servers providing the resources that you want to make available in the store. Then, optionally, you configure remote access to the store through NetScaler Gateway.

To add desktops and applications to the store

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Create Store.

3. On the Store Name page, specify a name for your store and click Next.

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

4. On the Delivery Controllers page, list the infrastructure providing the resources that you want to make available in the store. Click Add.

5. In the Add Delivery Controller dialog box, specify a name that will help you to identify the deployment and indicate whether the resources that you want to make available in the store are provided by XenDesktop, XenApp, AppController, or VDI-in-a-Box. For App Controller deployments, ensure that the name you specify does not contain any spaces.

6. If you are adding details of XenDesktop, XenApp, or VDI-in-a-Box servers, continue to Step 7. To make applications managed by App Controller available in the store, enter the name or IP address of an 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. Continue to Step 12.

7. To make desktops and applications provided by XenDesktop, XenApp, or VDI-in-a-Box available in the store, add the names or IP addresses of your servers to the Servers list. Specify multiple servers to enable fault tolerance, listing the entries in order of priority to set the failover sequence. For 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.

8. 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.

9. 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.

10. 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.

11. Click OK. You can configure stores to provide resources from any mixture of XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments. Repeat Steps 4 to 12, as necessary, to list additional deployments providing resources for the store. When you have added all the required resources to the store, click Next.

12. 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 an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the NetScaler Gateway Plug-in to establish the VPN tunnel.

    If it is not already enabled, the pass-through from NetScaler Gateway authentication method is automatically enabled when you configure remote access to the store. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

13. If you enabled remote access, continue to the next procedure to specify the NetScaler Gateway deployments through which users can access the store. Otherwise, on the Remote Access page, click Create. Once the store has been created, click Finish.

To provide remote access to the store through NetScaler Gateway

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

1. On the Remote Access page of the Create Store wizard, select from the NetScaler Gateway appliances list the deployments through which users can access the store. Any deployments you configured previously for other stores are available for selection in the list. If you want to add a further deployment to the list, click Add. Otherwise, continue to Step 13.

2. In the Add NetScaler Gateway Appliance dialog box, specify a name for the NetScaler Gateway deployment that will help users to identify it.

Users see the display name you specify in Citrix Receiver, so include relevant information in the name to help users decide whether to use that deployment. For example, you can include the geographical location in the display names for your 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 deployment. Specify the product version used in your deployment.

   The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN for StoreFront and the NetScaler Gateway virtual server is not supported.

4. If you are adding an Access Gateway 5.0 deployment, continue to Step 6. 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 domain credentials, select Domain.
   - If users are required to enter a tokencode obtained from a security token, select Security token.
   - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select Domain and security token.
   - If users are required to enter a one-time password sent by text message, select SMS authentication.
   - If users are required to present a smart card and enter a PIN, select Smart card.

   If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the Smart card fallback list. Continue to Step 7.

6. To add an Access Gateway 5.0 deployment, indicate whether the user logon point is hosted on a standalone appliance or an Access Controller server that is part of a cluster. If you are adding a cluster, click Next and continue to Step 8.

7. If you are configuring StoreFront for NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3, or a single Access Gateway 5.0 appliance, complete the NetScaler

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.

8. To configure StoreFront for an Access Gateway 5.0 cluster, list on the Appliances page the IP addresses or FQDNs of the appliances in the cluster and click Next.

9. 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.

10. For all deployments, 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.

11. 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.

12. Click Create to add your NetScaler Gateway deployment to the list on the Remote Access page.

13. Repeat Steps 1 to 12, as necessary, to add more NetScaler Gateway deployments to the NetScaler Gateway appliances list. If you enable access through multiple deployments by selecting more than one entry in the list, specify the default deployment to be used to access the store.

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

    For more information about modifying settings for stores, see Configure stores.

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. The Receiver for Web site 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 FQDN of the server or load balancing environment for your StoreFront deployment and *storename* is the name you specified for the store in Step 3.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure stores

StoreFront stores enumerate and aggregate desktops and applications from XenDesktop, XenApp, XenMobile App Controller, and VDI-in-a-Box, making these resources available to users. The tasks in this section describe how to modify settings for your stores using the Citrix StoreFront management console. Some advanced settings can only be changed by editing the store configuration files. For more information, see Configure StoreFront using the configuration files.

This section includes the following topics.

- To export store provisioning files for users
- Hide and advertise stores to users
- To manage the resources made available in stores
- To manage remote access to stores through NetScaler Gateway
- To manage Citrix Receiver updates
- To integrate Citrix Online applications with stores
- To configure support for connections through XenApp Services URLs
- Generate security keys for stores
- Remove stores

To export store provisioning files for users

Use the Export Multi-Store Provisioning File and Export Provisioning File tasks to generate files containing connection details for stores, including any NetScaler Gateway deployments and beacons configured for the stores. Make these files available to users to enable them to configure Citrix Receiver automatically with details of the stores. Users can also obtain Citrix Receiver provisioning files from Receiver for Web sites.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront. Select the Stores node in the left pane of the Citrix StoreFront management console.

2. To generate a provisioning file containing details for multiple stores, in the Actions pane, click Export Multi-Store Provisioning File and select the stores to include in the file. Select a store in the results pane and, in the Actions pane, click Export Provisioning File to generate a file for the selected store only.

3. Click Export and save the provisioning file with a .cr extension to a suitable location on your network.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Hide and advertise stores to users

Use the Hide Store task to prevent stores being presented to users to add to their accounts when they configure Citrix Receiver through email-based account discovery. By default, when you create a store it is presented as an option for users to add in Citrix Receiver when they discover the StoreFront deployment hosting the store. Hiding a store does not make it inaccessible, instead users must configure Citrix Receiver with connection details for the store, either manually, using a setup URL, or with a provisioning file. To resume advertising a hidden store, use the Advertise Store task.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To manage the resources made available in stores

Use the Manage Delivery Controllers task to add and remove from stores resources provided by XenDesktop, XenApp, App Controller, and VDI-in-a-Box, and to modify the details of the servers providing these resources.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click Manage Delivery Controllers.

3. In the Manage Delivery Controllers dialog box, click Add to include desktops and applications from another XenDesktop, XenApp, App Controller, or VDI-in-a-Box deployment in the store. To modify the settings for a deployment, select the entry in the Delivery controllers list and click Edit. Select an entry in the list and click Remove to stop the resources provided by the deployment being available in the store.

4. In the Add Delivery Controller or Edit 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, AppController, or VDI-in-a-Box. For App Controller deployments, ensure that the name you specify does not contain any spaces.

5. If you are adding details of XenDesktop, XenApp, or VDI-in-a-Box servers, continue to Step 6. To make applications managed by App Controller available in the store, enter the name or IP address of an 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. Continue to Step 10.

6. To make desktops and applications provided by XenDesktop, XenApp, or VDI-in-a-Box available in the store, click Add to enter the name or IP address of a server. 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. To modify the name or IP address of a server, select the entry in the Servers list and click Edit. Select an entry in the list and click Remove to stop StoreFront contacting the server to enumerate the resources available to the user.

7. Select from the Transport type list the type of connections for StoreFront to use for communications with the servers.

   - To send data over unencrypted connections, select HTTP. If you select this option, you must make your own arrangements to secure connections between StoreFront and your servers.

- To send data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), select HTTPS. If you select this option for 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.

8. Specify the port for StoreFront to use for connections to the servers. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. In the case of XenDesktop and XenApp servers, the specified port must be the port used by the Citrix XML Service.

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

10. Click OK. You can configure stores to provide resources from any mixture of XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments. Repeat Steps 3 to 10, as necessary, to add or modify other deployments in the Delivery controllers list.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To manage remote access to stores through NetScaler Gateway

Use the Enable Remote Access task to configure access to stores through NetScaler Gateway for users connecting from public networks.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click Enable Remote Access.

3. In the Enable Remote Access dialog box, 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 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 it is not already enabled, the pass-through from NetScaler Gateway authentication method is automatically enabled when you configure remote access to the store. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

4. If you enabled remote access, select from the NetScaler Gateway appliances list the deployments through which users can access the store. Any deployments you configured previously for this and other stores are available for selection in the list. If you want to add a further deployment to the list, click Add. Otherwise, continue to Step 16.

5. On the General Settings page, specify a name for the NetScaler Gateway deployment that will help users to identify it.

   Users see the display name you specify in Citrix Receiver, so include relevant information in the name to help users decide whether to use that deployment. For example, you can include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.

6. Enter the URL of the virtual server or user logon point (for Access Gateway 5.0) for your deployment. Specify the product version used in your deployment.

   The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN

7. If you are adding an Access Gateway 5.0 deployment, continue to Step 9. 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.

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

   If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the Smart card fallback list. Continue to Step 10.

9. To add an Access Gateway 5.0 deployment, indicate whether the user logon point is hosted on a standalone appliance or an Access Controller server that is part of a cluster. If you are adding a cluster, click Next and continue to Step 11.

10. If you are configuring StoreFront for NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3, or a single Access Gateway 5.0 appliance, complete the NetScaler Gateway authentication service URL in the Callback URL box. StoreFront automatically appends the standard portion of the URL. Click Next and continue to Step 13.

    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.

11. To configure StoreFront for an Access Gateway 5.0 cluster, list on the Appliances page the IP addresses or FQDNs of the appliances in the cluster and click Next.

12. 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

StoreFront uses the authentication service to authenticate remote users so that they do not need to re-enter their credentials when accessing stores.

13. For all deployments, 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.

14. 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.

15. Click Create to add your NetScaler Gateway deployment to the list in the Enable Remote Access dialog box.

16. Repeat Steps 4 to 15, as necessary, to add more NetScaler Gateway deployments to the NetScaler Gateway appliances list. If you enable access through multiple deployments by selecting more than one entry in the list, specify the default deployment to be used to access the store.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To manage Citrix Receiver updates

Use the Manage Citrix Receiver Updates task to specify the mechanism for delivery of updates to users who install Receiver for Windows on a device and access the store for the first time. If you enable automatic updates from the Citrix website, you can also provide additional plug-ins for installation on users' devices to ensure that they can immediately access all the functionality of the store once they have configured Receiver for Windows.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click Manage Citrix Receiver Updates.

3. Specify how first-time Receiver for Windows users accessing the store receive updates.

    - If you want users to receive updates automatically from Citrix, select Citrix (citrix.com). Users automatically receive the latest updates for Receiver for Windows and their plug-ins from the Citrix website, provided they are connected to the Internet.

    - If you are using Merchandising Server to manage updates for Receiver for Windows users, select Merchandising Server and specify the fully qualified domain name of your Merchandising Server appliance. If you are using HTTPS for communications with the authentication service, ensure that you install Secure Sockets Layer (SSL) certificates on your Merchandising Server appliance. For more information about using the StoreFront authentication service to enable Merchandising Server to identify users, see Configuring Authentication.

    - If you have an alternative strategy for managing updates, such as using a third-party electronic software distribution tool, select Do not check for updates. Users can still manually check for updates from the Receiver for Windows user interface

4. If you configured automatic updates from the Citrix website, specify the plug-ins to install on users' devices.

    - Select Offline Plug-in to enable Receiver for Windows users to access offline applications.

    - Select Secure Access Plug-in to enable users on public networks to establish virtual private network (VPN) connections to the store and other resources on the internal network. If you configured the store to provide full VPN access for users, the NetScaler Gateway Plug-in is included by default and cannot be removed.

    - Select HDX RealTime Media Engine to enable Receiver for Windows users to access audio and video communications provided by XenDesktop resources.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To integrate Citrix Online applications with stores

Use the Integrate with Citrix Online task to select the Citrix Online applications that you want to include in a store and specify the action that Citrix Receiver takes when users subscribe to a Citrix Online application from that store.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click Integrate with Citrix Online.

3. Select the Citrix Online applications that you want to include in the store and specify the action that Citrix Receiver takes when users subscribe to a Citrix Online application.

    - If you want to allow users without an account for the selected applications to visit the Citrix website and set up personal trial accounts, select Help users set up a trial account, if required.

    - If you want to prompt users to contact the system administrator to obtain an account for the selected applications, choose Ask users to contact their help desk for an account.

    - If accounts for all users are already in place for the selected applications, choose Add the app immediately.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure support for connections through XenApp Services URLs

Use the Configure Legacy Support task to configure access to your stores through 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 directly using the XenApp Services URL for the store. When you create a new store, the XenApp Services URL is enabled by default.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click Configure Legacy Support.

3. Select or clear the Enable legacy support check box to, respectively, enable or disable user access to the store through the displayed XenApp Services URL.

   The XenApp Services URL for a store has the form http[s]://*serveraddress*/Citrix/*storename*/PNAgent/config.xml, where *serveraddress* is the fully qualified domain name of the server or load balancing environment for your StoreFront deployment and *storename* is the name specified for the store when it was created.

4. If you enable legacy support, optionally specify a default store in your StoreFront deployment for users with the Citrix Online Plug-in.

   Specify a default store so that your users can configure the Citrix Online Plug-in with the server URL or load-balanced URL of the StoreFront deployment, rather than the XenApp Services URL for a particular store.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Generate security keys for stores

Use the Generate Security Keys task to generate new security keys for self-signed certificates used by a store. As part of security best practice, Citrix recommends that you periodically generate new security keys for self-signed certificates generated by StoreFront. When you generate new security keys, any users that 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Remove stores

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

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To create a Receiver for Web site

Use the Create Website task to add Receiver for Web sites, which enable users to access stores through a webpage.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Receiver for Web node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Create Website.

3. Select the store for which you want to create the Receiver for Web site. To create a site for a store hosted on another server, select Remote store and specify the URL of the remote store.

4. If you want to alter the URL to which users will browse to access the Receiver for Web site, make the required changes in the Website path box. Click Create and then, once the site has been created, click Finish.

   The URL for users to access the Receiver for Web site is displayed. For more information about modifying settings for Receiver for Web sites, see Configure Receiver for Web sites.

By default, when a user accesses a Receiver for Web site from a computer running Windows or Mac OS X, the site attempts to determine whether Citrix 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. For more information about modifying this behavior, see To disable detection and deployment of Citrix Receiver.

The default configuration for Receiver for Web sites requires that users install a compatible version of Citrix Receiver to access their desktops and applications. However, you can enable Receiver for HTML5 on your Receiver for Web sites so that users who cannot install Citrix Receiver can still access resources. For more information, see Configure Receiver for Web sites.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure Receiver for Web sites

Receiver for Web sites enable users to access stores through a webpage. The tasks described below enable you to modify settings for your Receiver for Web sites. Some advanced settings can only be changed by editing the site configuration files. For more information, see Configure Receiver for Web sites using the configuration files.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To add resource shortcuts to other websites

Use the Add Shortcuts to Websites task to provide users with rapid access to desktops and applications from websites hosted on the internal network. You generate URLs for resources available through the Receiver for Web site and embed these links on your websites. Users click on a link and are redirected to the Receiver for Web site, where they log on if they have not already done so. The Receiver for Web site automatically starts the resource. In the case of applications, users are also subscribed to the application if they have not subscribed previously.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Receiver for Web node in the left pane of the Citrix StoreFront management console and, in the results pane, select a site. In the Actions pane, click Add Shortcuts to Websites.

3. In the Add Shortcuts to Websites dialog box, click Add to enter the URL for a website on which you plan to host shortcuts. URLs must be specified in the form http[s]://*hostname*[:*port*], where *hostname* is the fully qualified domain name of the website host and *port* is the port used for communication with the host if the default port for the protocol is not available. Paths to specific pages on the website are not required. To modify a URL, select the entry in the Websites list and click Edit. Select an entry in the list and click Remove to delete the URL for a website on which you no longer want to host shortcuts to resources available through the Receiver for Web site.

4. Click Get app shortcuts and then click Save when you are prompted to save your configuration changes.

5. Log on to the Receiver for Web site and copy the URLs you require to your website.

Change the store for a Receiver for Web site

Use the Change Store task to switch the store that users access through a Receiver for Web site. Only a single store can be accessed through each site. To switch to a store hosted on another server, select Remote store and specify the URL of the remote store.

To configure site behavior for users without Citrix Receiver

Use the Deploy Citrix Receiver task to configure the behavior of a Receiver for Web site when a Windows or Mac OS X user without Citrix Receiver installed accesses the site. By default, Receiver for Web sites automatically attempt to determine whether Citrix Receiver is installed when accessed from computers running Windows or Mac OS X. For more information about modifying this behavior, see To disable detection and deployment of Citrix Receiver.

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. For more information, see To make Citrix Receiver installation files available on the server.

For users who cannot install Citrix Receiver, you can enable Receiver for HTML5 on your Receiver for Web sites. Receiver for HTML5 enables users to access desktops and applications directly within HTML5-compatible web browsers without needing to install Citrix Receiver. 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.

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. By default, XenDesktop and XenApp use port 8008 for Receiver for HTML5 connections. Ensure your firewalls and other network devices permit access to this port. If you change the WebSockets port number setting in the policy, ensure that you make the corresponding change in the StoreFront configuration. For more information, see WebSockets policy settings.

Receiver for HTML5 can only be used with Internet Explorer over HTTP connections. 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.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Receiver for Web node in the left pane of the Citrix StoreFront management console and, in the results pane, select a site. In the Actions pane, click Deploy Citrix Receiver.

3. Specify the response of the Receiver for Web site if Citrix Receiver cannot be detected on a user's device.

    - If you want the site to prompt the user to download and install the appropriate Citrix Receiver for their platform, select Install locally. Users must install Citrix Receiver to access desktops and applications through the site.

- If you want the site to prompt the user to download and install Citrix Receiver but fall back to Receiver for HTML5 if Citrix Receiver cannot be installed, select Use Receiver for HTML5 if local install fails. Users without Citrix Receiver are prompted to download and install Citrix Receiver every time they log on to the site.

- If you want the site to enable access to resources through Receiver for HTML5 without prompting the user to download and install Citrix Receiver, select Always use Receiver for HTML5. Users without Citrix Receiver always access desktops and applications on the site through Receiver for HTML5, provided they use an HTML5-compatible browser.

Remove Receiver for Web sites

Use the Remove Website task to delete a Receiver for Web site. When you remove a site, users can no longer use that webpage to access the store.

To add a NetScaler Gateway connection

Use the Add NetScaler Gateway Appliance task to add NetScaler Gateway deployments through which users can access your stores. You must enable the pass-through from NetScaler Gateway authentication method before you can configure remote access to your stores through NetScaler Gateway. For more information about configuring NetScaler Gateway for StoreFront, see Integrating NetScaler Gateway with XenMobile App Edition.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the NetScaler Gateway node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Add NetScaler Gateway Appliance.

3. On the General Settings page, specify a name for the NetScaler Gateway deployment that will help users to identify it.

   Users see the display name you specify in Citrix Receiver, so include relevant information in the name to help users decide whether to use that deployment. For example, you can include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.

4. Enter the URL of the virtual server or user logon point (for Access Gateway 5.0) for your deployment. Specify the product version used in your deployment.

   The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN for StoreFront and the NetScaler Gateway virtual server is not supported.

5. If you are adding an Access Gateway 5.0 deployment, continue to Step 7. Otherwise, specify the subnet IP address of the 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.

6. 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 domain credentials, select Domain.

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

If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the Smart card fallback list. Continue to Step 8.

7. To add an Access Gateway 5.0 deployment, indicate whether the user logon point is hosted on a standalone appliance or an Access Controller server that is part of a cluster. If you are adding a cluster, click Next and continue to Step 9.

8. If you are configuring StoreFront for NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3, or a single Access Gateway 5.0 appliance, complete the NetScaler Gateway authentication service URL in the Callback URL box. StoreFront automatically appends the standard portion of the URL. Click Next and continue to Step 11.

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

9. To configure StoreFront for an Access Gateway 5.0 cluster, list on the Appliances page the IP addresses or FQDNs of the appliances in the cluster and click Next.

10. On the Enable Silent Authentication page, list URLs for the authentication service running on the Access Controller servers. Add URLs for multiple servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

    StoreFront uses the authentication service to authenticate remote users so that they do not need to re-enter their credentials when accessing stores.

11. For all deployments, if you are making resources provided by 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.

12. 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.

13. Click Create to add details of your NetScaler Gateway deployment. Once the deployment has been added, click Finish.

    For more information about updating the details of your deployments, see Configure NetScaler Gateway connection settings.

To provide access to stores through NetScaler Gateway, one internal beacon point and at least two external beacon points are required. Citrix Receiver uses beacon points to determine whether users are connected to local or public networks and then selects the appropriate access method. By default, StoreFront uses the server URL or load-balanced URL of your deployment as the internal beacon point. The Citrix website and the virtual server or user logon point (for Access Gateway 5.0) URL of the first NetScaler Gateway deployment you add are used as external beacon points by default. For more information about changing beacon points, see To configure beacon points.

To enable users to access your stores through NetScaler Gateway, ensure that you configure remote user access for those stores.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure NetScaler Gateway connection settings

The tasks below describe how to update details of the NetScaler Gateway deployments through which users access your stores. For more information about configuring NetScaler Gateway for StoreFront, see Integrating NetScaler Gateway with XenMobile App Edition.

If you make any changes to your NetScaler Gateway deployments, ensure that users who access stores through these deployments update Citrix Receiver with the modified connection information. Where a Receiver for Web site is configured for a store, users can obtain an updated Citrix Receiver provisioning file from the site. Otherwise, you can export a provisioning file for the store and make this file available to your users.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To change general NetScaler Gateway settings

Use the Change General Settings task to modify the NetScaler Gateway deployment names shown to users and to update StoreFront with changes to the virtual server or user logon point URL, or the deployment mode of your NetScaler Gateway infrastructure.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the NetScaler Gateway node in the left pane of the Citrix StoreFront management console and, in the results pane, select a NetScaler Gateway deployment. In the Actions pane, click Change General Settings.

3. Specify a name for the NetScaler Gateway deployment that will help users to identify it.

   Users see the display name you specify in Citrix Receiver, so include relevant information in the name to help users decide whether to use that deployment. For example, you can include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.

4. Enter the URL of the virtual server or user logon point (for Access Gateway 5.0) for your deployment. Specify the product version used in your deployment.

   The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN for StoreFront and the NetScaler Gateway virtual server is not supported.

5. If your deployment is running Access Gateway 5.0, continue to Step 7. Otherwise, specify the subnet IP address of the NetScaler Gateway appliance, if necessary. A

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.

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

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

7. If your deployment consists of NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3, or a single Access Gateway 5.0 appliance, complete the NetScaler Gateway authentication service URL in the Callback URL box. StoreFront automatically appends the standard portion of the URL.

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

Manage Access Gateway 5.0 appliances

Use the Manage Appliances task to add, edit, or remove from StoreFront the IP addresses or FQDNs of the appliances in your Access Gateway 5.0 cluster.

Enable silent user authentication through Access Controller

Use the Enable Silent Authentication task to add, edit, or remove URLs for the authentication service running on the Access Controller servers for your Access Gateway 5.0 cluster. Enter URLs for multiple servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. StoreFront uses the authentication service to authenticate remote users so that they do not need to re-enter their credentials when accessing stores.

To manage Secure Ticket Authorities

Use the Secure Ticket Authority task to update the list of Secure Ticket Authorities (STAs) from which StoreFront obtains user session tickets and to configure session reliability. The STA is hosted on 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.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the NetScaler Gateway node in the left pane of the Citrix StoreFront management console and, in the results pane, select a NetScaler Gateway deployment. In the Actions pane, click Secure Ticket Authority.

3. Click Add to enter the URL for a server running the STA. To modify a URL, select the entry in the Secure Ticket Authority URLs list and click Edit. Select a URL in the list and click Remove to stop StoreFront obtaining session tickets from that STA. Enter 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.

4. 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.

Remove NetScaler Gateway deployments

Use the Remove NetScaler Gateway Appliance task to delete the details of a NetScaler Gateway deployment from StoreFront. Once a NetScaler Gateway deployment is removed, users are no longer be able to access stores through that deployment.

To configure beacon points

Use the Manage Beacons task to specify URLs inside and outside your internal network to be used as beacon points. 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 example, if the internal beacon point is accessible, the user is connected to the local network. However, if Citrix Receiver cannot contact the internal beacon point and receives responses from both the external beacon points, the user has an Internet connection but is outside the corporate network. This means that the user must connect to desktops and applications though NetScaler Gateway. When the user accesses a desktop or application, the server providing the resource is notified to provide details of the NetScaler Gateway appliance through which the connection must be routed. This means that the user does not need to log on to the appliance when accessing the desktop or application.

By default, StoreFront uses the server URL or load-balanced URL of your deployment as the internal beacon point. The Citrix website and the virtual server or user logon point (for Access Gateway 5.0) URL of the first NetScaler Gateway deployment you add are used as external beacon points by default.

If you change any beacon points, ensure that users update Citrix Receiver with the modified beacon information. Where a Receiver for Web site is configured for a store, users can obtain an updated Citrix Receiver provisioning file from the site. Otherwise, you can export a provisioning file for the store and make this file available to your users.

1. On the Windows Start screen of the primary StoreFront server in your deployment, click Citrix StoreFront.

2. Select the Beacons node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Manage Beacons.

3. Specify the URL to use as the internal beacon point.

   - To use the server URL or load-balanced URL of your StoreFront deployment, select Use the service URL.

   - To use an alternative URL, select Specify beacon address and enter a highly available URL within your internal network.

4. Click Add to enter the URL of an external beacon point. To modify a beacon point, select the URL in the External beacons list and click Edit. Select a URL in the list and click Remove to stop using that address as a beacon point.

   You must specify at least two highly available external beacon points that can be resolved from public networks. This enables Citrix Receiver to determine whether users are located behind an Internet paywall, such as in a hotel or Internet café. In such cases, all the external beacon points connect to the same proxy.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure smart card authentication

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

Prerequisites

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

Configure NetScaler Gateway

- On your NetScaler Gateway appliance, install a signed server certificate from a certificate authority. For more information, see Installing and Managing Certificates.

- Install on your appliance the root certificate of the certificate authority issuing your smart card user certificates. For more information, see To install a root certificate on NetScaler Gateway.

- Create and configure a virtual server for client certificate authentication. Create a certificate authentication policy, specifying SubjectAltName:PrincipalName for user name extraction from the certificate. Then, bind the policy to the virtual server and configure the virtual server to request client certificates. For more information, see Configuring and Binding a Client Certificate Authentication Policy.

- Bind the certificate authority root certificate to the virtual server. For more information, see To add a root certificate to a virtual server.

- You can ensure that users are not prompted for their smart card credentials again when they access their desktops and applications by creating a second virtual server for which client authentication is disabled in the Secure Sockets Layer (SSL) parameters. For more information, see Configuring Smart Card Authentication.

  You must also configure StoreFront to route user connections to resources through this virtual server. Users log on to the first virtual server and the second virtual server is used for connections to their resources, ensuring that they do not need to authenticate again. Configuring a second virtual server for user connections to resources is optional unless you plan to enable users to fall back to explicit authentication if they experience any issues with their smart cards.

- Create session policies and profiles for connections from NetScaler Gateway to StoreFront and bind them to the appropriate virtual server. For more information, see Access to StoreFront Through NetScaler Gateway.

- If you configured the virtual server used for connections to StoreFront to require client certificate authentication for all communications, you must create a further virtual server to provide the callback URL for StoreFront. This virtual server is used only by StoreFront to verify requests from the NetScaler Gateway appliance and so does not need to be publically accessible. A separate virtual server is required when client certificate authentication is mandatory because StoreFront cannot present a certificate to authenticate. For more information, see Creating Additional Virtual Servers.

Configure StoreFront

- You must use HTTPS for communications between StoreFront and users' devices to enable smart card authentication. Configure Microsoft Internet Information Services (IIS) for HTTPS before you create the StoreFront authentication service. To do this, obtain an SSL certificate in IIS and then add HTTPS binding to the default website.

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

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

  When IIS is configured to require client certificates for HTTPS connections to all StoreFront URLs, smart card users cannot connect through NetScaler Gateway and cannot fall back to explicit authentication. Users must log on again if they remove their smart cards from their devices. To enable this IIS site configuration, the authentication service and stores must be collocated on the same server, and a client certificate that is valid for all the stores must be used.

  If you are installing StoreFront on Windows Server 2012, note that non-self-signed certificates installed in the Trusted Root Certification Authorities certificate store on the server are not trusted when IIS is configured to use SSL and client certificate authentication. For more information about this issue, see http://support.microsoft.com/kb/2802568.

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

- Enable smart card authentication to StoreFront for local users on the internal network. For smart card users accessing stores through NetScaler Gateway, enable the pass-through with NetScaler Gateway authentication method and ensure that StoreFront is configured to delegate credential validation to NetScaler Gateway. For more information, see Configure the authentication service.

  If you want smart card users to be able to fall back to explicit authentication if they experience any issues with their smart cards, do not disable the user name and password authentication method. For more information about the user device configurations for which falling back to explicit authentication is available, see Use smart cards with StoreFront.

- If you plan to enable pass-through authentication when you install Receiver for Windows on domain-joined user devices, edit the default.ica file for the store to enable pass-through of users' smart card credentials when they access their desktops and applications. For more information, see To enable pass-through with smart card authentication for Receiver for Windows.

- If you created an additional NetScaler Gateway virtual server to be used only for user connections to resources, configure optimal NetScaler Gateway routing through this

virtual server for connections to the deployments providing the desktops and applications for the store. For more information, see To configure optimal NetScaler Gateway routing for a store.

- To enable users of non-domain-joined Windows desktop appliances to log on to their desktops using smart cards, enable smart card authentication to your Desktop Appliance sites. For more information, see Configure Desktop Appliance sites.

  Configure the Desktop Appliance site for both smart card and explicit authentication to enable users to log on with explicit credentials if they experience any issues with their smart cards.

- To enable users of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock to authenticate using smart cards, enable pass-through with smart card authentication to your XenApp Services URLs. For more information, see To configure authentication for XenApp Services URLs.

Configure user devices

- Ensure that your vendor's smart card middleware is installed on all user devices.
- For users with non-domain-joined Windows desktop appliances, install Receiver for Windows (Enterprise) using an account with administrator permissions. Configure Internet Explorer to start in full-screen mode displaying the Desktop Appliance site when the device is powered on. Note that Desktop Appliance site URLs are case sensitive. Add the Desktop Appliance site to the Local intranet or Trusted sites zone in Internet Explorer. Once you have confirmed that you can log on to the Desktop Appliance site with a smart card and access resources from the store, install the Citrix Desktop Lock. For more information, see To install the Desktop Lock.
- For users with domain-joined desktop appliances and repurposed PCs, install Receiver for Windows (Enterprise) using an account with administrator permissions. Configure Receiver for Windows with the XenApp Services URL for the appropriate store. Once you have confirmed that you can log on to the device with a smart card and access resources from the store, install the Citrix Desktop Lock. For more information, see To install the Desktop Lock.
- For all other users, install the appropriate version of Citrix Receiver on the user device. To enable pass-through of smart card credentials to XenDesktop and XenApp for users with domain-joined devices, use an account with administrator permissions to install Receiver for Windows at a command prompt with the /includeSSON option. For more information, see Configure and install Receiver for Windows using command-line parameters.

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

  Enable the Smart card authentication policy. To enable pass-through of users' smart card credentials, select Use pass-through authentication for PIN. Then, to pass users' smart card credentials through to XenDesktop and XenApp, enable the Local user name and password policy and select Allow pass-through authentication for all ICA connections. For more information, see ICA Settings Reference.

  If you enabled pass-through of smart card credentials to XenDesktop and XenApp for users with domain-joined devices, add the store URL to the Local intranet or Trusted sites zone in Internet Explorer. Ensure that Automatic logon with the current user name and password is selected in the security settings for the zone.
- Where necessary, provide users with connection details for the store (for users on the internal network) or NetScaler Gateway appliance (for remote users) using an appropriate method. For more information about providing configuration information to your users, see Citrix Receiver.

To enable pass-through with smart card authentication for Receiver for Windows

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

1. On the primary StoreFront server in your deployment, use a text editor to open the default.ica file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix*storename*\App_Data\ directory, where *storename* is the name specified for the store when it was created.

2. To enable pass-through of smart card credentials for users who access stores without NetScaler Gateway, add the following setting in the [Application] section.

   DisableCtrlAltDel=Off

   This setting applies to all users of the store. To enable both domain pass-through and pass-through with smart card authentication to desktops and applications, you must create separate stores for each authentication method. Then, direct your users to the appropriate store for their method of authentication.

3. To enable pass-through of smart card credentials for users accessing stores through NetScaler Gateway, add the following setting in the [Application] section.

   UseLocalUserAndPassword=On

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

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Set up highly available multi-site store configurations

For stores that aggregate resources from multiple deployments, particularly geographically dispersed deployments, you can configure load balancing and failover between deployments, mapping of users to deployments, and specific disaster recovery deployments to provide highly available resources. Where you have configured separate NetScaler Gateway appliances for your deployments, you can define the optimal appliance for users to access each of the deployments. If you deploy NetScaler Gateway in a global server load balancing configuration, you must update the store configuration with details for each of the appliances.

This section includes the following topics.

To configure load balancing, failover, disaster recovery, and user mapping for a store

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.

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 To manage the resources made available in stores.

2. On the primary StoreFront server in your deployment, 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.

```
<resourcesWingConfigurations>
  <resourcesWingConfiguration name="Default" wingName="Default" />
</resourcesWingConfigurations>
```

4. Specify your configuration as shown below.

```
<resourcesWingConfigurations>
  <resourcesWingConfiguration name="Default" wingName="Default">
    <userFarmMappings>
      <clear />
      <userFarmMapping name="user_mapping">
        <groups>
          <group name="domain\usergroup" sid="securityidentifier" />
          <group ... />
          ...
        </groups>
        <equivalentFarmSets>
          <equivalentFarmSet name="setname" loadBalanceMode="{LoadBalanced | Failover}"
           aggregationGroup="aggregationgroupname">
            <primaryFarmRefs>
              <farm name="primaryfarmname" />
              <farm ... />
              ...
            </primaryFarmRefs>
            <backupFarmRefs>
              <farm name="backupfarmname" />
              <farm ... />
```

```
            ...
          </backupFarmRefs>
        </equivalentFarmSet>
        <equivalentFarmSet ... >
          ...
        </equivalentFarmSet>
      </equivalentFarmSets>
    </userFarmMapping>
    <userFarmMapping>
      ...
    </userFarmMapping>
  </userFarmMappings>
 </resourcesWingConfiguration>
</resourcesWingConfigurations>
```

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 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

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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure subscription synchronization

To configure periodic synchronization of users' application subscriptions between stores in different StoreFront deployments, you execute Windows PowerShell commands.

1. On the primary StoreFront server in your deployment, use an account with administrator permissions to start Windows PowerShell.

2. 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\.

3. To specify the remote StoreFront deployment containing the store to be synchronized, type the following command.

   Add-DSSubscriptionsRemoteSyncCluster –clusterName *deploymentname*
   –clusterAddress *baseurl*

   Where *deploymentname* is a name that helps you identify the remote deployment and *baseurl* is the server URL or load-balanced URL of the remote deployment.

4. 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.

5. To configure synchronization to occur at particular times throughout the 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 Add further -startTime entries to specify additional synchronization times throughout the day.

6. Alternatively, to configure regular synchronization at a specific interval, type the following command.

Add-DSSubscriptionsSyncReoccuringSchedule –scheduleName *synchronizationname* –startTime *hh*:*mm*:*ss* -repeatMinutes *interval*

Where *synchronizationname* is a name that helps you identify the schedule you are creating. Use the -startTime setting to specify the delay in hours, minutes, and seconds before the new schedule becomes active once created. For *interval*, specify the time in minutes between each synchronization.

7. Add the 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.

8. If your local StoreFront deployment consists of multiple servers, use the Citrix StoreFront management console on the primary server 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.

9. Repeat Steps 1 to 8 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.

10. 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 the primary server in each deployment, type the following command.

    Restart-DSSubscriptionsStoreSubscriptionService

11. 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.

    Remove-DSSubscriptionsSchedule –scheduleName *synchronizationname*

    Where *synchronizationname* is the name that you specified for the schedule when you created it.

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

    Get-DSSubscriptionsSyncScheduleSummary

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure optimal NetScaler Gateway routing for a store

To configure optimal NetScaler Gateway appliances for your deployments, you edit the store configuration files.

1. On the primary StoreFront server in your deployment, 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.

   ```
   <optimalGatewayForFarmsCollection />
   ```

3. Specify the optimal NetScaler Gateway routing for your deployments as shown below.

   ```
   <optimalGatewayForFarmsCollection>
     <optimalGatewayForFarms enabledOnDirectAccess="{true | false}">
       <farms>
         <farm name="farmname" />
         ...
       </farms>
       <optimalGateway key="_" name="deploymentname" stasUseLoadBalancing="{true | false}"
        stasBypassDuration="hh:mm:ss" enableSessionReliability="{true | false}"
        useTwoTickets="{true | false}">
         <hostnames>
           <add hostname="appliancefqdn:port" />
         </hostnames>
         <staUrls>
           <add staUrl="https://stapath/scripts/ctxsta.dll" />
           ...
         </staUrls>
       </optimalGateway>
     </optimalGatewayForFarms>
     <optimalGatewayForFarms>
       ...
     </optimalGatewayForFarms>
   </optimalGatewayForFarmsCollection>
   ```

   Use the following elements to define your configuration.

   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. Set the value of the enabledOnDirectAccess

farms

Specifies a set of, typically collocated, XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments that share a common optimal NetScaler Gateway appliance. 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.

optimalGateway

Specifies details of the optimal NetScaler Gateway appliance for users to access resources provided by the listed deployments. Enter a name for the NetScaler Gateway appliance that enables you to identify it. Set the value of the stasUseLoadBalancing attribute to true to randomly obtain session tickets from all STAs, evenly distributing requests across all the STAs. When the value of the stasUseLoadBalancing attribute is 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. Use the stasBypassDuration attribute to set the time period, in hours, minutes, and seconds, for which an STA is considered unavailable after a failed request. To keep disconnected sessions open while Citrix Receiver attempts to reconnect automatically, set the value of the enableSessionReliability attribute to true. 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.

hostnames

Specifies the fully qualified domain name (FQDN) and port of the optimal NetScaler Gateway appliance.

staUrls

Specifies the URLs for XenDesktop, XenApp, and VDI-in-a-Box servers running the Secure Ticket Authority (STA). For XenDesktop and XenApp servers, *stapath* is the fully FQDN or IP address of the server. In the case of VDI-in-a-Box servers, *stapath* is the fully qualified domain name or IP address of the VDI-in-a-Box server, or the grid-wide virtual IP address, followed by /dt/sta.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure a store for NetScaler Gateway global server load balancing

1. Use the Enable Remote Access task to configure the store with details of your load-balanced NetScaler Gateway deployment. For more information, see To 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.

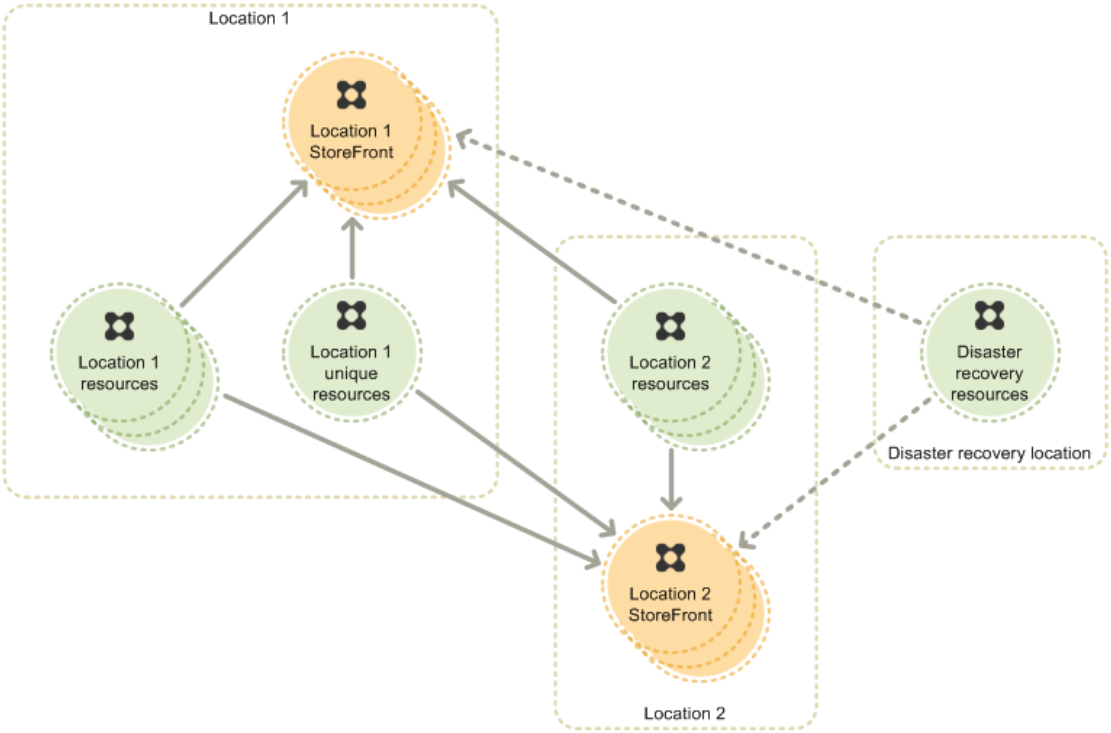
3. Repeat the process using exactly the same settings except for the display name and the subnet IP address. For the subnet IP address, enter the virtual server IP address for another appliance in your deployment.

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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Example highly available multi-site store configurations

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.

This section includes the following topics.

- Load balancing and failover example
- User mapping example

- Subscription synchronization example
- Optimal NetScaler Gateway routing example

Load balancing and failover example

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="S-1-1-0" />
        </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>
          <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="None">
            <primaryFarmRefs>
              <farm name="Location1UniqueDeployment" />
            </primaryFarmRefs>
            <backupFarmRefs>
            </backupFarmRefs>
          </equivalentFarmSet>
```

```
      </equivalentFarmSets>
    </userFarmMapping>
  </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

User mapping example

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 domain.

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

```
<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>
      </userFarmMapping>
      <userFarmMapping name="UserMapping2">
        <groups>
          <group name="Location2Users"
           sid="S-1-5-21-1004336348-1177238915-682003330-1002" />
        </groups>
        <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="UserMapping3">
      <groups>
        <group name="Location1Users"
         sid="S-1-5-21-1004336348-1177238915-682003330-1001" />
        <group name="Location2Users"
         sid="S-1-5-21-1004336348-1177238915-682003330-1002" />
      </groups>
      <equivalentFarmSets>
        <equivalentFarmSet name="Location1Unique"
         loadBalanceMode="LoadBalanced" aggregationGroup="None">
          <primaryFarmRefs>
            <farm name="Location1UniqueDeployment" />
          </primaryFarmRefs>
          <backupFarmRefs>
          </backupFarmRefs>
        </equivalentFarmSet>
      </equivalentFarmSets>
    </userFarmMapping>
  </userFarmMappings>
 </resourcesWingConfiguration>
</resourcesWingConfigurations>
```

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.

Subscription synchronization example

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. This is because the StoreFront deployments in each location maintain details of users' application subscriptions separately, by default.

To ensure that users only need to subscribe to applications in one location, you configure subscription synchronization between the stores provided by the two StoreFront deployments. First, you ensure that both stores have the same name, "Location1and2Store." Then, on the primary StoreFront server in Location 1, you import the StoreFront modules UtilsModule.psm1 and SubscriptionSyncModule.psm1. You add the Active Directory domain machine accounts for each StoreFront server in the Location 2 deployment to the CitrixSubscriptionSyncUsers local users group on the Location 1 primary server. Then, you configure synchronization of users' application subscriptions from Location 1 to Location 2 by executing the following Windows PowerShell commands.

```
Add-DSSubscriptionsRemoteSyncCluster –clusterName "Location2"
  –clusterAddress "location2storefront.example.com"
Add-DSSubscriptionsRemoteSyncStore –clusterName "Location2"
  –storeName "Location1and2Store"
Add-DSSubscriptionsSyncSchedule –scheduleName "Location1Sync2Daily"
  –startTime 06:00:00 -startTime 18:00:00
```

Using the Citrix StoreFront management console on the primary server, you propagate the configuration changes to the other servers in the Location 1 deployment. Then, you repeat the process on the primary StoreFront server in Location 2, including importing the modules and adding the Location 1 StoreFront server machine accounts to the synchronization service users group. You execute the following Windows PowerShell commands and propagate the change to the other servers in Location 2.

```
Add-DSSubscriptionsRemoteSyncCluster –clusterName "Location1"
  –clusterAddress "location1storefront.example.com"
Add-DSSubscriptionsRemoteSyncStore –clusterName "Location1"
  –storeName "Location1and2Store"
Add-DSSubscriptionsSyncSchedule –scheduleName "Location2Sync1Daily"
  –startTime 06:30:00 -startTime 18:30:00
```

To start synchronizing users' application subscriptions between the stores, you restart the subscription store service on the primary StoreFront servers in both Location 1 and Location 2. With this configuration, users' application subscriptions are synchronized from Location 1 to Location 2 every day, once in the morning and again in the evening. Synchronization from Location 2 to Location 1 also occurs twice daily, but is offset by 30 minutes to ensure that a conflict cannot arise whereby both deployments attempt to synchronize

Optimal NetScaler Gateway routing example

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

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

- To enable ICA file signing
- To configure communication time-out duration and retry attempts
- To configure the password expiry notification period
- To disable file type association
- To enable socket pooling
- To customize the Citrix Receiver logon dialog box
- To prevent Receiver for Windows from caching passwords

To enable ICA file signing

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 certificate authority or from your organization's private certificate authority. If you are unable to obtain a suitable certificate from a certificate authority, you can either use an existing SSL certificate, such as a server certificate, or create a new root certificate 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.

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. On the primary StoreFront server in your deployment, 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.

```
<certificateManager>
  <certificates>
    <clear />
    <add ... />
    ...
  </certificates>
</certificateManager>
```

4. Include details of the certificate to be used for signing as shown below.

```
<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.

   ```
   <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 hashAgorithm attribute to sha256, sha384, or sha512, as required.

8. Using an account with local administrator permissions, start Windows PowerShell and, at a command prompt, type the following commands to enable the store to access the private key.

   ```
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
     $certificate = Get-DSCertificate "certificatethumbprint"

   Add-DSCertificateKeyReadAccess $certificate "IIS APPPOOL\Citrix Delivery
     Services Resources"
   ```

   Where *certificatethumbprint* is the digest of the certificate data produced by the hash algorithm.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure communication time-out duration and retry attempts

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 both the authentication service and store.

1. On the primary StoreFront server in your deployment, use a text editor to open the web.config files for both the authentication service and store, which are 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 files.

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

3. In both files, 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure the password expiry notification period

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.

1. On the primary StoreFront server in your deployment, 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To disable file type association

By default, file type association is enabled in stores so that content is seamlessly redirected to users' subscribed applications when they open local files of the appropriate types. To disable file type association, you edit the store configuration file.

1. On the primary StoreFront server in your deployment, 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To enable socket pooling

Socket pooling is disabled by default in stores. When socket pooling is enabled, StoreFront maintains a pool of sockets, rather than creating a socket each time one is needed and returning it to the operating system when the connection is closed. Enabling socket pooling enhances performance, particularly for Secure Sockets Layer (SSL) connections. To enable socket pooling, you edit the store configuration file.

1. On the primary StoreFront server in your deployment, 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To customize the Citrix Receiver logon dialog box

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.

1. On the primary StoreFront server in your deployment, use a text editor to open the Authenticate.aspx file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication\Views\ExplicitForms\ directory.

2. Locate the following lines in the file.

   ```
   <%-- Html.RenderPartial("LabelRequirement",
               new FormsViewLabel{Text = Localise(ExplicitMessages.AuthenticateHeadingKey),
                           Type = FormsElements.LabelTypeHeading}); --%>
   ```

3. Uncomment the statement by removing the leading and trailing double hyphens, as shown below.

   ```
   <% Html.RenderPartial("LabelRequirement",
               new FormsViewLabel{Text = Localise(ExplicitMessages.AuthenticateHeadingKey),
                           Type = FormsElements.LabelTypeHeading}); %>
   ```

   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.

   ```
   <data name="AuthenticateHeadingText" xml:space="preserve">
     <value>Please log on</value>
   </data>
   ```

6. 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.

   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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations

of the secondary servers are also updated.

To prevent Receiver for Windows from caching passwords

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.

1. On the primary StoreFront server in your deployment, use a text editor to open the Authenticate.aspx file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication\Views\ExplicitForms\ directory.

2. Locate the following line in the file.

   ```
   <% Html.RenderPartial("SaveCredentialsRequirement",
              SaveCredentials); %>
   ```

3. Comment the statement by adding leading and trailing double hyphens, as shown below.

   ```
   <%-- Html.RenderPartial("SaveCredentialsRequirement",
               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).

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure Receiver for Web sites using the configuration files

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

- To configure how resources are displayed for users
- To make Citrix Receiver installation files available on the server
- To disable detection and deployment of Citrix Receiver
- To configure workspace control
- To stop offering provisioning files to users
- To configure Receiver for HTML5 use of browser tabs
- To configure store time-out duration and retry attempts
- To configure session duration

To configure how resources are displayed for users

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.

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.

1. On the primary StoreFront server in your deployment, 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.

   <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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To make Citrix Receiver installation files available on the server

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.

1. On the primary StoreFront server in your deployment, 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*storename*Web\ 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To disable detection and deployment of Citrix Receiver

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.

1. On the primary StoreFront server in your deployment, 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.

   <pluginAssistant enabled="true" ... >

3. Change the value of the enabled attribute to false to disable detection and deployment of Citrix Receiver for the site.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure workspace control

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.

1. On the primary StoreFront server in your deployment, 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.

   ```
   <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

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To stop offering provisioning files to users

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.

1. On the primary StoreFront server in your deployment, 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.

   ```
   <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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure Receiver for HTML5 use of browser tabs

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.

1. On the primary StoreFront server in your deployment, 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.

   <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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure store time-out duration and retry attempts

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.

1. On the primary StoreFront server in your deployment, 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.

   <communication attempts="2" timeout="00:01:00">

3. Change the value of the attempts attribute to the 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure session duration

Once authenticated, users can, by default, access XenDesktop, XenApp, App Controller, 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.

1. On the primary StoreFront server in your deployment, 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.

   <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, App Controller, 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.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Configure Desktop Appliance sites

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, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To create or remove Desktop Appliance sites

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. On the primary StoreFront server in your deployment, use an account with administrator permissions to start Windows PowerShell.

2. 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\.

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

   Install-DSDesktopAppliance -FriendlyName *sitename* -SiteId *iisid*
   -VirtualPath *sitepath* -HostBaseUrl *baseurl* -UseHttps {$False | $True}
   -StoreUrl *storepath* [-EnableMultiDesktop {$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 *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 *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. The variable *baseurl*, specifies the URL of your StoreFront server or the load balancing environment for a multiple server deployment.

   Indicate whether StoreFront is configured for HTTPS by setting -UseHttps to the appropriate value. Ensure that the -UseHttps setting is consistent with the protocol in the URL specified for -HostBaseURL. Use *storepath* to specify the relative path in IIS to the store providing the resources for the site, for example, /Citrix/Store.

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.

4. 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.

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

   Get-DSDesktopAppliancesSummary

To configure user authentication

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. On the primary StoreFront server in your deployment, 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*storename*DesktopAppliance 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.

To enable users to choose between multiple desktops

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. On the primary StoreFront server in your deployment, 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*storename*DesktopAppliance 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.

To configure authentication for XenApp Services URLs

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.

1. On the primary StoreFront server in your deployment, use an account with local administrator permissions to start Windows PowerShell.

2. At a command prompt, type the following command to configure the user authentication method for users accessing the store through the XenApp Services URL.

   & "*installationlocation*\Scripts\EnablePnaForStore.ps1" –SiteId *iisid* –ResourcesVirtualPath *storepath* –LogonMethods {prompt | sson | smartcard_sson}

   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 -LogonMethods argument to prompt. For domain pass-through, use sson and for pass-through with smart card authentication, set the argument to smartcard_sson.

Important: In multiple server deployments, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

Secure your StoreFront deployment

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

Certificates in 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 either a certificate with a Subject or Subject Alternative Name entry of **discoverReceiver.*domain*** (where *domain* is the domain containing your users' email accounts), or a wildcard certificate for the domain containing your users' email accounts. 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.

StoreFront communications

In a production environment, Citrix recommends using the Internet Protocol security (IPsec) or HTTPS protocols to secure data passing between StoreFront and your servers. IPsec is a set of standard extensions to the Internet Protocol that provides authenticated and encrypted communications with data integrity and replay protection. Because IPsec is a network-layer protocol set, higher level protocols can use it without modification. HTTPS uses the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to provide strong data encryption.

The SSL Relay can be used to secure data traffic between StoreFront and 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

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.

StoreFront security separation

If you deploy any web applications in the same web domain (domain name and port) as StoreFront, then any security risks in those web applications could potentially reduce the security of your StoreFront deployment. Where a greater degree of security separation is required, Citrix recommends that you deploy StoreFront in a separate web domain.

ICA file signing

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

User change password

You can enable Receiver for Web site users logging on with Microsoft 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 StoreFront

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, ensure that any configuration changes you make on the primary server are propagated to the server group so that the configurations of the secondary servers are also updated.

To configure log throttling

1. On the primary StoreFront server in your deployment, 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*storename*Web\ directories, respectively, where *storename* is the name specified for the store when it was created.

2. Locate the following element in the file.

   <logger duplicateInterval="00:01:00" duplicateLimit="10">

   By default, StoreFront is configured to limit the number of duplicate log entries to 10 per minute.

3. Change the value of the duplicateInterval attribute to the set the time period in hours, minutes, and seconds over which duplicate log entries are monitored. Use the duplicateLimit attribute to set the number of duplicate entries that must be logged within the specified time interval to trigger log throttling.

When log throttling is triggered, a warning message is logged to indicate that further identical log entries will be suppressed. Once the time limit elapses, normal logging resumes and an informational message is logged indicating that duplicate log entries are no longer being suppressed.

To enable tracing

1. On the primary StoreFront server in your deployment, use an account with local administrator permissions to start Windows PowerShell.

2. At a command prompt, type the following commands to enable tracing.

   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Verbose

3. To disable tracing, type the following commands.

   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Off

   Due to the large amount of data that potentially can be generated, tracing may significantly impact the performance of StoreFront. Accordingly, Citrix recommends that you disable tracing unless it is specifically required for troubleshooting.

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