StoreFront 1.2

2014-11-09 04:44:01 UTC

Contents

StoreFront 1.2

Citrix StoreFront authenticates users to XenDesktop sites, XenApp farms, and AppController, enumerating and aggregating available desktops and applications into stores that users access through Citrix Receiver or Receiver for Web sites. The StoreFront database records details of users' application subscriptions to enable synchronization of those applications across all their devices.

The topics in this section provide information about deploying, configuring, and managing StoreFront. Readers are assumed to be familiar with XenDesktop, XenApp, and AppController.

About StoreFront	Planning Your StoreFront Deployment
Known Issues in StoreFront 1.2	Installing and Setting Up StoreFront
System Requirements for StoreFront 1.2	Managing Your StoreFront Deployment

About StoreFront

StoreFront provides authentication and resource delivery services for Citrix Receiver.

- The StoreFront authentication service authenticates users to XenDesktop sites, XenApp farms, and AppController. When a user's credentials have been validated, the authentication service handles all subsequent interactions to ensure that the user only needs to log on once.
- StoreFront stores enumerate and aggregate the desktops and applications currently available from XenDesktop sites, XenApp farms, and AppController. Users access stores through Citrix Receiver or a Receiver for Web site.
- Receiver for Web sites enable users to access StoreFront stores through a Web page. To access their desktops and applications, users require a compatible version of Citrix Receiver. For users running Windows or Mac OS X, Receiver for Web sites attempt to determine whether Citrix Receiver is installed and, if a suitable client cannot be detected, users are prompted to download and install Citrix Receiver.
- The StoreFront database records details of users' application subscriptions, plus associated shortcut names and locations. When a user accesses a store, the application synchronization feature automatically updates the subscribed applications on the user device to match the configuration stored in the StoreFront database, ensuring users have a consistent experience across all their devices.

You manage the StoreFront components with the Citrix StoreFront management console. If you want to perform certain advanced administration tasks, you might also need to edit the StoreFront configuration files.

What's New

Separate desktop and application views. When both desktops and applications are available from a site, Receiver for Web displays separate desktop and application views with behavior that is tailored to the types of resources being delivered. For more information, see Optimize the user experience.

Receiver for HTML5 integration. Install Receiver for HTML5 on your StoreFront servers to enable users with compatible browsers to access applications on Receiver for Web sites using Receiver for HTML5. For more information, see Receiver for HTML5.

Streamlined initial configuration. The StoreFront initial configuration process has been refined to enable you to create a store complete with a Receiver for Web site and remote access through a single, wizard-driven procedure. For more information, see Installing and Setting Up StoreFront.

SmartAccess support. For users connecting to StoreFront through Access Gateway Enterprise Edition, you can use SmartAccess to control user access to XenDesktop and XenApp resources on the basis of Access Gateway session policies. For more information, see User Authentication.

Other Features

High availability. You can group your StoreFront servers for increased scalability and fault tolerance. For more information, see Planning Your StoreFront Deployment.

Application synchronization. Subscribed applications follow users from device to device so that they do not need to subscribe to the same applications each time they use a different device. For more information, see Planning Your StoreFront Deployment.

Automatically provisioned applications. You can automatically subscribe all users to a core set of applications. For more information, see Integrating StoreFront into Your Environment.

Known Issues in StoreFront 1.2

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

Receiver for Web site Logon screen may 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]

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

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

Users cannot log on to Receiver for Web sites after enabling explicit authentication

If you create a Receiver for Web site for a store that uses an authentication service for which explicit authentication is disabled and you subsequently enable explicit authentication, users cannot log on to the site. To resolve this issue, restart Microsoft Internet Information Services (IIS) on the server hosting the Receiver for Web site. [#275275]

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

If you disable the Pass-through from Citrix Access Gateway authentication method, users cannot access their resources through Access Gateway even if the store is configured for remote access. Instead, users receive the error message "Unable to launch your application. Contact your help desk with the following information: Cannot connect to the Citrix XenApp server. Protocol Driver error." To resolve this issue, set the value of the requireTokenConsistency attribute to false in the store configuration file if you disable the Pass-through from Citrix Access Gateway authentication method. [#320650]

Users' desktops may be disconnected when logging on to a Receiver for Web site twice

Users logging on from two different devices to a Receiver for Web site from which both applications and more than one desktop are available may find that their desktops are disconnected on the first device when they log on using the second device. To work around this issue, set the value of the autoReconnectAtLogon attribute to false in the site configuration file. For more information on configuring workspace control for Receiver for Web sites, see Configuring Receiver for Web Using the Configuration Files. [#322168]

StoreFront configuration files appear unsynchronized when no changes have been made

In multiple server deployments, clicking OK in the Citrix StoreFront management console without changing any settings updates the configuration files for the selected

authentication service, store, or Receiver for Web site. This results in the configuration files becoming unsynchronized across the server group. To work around this issue, after clicking OK in the Citrix StoreFront management console, use the Propagate Changes task to update the configuration of all the other servers in the deployment. For more information, see Configuring Server Groups. [#324509]

System Requirements for StoreFront 1.2

This topic lists the supported Citrix product versions and platform requirements for installing StoreFront, and the requirements for users to access StoreFront stores. It is assumed that all computers meet the minimum hardware requirements for the installed operating system.

Citrix Server Requirements

StoreFront can be used with the following product versions.

- AppController
  - Citrix AppController 2.0
  - Citrix AppController 1.1
  - Citrix AppController 1.0
- XenDesktop
  - Citrix XenDesktop 5.6
  - Citrix XenDesktop 5.5
  - Citrix XenDesktop 5.0
  - Citrix XenDesktop 4.0
- XenApp
  - Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2
  - Citrix XenApp 6.0 for Microsoft Windows Server 2008 R2
  - Citrix XenApp 5.0, with Feature Pack 3, for Microsoft Windows Server 2008 x64 Edition
  - Citrix XenApp 5.0, with Feature Pack 3, for Microsoft Windows Server 2008
  - Citrix XenApp 5.0, with Feature Pack 3, for Microsoft Windows Server 2003 x64 Edition
  - Citrix XenApp 5.0, with Feature Pack 3, for Microsoft Windows Server 2003
  - Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2008 x64 Edition
  - Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2008
  - Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003 x64 Edition

    - Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003
    - Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003 x64 Edition
    - Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003
    - Citrix XenApp 5.0 for Microsoft Windows Server 2008 x64 Edition
    - Citrix XenApp 5.0 for Microsoft Windows Server 2008
    - Citrix XenApp 5.0 for Microsoft Windows Server 2003 x64 Edition
    - Citrix XenApp 5.0 for Microsoft Windows Server 2003
- VDI-in-a-Box
    - VDI-in-a-Box 5.2

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.

- Citrix Merchandising Server 2.2
- Citrix Merchandising Server 2.1

For more information, see Configuring Authentication.

Access Gateway Requirements

StoreFront enables user access to desktops and applications from public networks with the following versions of Access Gateway.

- Citrix Access Gateway 10
- Citrix Access Gateway 9.3, Enterprise Edition
- Citrix Access Gateway 5.0.4

Web Server Requirements

StoreFront is only supported for installation on Windows Server 2008 R2 with Service Pack 1. Microsoft Internet Information Services 7.5 and Microsoft .NET Framework 3.5 with Service Pack 1 are required on the Web server. If either of these prerequisites are installed but not enabled, the StoreFront installer enables them before installing the product.

In addition, Windows PowerShell 2.0 and Microsoft Management Console 3.0, which are both default components of Windows Server 2008 R2, must be installed on the Web server before you can install StoreFront.

Citrix recommends that you use a server with at least 2 GB of RAM to host StoreFront.

Database Requirements

StoreFront requires a Microsoft SQL Server database to provide the application synchronization feature. If a suitable database is not available, either locally or on another server in the same Active Directory forest, you cannot create StoreFront stores. StoreFront supports the following versions of SQL Server.

- Microsoft SQL Server 2012 Express
- Microsoft SQL Server 2008 R2 Enterprise
- Microsoft SQL Server 2008 R2 Express

User Device Requirements

To access their desktops and applications, all users require a Citrix client. Citrix Receiver users can either access stores directly through Citrix Receiver or they can use a Web browser to log on to a Receiver for Web site for the store. Additionally, limited support with reduced functionality is available for clients that can connect to Web Interface XenApp Services sites.

The following Citrix Receiver versions can be used to access StoreFront stores directly. Connections through Access Gateway can be made using both the Access Gateway Plug-in and clientless access.

Client	Connect from local network	Connect through Access Gateway
Citrix Receiver for Windows 3.3	Yes	Yes
Citrix Receiver for Windows 3.2	Yes	Yes
Citrix Receiver for Windows 3.1	Yes	Yes
Citrix Receiver for Mac 11.6	Yes	Yes
Citrix Receiver for Mac 11.5	Yes	Yes
Citrix Receiver for iOS 5.6	Yes	Yes
Citrix Receiver for iOS 5.5	Yes	No
Citrix Receiver for Android 3.1	Yes	Yes

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

Client	Operating system	Browser

Citrix Receiver for Windows 3.3	Windows 7 64-bit Editions with Service Pack 1 Windows 7 32-bit Editions with Service Pack 1	Internet Explorer 9 (32-bit mode) Internet Explorer 8 (32-bit mode) Mozilla Firefox 13 Mozilla Firefox 12 Google Chrome 19 Google Chrome 18
	Windows Vista 64-bit Editions with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows XP Professional x64 Edition with Service Pack 2 Windows XP Professional with Service Pack 3	Internet Explorer 8 (32-bit mode)
Citrix Receiver for Mac 11.6	Mac OS X 10.7 Lion	Safari 5.1 Mozilla Firefox 13 Google Chrome 19
	Mac OS X 10.6 Snow Leopard	Safari 5.0 Mozilla Firefox 13 Google Chrome 19

The following clients can be used to access StoreFront stores with reduced functionality through XenApp Services URLs. For more information, see User Access Options. Connections through Access Gateway can be made using both the Access Gateway Plug-in and clientless access.

Client	Connect from local network	Connect through Access Gateway
Citrix Receiver for Windows 3.0	Yes	Yes
Citrix Online Plug-in for Windows 12.1	Yes	Yes
Citrix Online Plug-in for Windows 12.0	Yes	Yes
Citrix Receiver for Mac 11.4	Yes	Yes
Citrix Online Plug-in for Macintosh 11.2	Yes	Yes

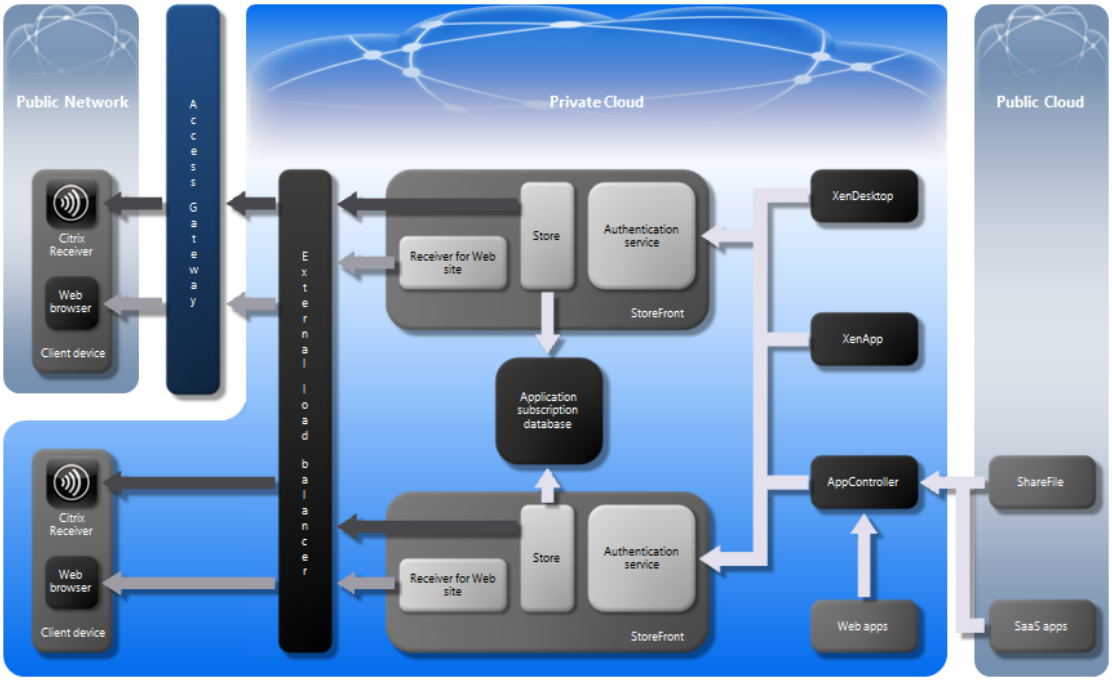
Citrix Receiver for Linux 12.1	Yes	No
Citrix Receiver for Linux 12.0	Yes	No
Citrix Receiver for iOS 5.0.2	Yes	Yes

If you plan to deliver offline applications to users, the Citrix Offline Plug-in is required in addition to Citrix 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.

Planning Your StoreFront Deployment

StoreFront employs Microsoft .NET technology running on Microsoft Internet Information Services (IIS) along with Microsoft SQL Server to provide authentication and resource delivery services for Citrix Receiver. StoreFront integrates with your XenDesktop, XenApp, and CloudGateway Enterprise deployments, providing users with a single, self-service access point for their desktops, applications, and data.

The figure shows the components in a typical multiple server StoreFront deployment.



StoreFront Components

The following services provide the functionality of StoreFront.

- **Authentication service**—authenticates users to XenDesktop sites, XenApp farms, and AppController, handling all interactions to ensure that users only need to log on once.
- **Store**—retrieves user credentials from the authentication service to authenticate users to the infrastructure providing the resources. Enumerates the available resources and sends the details to Citrix Receiver.
- **Receiver for Web site**—enables users to access stores through a Web page.
- **Application subscription database**—stores details of user subscriptions, plus associated shortcut names and locations.

Three of the core components of StoreFront, the authentication service, the stores, and the Receiver for Web sites, run on IIS. The other main component, the application subscription database, requires SQL Server. StoreFront can be configured either in standalone mode, with all the components installed on a single server, or as a multiple server deployment. For single-server deployments, SQL Server must be installed locally on the StoreFront server. In multiple server environments, the application subscription database can be hosted on one of the StoreFront servers or on a dedicated database server.

StoreFront servers and the application subscription database must reside within the same Active Directory forest as the XenDesktop and XenApp servers hosting users' resources. For multiple server deployments, all the StoreFront servers in the group must reside within the same domain.

Other Citrix Components

The following Citrix products and technologies integrate with StoreFront to enable you to deliver resources to your users.

- **Citrix Receiver**—enables users to access their desktops, applications, and data from any device. Citrix Receiver provides users with a consistent experience across all their devices, with resources following them from device to device.

- **XenDesktop/XenApp**—provide desktops, content, and online and offline applications for users. XenDesktop and XenApp enable you to virtualize and deliver desktops and applications as an on-demand service.

- **AppController**—extends user identities to Web applications and software-as-a-service (SaaS) solutions, and enables centralized management of native mobile applications and ShareFile data. AppController provides pass-through authentication for users to Web applications hosted on your internal network and to software-as-a-service (SaaS) applications provided by third parties over public networks. You can also use AppController to configure role-based management and delivery of native mobile applications and ShareFile data, allowing ShareFile documents to follow users from device to device.

- **ShareFile**—enables users to securely access, share, and synchronize files and data on multiple devices. Integration with CloudGateway enables you to configure pass-through authentication to ShareFile for users.

- **Access Gateway**—secures user connections to StoreFront stores and Receiver for Web sites over public networks. Access Gateway enables remote users to access their desktops, applications, and data securely, while providing you with granular control over access to internal resources.

Third-Party Components

The following third-party products integrate with your StoreFront deployment to provide additional functionality.

- **External load balancer**—provides for failover between servers and balances server loads in a multiple server StoreFront deployment.

- **Web apps**—applications accessed through a Web browser and hosted on the internal network.
- **SaaS apps**—Web applications hosted externally by third parties and delivered over public networks.

Recommendations

When planning your StoreFront deployment, consider the following recommendations.

- In a production environment, Citrix recommends using HTTPS to secure communications between StoreFront and users' devices. To use HTTPS, StoreFront requires that the IIS instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.
- Citrix recommends that you back up the application subscription database regularly so that you can restore from the backup if the database fails.
- Consider implementing database mirroring or clustering to enable automatic failover and provide high availability of the application subscription database.
- To configure a multiple server deployment for high availability, install your StoreFront servers within a load-balanced environment. Configure the external load balancer for failover between servers to provide a fault-tolerant deployment.

User Access Options

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

Direct Store Access

Users with compatible versions of Citrix Receiver can access StoreFront stores directly within the Citrix Receiver user interface. Accessing stores directly from Citrix Receiver provides the best user experience and the greatest functionality. For the Citrix Receiver versions that can be used to access stores directly, see System Requirements for StoreFront 1.2.

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.

- **Email-based account discovery.** You can configure Service Location (SRV) locator resource records for Access Gateway or StoreFront on your Active Directory Domain Name System (DNS) server to enable Citrix Receiver to locate available stores on the basis of users' email addresses. Users do not need to know the access details for their stores, instead they enter their email addresses during initial Citrix Receiver configuration. 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 Configuring Email-Based Account Discovery.

- **Provisioning files.** You can provide users with provisioning files containing connection details for their stores. After installation, users open the file to configure Citrix Receiver automatically. By default, Receiver for Web sites offer users a provisioning file for the single store for which the site is configured. Alternatively, you can use the Citrix StoreFront management console to generate provisioning files for single or multiple stores that you can manually distribute to your 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 installation, users click on the URL to configure Citrix Receiver automatically. Enter details of your deployment into the tool and generate a URL that you can manually 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 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, users cannot set up accounts manually and must use one of the alternative methods above. For more information, see the Citrix Receiver documentation.

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 created for the store by default. To access their desktops and applications through Receiver for Web sites, users also require a compatible version of Citrix Receiver. For the Citrix Receiver and Web browser combinations that can be used to access Receiver for Web sites, see System Requirements for StoreFront 1.2.

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. For more information, see Configuring Receiver for Web Using the Configuration Files.

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.

Users accessing stores through a Receiver for Web site benefit from many of the features available with direct store access through Citrix Receiver, such as application synchronization, but with the following exceptions.

- Only a single store can be accessed through each Receiver for Web site.
- Receiver for Web sites do not support domain pass-through authentication.
- Receiver for Web sites cannot initiate SSL virtual private network (VPN) connections. Users logging on through Access Gateway without a VPN connection cannot access Web applications for which AppController requires that such a connection is used.
- Subscribed applications are not available in the Start menu 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.
- Receiver for Web sites do not support offline applications.
- Receiver for Web sites do not support applications to which users need to request access before subscribing.
- Receiver for Web sites do not support Citrix Online products integrated into stores. Citrix Online products must be delivered with AppController or made available as XenApp hosted applications to enable access through Receiver for Web sites.

XenApp Services URLs

Users with older Citrix clients that support Web Interface XenApp Services sites can access stores directly by configuring their clients with the XenApp Services URL for the store. When you create a new store, the XenApp Services URL for the store is enabled by default. For the clients that can be used to access stores through XenApp Services URLs, see System Requirements for StoreFront 1.2.

User access to stores through XenApp Services URLs is subject to the following limitations.

- The XenApp Services URL for the store cannot be modified.
- Modifying XenApp Services settings by editing the configuration file, config.xml, is not supported.
- Workspace control is not supported.
- User requests to change their passwords are routed to the domain controller directly through the XenDesktop sites or XenApp farms providing desktops and applications for the store, bypassing the StoreFront authentication service.

Configuring Email-Based Account Discovery

During initial configuration, Citrix Receiver can contact Active Directory Domain Name System (DNS) servers to obtain details of the stores available for users. This means that users do not need to know the access details for their stores when they install and configure Citrix Receiver. Instead, users enter their email addresses and Citrix Receiver contacts the DNS server for the domain specified in the email address to obtain the required information. Users are presented with a list of the available stores from which to select.

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

You must install a valid server certificate on the Access 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 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 local network, you must also configure Access 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 menu, click Administrative Tools > 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, click in the Service box and enter the host value _citrixreceiver.

5. Click in the Protocol box and enter the value _tcp.

6. In the Host offering this service box, specify the fully qualified domain name (FQDN) and port for your Access Gateway appliance (to support both local and remote users) or StoreFront server (to support users on the local network 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 FQDN on your internal DNS server and another record on your external server specifying the Access Gateway FQDN. With this configuration, users on the local network are provided with the StoreFront details, while remote users receive Access Gateway connection information.

   Note: Your StoreFront FQDN must be unique and different from the Access Gateway virtual server FQDN. Using the same FQDN for StoreFront and the Access Gateway virtual server is not supported. Citrix Receiver requires that the StoreFront FQDN is a unique address that is only resolvable from user devices connected to the internal network. If this is not the case, Receiver for Windows users cannot use email-based account discovery.

7. If you configured a SRV record for your Access Gateway appliance, add the StoreFront connection details to Access Gateway in a session profile or global setting.

User Authentication

Local Users

StoreFront supports the following authentication methods for local users on the internal network.

- **User name and password.** Users enter their credentials when they access their stores.
- **Domain pass-through.** Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores. To use this option, users require Receiver for Windows. Pass-through authentication must be enabled when Receiver for Windows is installed on users' devices.

For more information about configuring user authentication in StoreFront, see Configuring the Authentication Service.

Remote Users

Deploy Access Gateway to secure connections to StoreFront stores and Receiver for Web sites from remote users over public networks. For more information about configuring StoreFront for Access Gateway, see To add an Access Gateway connection. For more information about setting up Access Gateway to connect to StoreFront, see Integrating Access Gateway with CloudGateway.

When deployed with Access Gateway Enterprise Edition, StoreFront supports the following authentication methods for remote users.

- **Security token.** Users log on to Access 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 log on to Access Gateway with user names, passwords, and security token passcodes.
- **Client certificate.** Users log on to Access Gateway and are authenticated based on the attributes of the client certificate presented to Access Gateway. Client certificate authentication can also be used with other authentication types to provide double-source authentication.

StoreFront uses the Access Gateway authentication service to provide pass-through authentication for remote users so that they only need to enter their credentials once. For more information about configuring StoreFront for pass-through authentication from Access Gateway, see Configuring the Authentication Service.

Users can connect to stores directly with pass-through authentication through an SSL virtual private network (VPN) tunnel using the Access Gateway Plug-in. Remote users who cannot install the Access Gateway Plug-in can use clientless access to connect to stores directly with pass-through authentication. To use clientless access to connect directly 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 Access Gateway to act as a secure remote proxy. Users log on to Access Gateway directly and use the Receiver for Web site to access their applications without needing to authenticate again. For more information about configuring Access Gateway as a remote proxy, see Creating and Applying Web and File Share Links.

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

For users connecting to StoreFront through Access Gateway Enterprise Edition, you can use SmartAccess to control user access to XenDesktop and XenApp resources on the basis of Access Gateway session policies. For more information about Smart Access, see Configuring SmartAccess on Access Gateway Enterprise Edition.

Note: Your StoreFront fully qualified domain name (FQDN) must be unique and different from the Access Gateway virtual server FQDN. Using the same FQDN for StoreFront and the Access Gateway virtual server is not supported. Citrix Receiver requires that the StoreFront FQDN is a unique address that is only resolvable from user devices connected to the internal network. If this is not the case, Receiver for iOS users experience connectivity issues and Receiver for Windows users cannot use email-based account discovery.

Optimize the user experience

StoreFront includes features designed to enhance the user experience. These features are enabled by default when you create new stores and Receiver for Web sites.

Receiver for Web desktop and application views

When both desktops and applications are available from a site, Receiver for Web 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 site, if only a single desktop is available for a user, Receiver for Web starts that desktop automatically when the user logs on. You can configure which views appear for your sites and prevent Receiver for Web from automatically starting desktops for users. For more information, see Configuring Receiver for Web Using the Configuration Files.

The behavior of the Receiver for Web views 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 to enable users to restart their desktops are provided on the desktop view. If users have access to multiple instances of a desktop from a single desktop group, Receiver for Web distinguishes the desktops for users by appending a numerical suffix to the desktop name.

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. For more information, see Applications and desktop groups. File type association is enabled by default for StoreFront stores. For more information about disabling file type association, see Configuring StoreFront Using the Configuration Files.

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 and is configured to automatically reconnect users logging on to the site to any applications that they left running. This configuration enables a user to log on to a site, start their applications, and 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 automatically disconnected when the user logs off from that site,

provided that the same browser is used to log on, start the resources, and log off. For more information about configuring workspace control, see Configuring Receiver for Web Using the Configuration Files.

Workspace control on Receiver for Web sites is subject to the following requirements and limitations.

- Workspace control is not available when Receiver for Web sites are accessed from hosted desktops and applications.
- For users accessing Receiver for Web sites through Internet Explorer, workspace control is only enabled if the site can detect that Citrix Receiver is installed on users' devices.
- 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.
- 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.

Additional recommendations

When publishing applications, consider the following options to enhance the experience for users accessing the applications through StoreFront stores.

- Consider organizing XenDesktop 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 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. For more information about application folders, see To create an application.
- Ensure that you include meaningful descriptions for published applications, as these descriptions are visible to users in Citrix Receiver. For more information about including descriptions when publishing XenDesktop applications, see To create an application.
- You can automatically subscribe all users of a store to a XenDesktop application by appending the string KEYWORDS:Auto to the description you provide when you publish the application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
- To automatically subscribe all users of a store to a web or software-as-a-service (SaaS) application managed by AppController, select the App is available in Receiver to all users automatically check box when you configure the application settings. For more information, see To configure settings to create user accounts.
- 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; for example, KEYWORDS:Auto Featured.

- By default, XenDesktop hosted shared desktops are treated like other virtual desktops by Receiver for Web. To change this behavior, append the string KEYWORDS:TreatAsApp to the desktop description. The desktop is displayed in the application view rather than the desktop view and users must subscribe to the desktop before they can access it. In addition, the desktop is not automatically started when the user logs on to the site and is not accessed with the Desktop Viewer, even if Receiver for Web is configured to do this for other desktops.

Installing and Setting Up StoreFront

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

1. If you plan to use StoreFront to deliver XenDesktop and XenApp resources to users, join the StoreFront server to a domain within the Active Directory forest that contains your XenDesktop sites and XenApp farms.

2. Ensure that a Microsoft SQL Server database is available in your environment.

   If you plan to configure a single-server deployment, SQL Server must be installed locally on the StoreFront server. In the case of multiple server deployments, SQL Server can either be installed on one of the StoreFront servers or on another server in the same Active Directory forest. For more information about installing SQL Server, see http://technet.microsoft.com/en-us/library/bb500469.aspx.

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

4. Optionally, install the .NET Framework 3.5.1 Features > .NET Framework 3.5.1 feature and the Web Server (IIS) role on the StoreFront server, enabling the following role services and their dependencies.

   - Web Server > Common HTTP Features > Static Content, Default Document, HTTP Errors, HTTP Redirection
   - Web Server > Application Development > ASP.NET, .NET Extensibility, ISAPI Extensions, ISAPI Filters
   - Web Server > Health and Diagnostics > HTTP Logging
   - Web Server > Security > Windows Authentication, Request Filtering
   - Management Tools > IIS Management Console, IIS Management Scripts and Tools
   - Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools

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

5. Optionally, use the Internet Information Services (IIS) Manager console on the StoreFront server to create a server certificate signed by your domain certificate authority. For more information, see http://technet.microsoft.com/en-us/library/cc731014(WS.10).aspx.

6. If you installed a server certificate on the StoreFront server, add HTTPS binding to the default Web site. For more information, see http://technet.microsoft.com/en-us/library/cc731692(WS.10).aspx.

7. Install StoreFront.

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

To install StoreFront

If you plan to use StoreFront to deliver XenDesktop and XenApp resources to users, ensure that the StoreFront server is joined to a domain within the Active Directory forest containing your XenDesktop and XenApp servers before starting the installation. In addition, ensure that a Microsoft SQL Server database is available in your environment. For single-server deployments, SQL Server must be installed locally on the StoreFront server. In the case of multiple server deployments, SQL Server can either be installed on one of the StoreFront servers or on another server in the same Active Directory forest. If you plan to configure a multiple server deployment, set up a load balancing environment for your StoreFront servers.

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. If a message appears indicating that Microsoft .NET Framework 3.5 with Service Pack 1 will be enabled, 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 that all three StoreFront components are listed for installation and click Install.

   Before the components are installed, the .NET Framework 3.5.1 Features > .NET Framework 3.5.1 feature and the Web Server (IIS) role are deployed, and the following role services are enabled if they are not already configured on the server.

   - Web Server > Common HTTP Features > Static Content, Default Document, HTTP Errors, HTTP Redirection
   - Web Server > Application Development > ASP.NET, .NET Extensibility, ISAPI Extensions, ISAPI Filters
   - Web Server > Health and Diagnostics > HTTP Logging
   - Web Server > Security > Windows Authentication, Request Filtering
   - Management Tools > IIS Management Console, IIS Management Scripts and Tools
   - Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools
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 from a command prompt

If you plan to use StoreFront to deliver XenDesktop and XenApp resources to users, ensure that the StoreFront server is joined to a domain within the Active Directory forest containing your XenDesktop and XenApp servers before starting the installation. In addition, ensure that a Microsoft SQL Server database is available in your environment. For single-server deployments, SQL Server must be installed locally on the StoreFront server. In the case of multiple server deployments, SQL Server can either be installed on one of the StoreFront servers or on another server in the same Active Directory forest. If you plan to configure a multiple server deployment, set up a load balancing environment for your StoreFront servers.

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

   CitrixStoreFront-x64.exe [-silent]

   Use the -silent argument to perform a silent installation of StoreFront and all the prerequisites.

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-12/dws-first-auth-store.html

To deploy a single server

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, click Start > All Programs > Citrix > Citrix StoreFront.

2. In the results pane of the Citrix StoreFront management console, click Deploy a single server.

   Note: The Citrix StoreFront management console checks whether Microsoft SQL Server is installed on the server and, if it is not, the option to deploy a single server is unavailable. A locally installed database is required for single-server StoreFront deployments.

3. Specify the base URL to be used to access the StoreFront services and then click Create to set up the authentication service, which authenticates users to XenDesktop sites, XenApp farms, and AppController.

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

   StoreFront stores enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users.

5. On the Delivery Controllers page, list the XenDesktop, XenApp, and CloudGateway Enterprise deployments providing the resources that you want to make available in the store. Click Add.

6. 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 through the store are provided by CloudGateway Enterprise (through AppController), XenApp, or XenDesktop.

7. If you are configuring a XenDesktop site or XenApp farm, continue to Step 9. To make applications managed by CloudGateway Enterprise available in the store, enter the name or IP address of an AppController virtual appliance in the Server box and specify the port for StoreFront to use for connections to AppController. The default port is 443.

8. If you manage user access to ShareFile through AppController, select the Data provisioning check box to enable synchronization of users' ShareFile data and documents across all their devices. Continue to Step 13.

9. To make desktops and applications provided by a XenDesktop site or XenApp farm available in the store, add the names or IP addresses of XenDesktop controllers or XenApp servers running the Citrix XML Service to the Servers list. Specify multiple servers in a site or farm to enable fault tolerance, listing the entries in order of priority to set the failover sequence.

10. 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 the XenDesktop site or XenApp farm.

- To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select HTTPS. If you select this option, ensure that the Citrix XML Service on your servers is set to share its port with IIS and that IIS is configured to support HTTPS.

- To send data over secure connections to XenApp servers only, 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 XenDesktop sites or XenApp farms, ensure that the server names you specify in the Servers list match exactly (including the case) the names on the certificates for the servers.

11. Specify the port for StoreFront to use for connections to the XenDesktop site or XenApp farm. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service.

12. If you are using the SSL Relay to secure connections between StoreFront and a XenApp farm, 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.

13. Click OK. Repeat Steps 5 to 13, as necessary, to list additional XenDesktop, XenApp, and CloudGateway Enterprise deployments on the Delivery Controllers page. Click Next.

14. On the Remote Access page, specify whether and how users connecting from public networks can access the store through Access 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. If you select this option, continue to Step 26.

    - To make only resources available through the store available to users on public networks through Access Gateway, select No VPN tunnel. Users log on directly to Access Gateway and do not need to use the Access Gateway Plug-in.

    - To make the store and other resources on the internal network available to users on public networks through an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the Access Gateway Plug-in to establish the VPN tunnel.

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

15. If you enabled remote access, list the Access Gateway deployments through which users access the store. Click Add.

16. On the Gateway Settings page, specify a name for the Access Gateway deployment that will help users to identify it.

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

17. Enter the URL of the user logon point or virtual server for your Access Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone Access Gateway appliance or an Access Controller server that is part of an Access Gateway cluster.

18. Unless you are configuring remote access through an Access Gateway Enterprise Edition deployment, click Next and continue to Step 20. For Access Gateway Enterprise Edition deployments, select the Set server as Access Gateway Enterprise Edition check box and specify the subnet IP address of the Access Gateway appliance.

    The subnet address is the IP address that Access Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Access Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

19. Select from the Logon type list the authentication method used for Citrix Receiver users accessing their desktops and applications through Access Gateway Enterprise Edition. Click Next.

    - If users are not required to authenticate, select No Authentication.
    - If users are required to enter their domain credentials, select Domain only.
    - If users are required to enter a tokencode obtained from a security token, select Security token only.
    - 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.

20. If you are configuring StoreFront for an Access Gateway cluster, list on the Appliances page the IP addresses or fully qualified domain names of the Access Gateway appliances in the cluster and click Next.

21. On the Enable Silent Authentication page, specify the URL for an appliance running the Access Gateway authentication service. For Access Gateway clusters, enter URLs for multiple Access Controller servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

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

22. On the Secure Ticket Authority (STA) page, specify the URL for a server running the STA. Enter URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

    The STA can be hosted by the Citrix XML Service and issues session tickets in response to requests for connections to XenDesktop sites and XenApp farms. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.

23. If you want XenDesktop and XenApp 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.

24. Click Create to configure remote user access to the store through your Access Gateway deployment.

25. Repeat Steps 15 to 24, as necessary, to list additional Access Gateway deployments on the Remote Access page. If you add multiple deployments, specify a default Access Gateway appliance to be used to access the store.

26. On the Remote Access page, click Create and then, once the store has been created, click Finish.

    StoreFront automatically establishes a trust relationship between the new store and the authentication service.

    The URL for users to access the Receiver for Web site for the new store is displayed. The Receiver for Web site enables users to access their desktops and applications through a Web page.

Your store is now available for users to access with Citrix Receiver and through the Receiver for Web site. After creating the store, further options become available in the Citrix StoreFront management console. For more information, see Managing Your StoreFront Deployment.

By default, the store is configured to specify that Citrix Receiver Updater for Windows and Citrix Receiver Updater for Mac users accessing the store receive plug-in updates directly from the Citrix Update Service on the Citrix Web site. The specific plug-ins included depend on the configuration of the store. For more information about configuring plug-in update settings, see To manage Citrix Receiver updates.

To deploy a multiple server group

If you plan to use a remote database with your multiple server deployment, ensure that you set up the database before starting to configure StoreFront.

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, click Start > All Programs > Citrix > Citrix StoreFront.

2. In the results pane of the Citrix StoreFront management console, click Deploy a multiple server group.

3. Specify the URL of the load balancing environment hosting the StoreFront server in the Hostname (load balancer) box.

   In order to configure a multiple server deployment, the StoreFront servers must be part of an existing load balancing environment.

4. Provide details of the SQL Server instance to be used to record details of users' application subscriptions for your first store. Enter the fully qualified domain name of the database server and the name of the database.

   If you are using a mirrored database, enter details for one of the database servers, create the store, and then edit the store configuration file to include details of the failover partner.

5. Click Test Connection to ensure that StoreFront can access the specified database. If the database details you provide cannot be verified, select the Specify connection string check box to manually compose the database connection string.

   Note: The credentials with which you log on to the StoreFront server are used to test the database connection. Ensure that this user account has permissions to access the database to enable StoreFront to validate the connection details.

6. Click Create to set up the authentication service, which authenticates users to XenDesktop sites, XenApp farms, and AppController.

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

   StoreFront stores enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users.

8. On the Delivery Controllers page, list the XenDesktop, XenApp, and CloudGateway Enterprise deployments providing the resources that you want to make available in the store. Click Add.

9. 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 through the store are provided by CloudGateway Enterprise (through AppController), XenApp, or XenDesktop.

10. If you are configuring a XenDesktop site or XenApp farm, continue to Step 12. To make applications managed by CloudGateway Enterprise available in the store, enter the

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

11. If you manage user access to ShareFile through AppController, select the Data provisioning check box to enable synchronization of users' ShareFile data and documents across all their devices. Continue to Step 16.

12. To make desktops and applications provided by a XenDesktop site or XenApp farm available in the store, add the names or IP addresses of XenDesktop controllers or XenApp servers running the Citrix XML Service to the Servers list. Specify multiple servers in a site or farm to enable fault tolerance, listing the entries in order of priority to set the failover sequence.

13. 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 the XenDesktop site or XenApp farm.

    - To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select HTTPS. If you select this option, ensure that the Citrix XML Service on your servers is set to share its port with IIS and that IIS is configured to support HTTPS.

    - To send data over secure connections to XenApp servers only, 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 XenDesktop sites or XenApp farms, ensure that the server names you specify in the Servers list match exactly (including the case) the names on the certificates for the servers.

14. Specify the port for StoreFront to use for connections to the XenDesktop site or XenApp farm. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service.

15. If you are using the SSL Relay to secure connections between StoreFront and a XenApp farm, 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.

16. Click OK. Repeat Steps 8 to 16, as necessary, to list additional XenDesktop, XenApp, and CloudGateway Enterprise deployments on the Delivery Controllers page. Click Next.

17. On the Remote Access page, specify whether and how users connecting from public networks can access the store through Access 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. If you select this option, continue to Step 29.

    - To make only resources available through the store available to users on public networks through Access Gateway, select No VPN tunnel. Users log on directly to Access Gateway and do not need to use the Access Gateway Plug-in.

- To make the store and other resources on the internal network available to users on public networks through an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the Access Gateway Plug-in to establish the VPN tunnel.

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

18. If you enabled remote access, list the Access Gateway deployments through which users access the store. Click Add.

19. On the Gateway Settings page, specify a name for the Access Gateway deployment that will help users to identify it.

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

20. Enter the URL of the user logon point or virtual server for your Access Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone Access Gateway appliance or an Access Controller server that is part of an Access Gateway cluster.

21. Unless you are configuring remote access through an Access Gateway Enterprise Edition deployment, click Next and continue to Step 23. For Access Gateway Enterprise Edition deployments, select the Set server as Access Gateway Enterprise Edition check box and specify the subnet IP address of the Access Gateway appliance.

    The subnet address is the IP address that Access Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Access Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

22. Select from the Logon type list the authentication method used for Citrix Receiver users accessing their desktops and applications through Access Gateway Enterprise Edition. Click Next.

    - If users are not required to authenticate, select No Authentication.
    - If users are required to enter their domain credentials, select Domain only.
    - If users are required to enter a tokencode obtained from a security token, select Security token only.
    - 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.

23. If you are configuring StoreFront for an Access Gateway cluster, list on the Appliances page the IP addresses or fully qualified domain names of the Access Gateway appliances in the cluster and click Next.

24. On the Enable Silent Authentication page, specify the URL for an appliance running the Access Gateway authentication service. For Access Gateway clusters, enter URLs for multiple Access Controller servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

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

25. On the Secure Ticket Authority (STA) page, specify the URL for a server running the STA. Enter URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

    The STA can be hosted by the Citrix XML Service and issues session tickets in response to requests for connections to XenDesktop sites and XenApp farms. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.

26. If you want XenDesktop and XenApp 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.

27. Click Create to configure remote user access to the store through your Access Gateway deployment.

28. Repeat Steps 18 to 27, as necessary, to list additional Access Gateway deployments on the Remote Access page. If you add multiple deployments, specify a default Access Gateway appliance to be used to access the store.

29. On the Remote Access page, click Create and then, once the store has been created, click Finish.

    StoreFront automatically establishes a trust relationship between the new store and the authentication service.

    The URL for users to access the Receiver for Web site for the new store is displayed. The Receiver for Web site enables users to access their desktops and applications through a Web page.

Your store is now available for users to access with Citrix Receiver and through the Receiver for Web site. After creating the store, further options become available in the Citrix StoreFront management console. For more information, see Managing Your StoreFront Deployment.

By default, the store is configured to specify that Citrix Receiver Updater for Windows and Citrix Receiver Updater for Mac users accessing the store receive plug-in updates directly from the Citrix Update Service on the Citrix Web site. The specific plug-ins included depend on the configuration of the store. For more information about configuring plug-in update settings, see To manage Citrix Receiver updates.

The first server you configure acts as the primary server in your multiple server deployment. You can add secondary servers by selecting the option to join an existing server group when installing further instances of StoreFront.

To manage your 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 set up a remote database

If you plan to use a remote database with a multiple server StoreFront deployment, follow the steps below to set up the database.

1. Join the database server to a domain within the Active Directory forest to which you plan to add your StoreFront servers.

2. Install SQL Server. Ensure that you install the SQL Server Management Tools.

   For more information about installing SQL Server, see http://technet.microsoft.com/en-us/library/bb500469(sql.105).aspx.

3. When installation is complete, ensure that the SQL Server Browser Windows service is started.

   This service enables the Citrix StoreFront management console to locate the database on the network. For more information about starting the SQL Server Browser service, see http://technet.microsoft.com/en-us/library/ms189093(sql.105).aspx.

4. To create the StoreFront database, use SQL Server Management Studio to run the following commands. Replace the variables surrounded by "%%" with the appropriate values for your deployment, where %%*DATABASE_NAME*%% is a valid SQL Server database name, %%*MDF_FILE*%% is the path to the database data (.mdf) file on the server, and %%*LOG_FILE*%% is the path to the database transaction log (.ldf) file.

   ```
   USE [master]

   CREATE DATABASE [%%DATABASE_NAME%%] ON  PRIMARY
   ( NAME = N'MyApps', FILENAME = N'%%MDF_FILE%%' , SIZE = 10240KB ,
     MAXSIZE = UNLIMITED, FILEGROWTH = 10% )
   LOG ON
   ( NAME = N'MyApps_log', FILENAME = N'%%LOG_FILE%%' , SIZE = 10240KB ,
     MAXSIZE = 2048GB , FILEGROWTH = 10% )
   COLLATE latin1_general_CI_AS_KS

   IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
   begin
   EXEC [%%DATABASE_NAME%%].[dbo].[sp_fulltext_database] @action = 'enable'
   end

   ALTER DATABASE [%%DATABASE_NAME%%] SET ANSI_NULL_DEFAULT OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET ANSI_NULLS OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET ANSI_PADDING OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET ANSI_WARNINGS OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET ARITHABORT OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET AUTO_CLOSE OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET AUTO_CREATE_STATISTICS ON
   ALTER DATABASE [%%DATABASE_NAME%%] SET AUTO_SHRINK OFF
   ALTER DATABASE [%%DATABASE_NAME%%] SET AUTO_UPDATE_STATISTICS ON
   ALTER DATABASE [%%DATABASE_NAME%%] SET CURSOR_CLOSE_ON_COMMIT OFF
   ```

```
ALTER DATABASE [%%DATABASE_NAME%%] SET CURSOR_DEFAULT  GLOBAL
ALTER DATABASE [%%DATABASE_NAME%%] SET CONCAT_NULL_YIELDS_NULL OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET NUMERIC_ROUNDABORT OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET QUOTED_IDENTIFIER OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET RECURSIVE_TRIGGERS OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET DISABLE_BROKER
ALTER DATABASE [%%DATABASE_NAME%%] SET AUTO_UPDATE_STATISTICS_ASYNC OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET DATE_CORRELATION_OPTIMIZATION OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET TRUSTWORTHY OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET ALLOW_SNAPSHOT_ISOLATION OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET PARAMETERIZATION SIMPLE
ALTER DATABASE [%%DATABASE_NAME%%] SET READ_COMMITTED_SNAPSHOT OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET HONOR_BROKER_PRIORITY OFF
ALTER DATABASE [%%DATABASE_NAME%%] SET READ_WRITE
ALTER DATABASE [%%DATABASE_NAME%%] SET RECOVERY FULL
ALTER DATABASE [%%DATABASE_NAME%%] SET MULTI_USER
ALTER DATABASE [%%DATABASE_NAME%%] SET PAGE_VERIFY NONE
ALTER DATABASE [%%DATABASE_NAME%%] SET DB_CHAINING OFF
```

For more information about SQL Server Management Studio, see http://technet.microsoft.com/en-us/library/ms174173.aspx.

5. To create the database tables, run the following commands. Replace the variables surrounded by "%%" with the appropriate values for your deployment, where %%*DATABASE_NAME*%% is the name you defined in the preceding step.

```
USE [%%DATABASE_NAME%%]

/****** Object:  Table [dbo].[User]  ******/
SET ANSI_NULLS ON

SET QUOTED_IDENTIFIER ON

CREATE TABLE [dbo].[User](
 [id] [int] IDENTITY(1,1) NOT NULL,
    [username] [nvarchar](100) COLLATE latin1_general_CS_AS_KS NOT NULL,
CONSTRAINT [PK_users] PRIMARY KEY CLUSTERED
(
    [id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF,
 IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  = ON, ALLOW_PAGE_LOCKS  = OFF)
 ON [PRIMARY]
) ON [PRIMARY]

CREATE UNIQUE NONCLUSTERED INDEX [username_idx] ON [dbo].[User]
(
    [username] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF,
 SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF,
 ONLINE = OFF, ALLOW_ROW_LOCKS  = ON, ALLOW_PAGE_LOCKS  = OFF)
 ON [PRIMARY]

/****** Object:  Table [dbo].[Subscription]  ******/
SET ANSI_NULLS ON

SET QUOTED_IDENTIFIER ON
```

```
CREATE TABLE [dbo].[Subscription](
 [id] [int] IDENTITY(1,1) NOT NULL,
 [subscription_ref] [varchar](32) COLLATE latin1_general_CS_AS_KS NOT NULL,
    [resource_id] [nvarchar](400) COLLATE latin1_general_CS_AS_KS NOT NULL,
 [user_id] [int] NOT NULL,
    [status] [int] NOT NULL,
    [metadata] [nvarchar](max) NULL,
    [secure_metadata] [nvarchar](max) NULL,
CONSTRAINT [PK_subscriptions] PRIMARY KEY CLUSTERED
(
 [id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF,
 IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  = ON, ALLOW_PAGE_LOCKS  = OFF)
 ON [PRIMARY]
) ON [PRIMARY]

CREATE UNIQUE NONCLUSTERED INDEX [subscription_ref_idx] ON
 [dbo].[Subscription]
(
[subscription_ref] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF,
 SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF,
 ONLINE = OFF, ALLOW_ROW_LOCKS  = ON, ALLOW_PAGE_LOCKS  = OFF)
 ON [PRIMARY]

CREATE UNIQUE NONCLUSTERED INDEX [user_resource_idx] ON [dbo].[Subscription]
(
[user_id] ASC,
[resource_id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF,
 SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF,
 ONLINE = OFF, ALLOW_ROW_LOCKS  = ON, ALLOW_PAGE_LOCKS  = OFF)
 ON [PRIMARY]

/****** Object:  Default [DF_subscriptions_status] ******/
ALTER TABLE [dbo].[Subscription]
 ADD  CONSTRAINT [DF_subscriptions_status]
 DEFAULT ((0)) FOR [status]

/****** Object:  ForeignKey [FK_subscriptions_user_id] ******/
ALTER TABLE [dbo].[Subscription]
 WITH CHECK ADD  CONSTRAINT [FK_subscriptions_user_id]
 FOREIGN KEY([user_id])
REFERENCES [dbo].[User] ([id])

ALTER TABLE [dbo].[Subscription]
 CHECK CONSTRAINT [FK_subscriptions_user_id]

CREATE TABLE [dbo].[SchemaDetails](
    [major_version] [int] NOT NULL,
 [minor_version] [int] NOT NULL,
    [details] [nvarchar](max) NULL
) ON [PRIMARY]

INSERT INTO [dbo].[SchemaDetails] ([major_version], [minor_version])
```

```
VALUES (1, 0)
```

6. On the server hosting the database, create a local group. Add the computer accounts of the servers on which you plan to install StoreFront as members of the group.

   Creating a local group on the server hosting the database enables remote StoreFront servers to connect to the database using their local machine accounts. If you add any further servers to your deployment in the future, add their machine accounts to the group.

7. Using SQL Server Management Studio, run the following commands to create a database user login for the new Windows group. Replace the variables surrounded by "%%" with the appropriate values for your deployment, where %%*DATABASE_NAME*%% is the name you defined previously and %%*WINDOWS_USER*%% is the fully qualified local group name for the group you created in the preceding step, in the form *databaseservername.domain\localdatabaseusersgroup*.

   ```
   USE [master]
   CREATE LOGIN [%%WINDOWS_USER%%] FROM WINDOWS;
   ALTER LOGIN [%%WINDOWS_USER%%]
    WITH DEFAULT_DATABASE = [%%DATABASE_NAME%%];
   ```

   For more information about login properties, see http://technet.microsoft.com/en-us/library/ms178316(sql.105).aspx.

8. To create a new database user mapped to the new login and grant permissions on the database to the user, run the following commands. Replace the variables surrounded by "%%" with the appropriate values for your deployment, where %%*DATABASE_NAME*%% and %%*WINDOWS_USER*%% are, respectively, the database name and fully qualified local group name you defined previously.

   ```
   USE [%%DATABASE_NAME%%]
   CREATE USER [CitrixSubscriptionDBUsers] FOR LOGIN [%%WINDOWS_USER%%];

   EXEC sp_addrolemember N'db_datawriter', N'CitrixSubscriptionDBUsers';
   EXEC sp_addrolemember N'db_datareader', N'CitrixSubscriptionDBUsers';
   ```

9. Using SQL Server Configuration Manager, enable TCP/IP connections to the database and restart the SQL Server process.

   For more information about enabling server network protocols, see http://technet.microsoft.com/en-us/library/ms191294.aspx.

10. Ensure that the appropriate ports on the server hosting the database are open to inbound connections to allow your StoreFront servers to access the database. For more information about the ports used by SQL Server, see http://technet.microsoft.com/en-us/library/cc646023.aspx.

To join an existing server group

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, click Start > All Programs > Citrix > 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 secondary 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.

5. Once the new server has joined the deployment, return to the primary server and, in the left pane of the Citrix StoreFront management console, select the Server Group node. In the Actions pane, click Propagate Changes.

6. In the Propagate Changes dialog box, click OK.

   The configurations of all the secondary servers in the deployment, including the new server you just added, are updated to match the configuration of the primary server.

The new secondary server is added to your deployment and all servers in the group are updated with details of the new server.

To manage your 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.

Uninstalling StoreFront

In addition to the product itself, uninstalling StoreFront removes the configurations of the authentication service, the stores, and the Receiver for Web sites. In single-server deployments, users' application subscription data are also deleted from the database, whereas in multiple server deployments these data are retained. The prerequisites and the application subscription database, if installed, are not removed from the server.

1. Log on to the StoreFront server using an account with local administrator permissions.
2. On the Windows Start menu, click Control Panel > Programs and Features.
3. Select Citrix StoreFront and click Uninstall to remove all StoreFront components from the server.

Upgrading StoreFront

To upgrade an existing StoreFront deployment to the most recent version, you run the installer. Once the upgrade process is started, it cannot be rolled back. If the upgrade is interrupted or cannot be completed, the server might be left with a mixture of old and updated files making it difficult to repair or remove the StoreFront installation. Before starting to upgrade, you must disconnect users from the StoreFront server and prevent users from accessing the server while the upgrade is in progress. This ensures that all StoreFront files are accessible by the installer during the upgrade. Files that cannot be accessed by the installer are not upgraded, potentially resulting in a failed upgrade. Citrix recommends that you back up your data before upgrading.

To upgrade a single server

With a single-server deployment, uninstalling StoreFront removes the configurations of the authentication service, the stores, and the Receiver for Web sites. In addition, users' application subscription data are deleted from the database. This means that if you decide to uninstall StoreFront from an existing single-server deployment before installing the latest version, not only must you manually reconfigure your settings, but users will need to resubscribe to all their applications. Upgrading enables you to preserve your configuration settings and users' application subscription data.

1. Restart the StoreFront server.

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

2. Stop Microsoft Internet Information Services (IIS).

   Stopping IIS disconnects all current user connections and prevents any additional users from connecting to the server during the upgrade. This also stops all StoreFront services so that files cannot be locked while the upgrade is in progress. For more information about stopping IIS, see http://technet.microsoft.com/en-us/library/cc732317.aspx.

3. Run the StoreFront installation file as an administrator.

   For more information, see Installing and Setting Up StoreFront.

4. Restart the StoreFront server and then restart IIS. Check that all the StoreFront services are running.

   Restarting the server ensures that all caches are cleared before the StoreFront services are started.

To upgrade a multiple server group

Uninstalling StoreFront from all the servers in a multiple server deployment removes the configurations of the authentication service, the stores, and the Receiver for Web sites, but retains users' subscription data on the external database. This means that if you decide to uninstall StoreFront from a server in an existing multiple server deployment before installing the latest version, you must manually reconfigure your settings. However, providing you use the same configuration settings, you can connect your new stores to the existing application subscription database so that users do not need to resubscribe to their applications.

1. Remove a StoreFront server from the load balancing environment.

   Upgrading your servers one-by-one enables you to maintain the availability of your StoreFront deployment so that users do not experience any loss of service. Removing the server from the load balancing environment prevents users from connecting to the server during the upgrade.

2. Restart the StoreFront server.

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

3. Stop the following services in order.

   - Citrix Configuration Replication
   - Citrix Credential Wallet
   - Citrix Peer Name Resolution Service

   Stopping these services disconnects all current user connections and ensures that files cannot be locked while the upgrade is in progress.

4. Run the StoreFront installation file as an administrator.

   For more information, see Installing and Setting Up StoreFront.

5. Restart the StoreFront server and then restart the following services in order. Check that these and all the other StoreFront services are running.

   - Citrix Peer Name Resolution Service
   - Citrix Credential Wallet
   - Citrix Configuration Replication

   Restarting the server ensures that all caches are cleared before the StoreFront services are restarted.

6. Add the upgraded server back into the load balancing environment. Repeat the procedure above for each of the remaining servers in your StoreFront deployment until you have upgraded them all.

Managing 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.

The topics in this section describe:

- Creating the authentication service
- Configuring the authentication service
- Creating stores
- Configuring stores
- Creating Receiver for Web sites
- Configuring Receiver for Web sites
- Adding an Access Gateway connection
- Configuring Access Gateway connection settings
- Configuring beacon points
- Configuring server groups
- Configuring StoreFront using the configuration files
- Configuring Receiver for Web using the configuration files

To create the authentication service

Use the Create Authentication Service task to configure the StoreFront authentication service. The authentication service authenticates users to XenDesktop sites, XenApp farms, and AppController, handling all interactions to ensure that users only need to log on once.

You can only configure one authentication service per StoreFront server. This task is only available when the existing authentication service has been removed.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 Pass-through from Citrix Access Gateway check box to enable pass-through authentication from Access Gateway. Users authenticate to Access Gateway and are automatically logged on when they access their stores.
4. Once the authentication service has been created, click Finish.

   The authentication service URL is displayed. For more information about modifying settings for the authentication service, see Configuring 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.

Configuring the Authentication Service

The authentication service authenticates users to XenDesktop sites, XenApp farms, and AppController, handling all interactions to ensure that users only need to log on once. The tasks described below enable you 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 Configuring 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 clicking Enable Method or Disable Method, as appropriate, in the Actions pane. To remove an authentication method from the authentication service or to add a new one, use the Add/Remove Methods task.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 Pass-through from Citrix Access Gateway check box to enable pass-through authentication from Access Gateway. Users authenticate to Access Gateway and are automatically logged on when they access their stores.

Generating 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. Generating new security keys requires that all users reauthenticate to their stores, so this task is best carried out during periods of low user activity.

Removing the Authentication Service

Use the Remove Service task to delete the authentication service. Before removing the authentication service, first delete all the stores that use the service and their associated Receiver for Web sites. Ensure that the authentication service is not being used by any Merchandising Server appliances when you remove the service or Merchandising Server will not be able to identify users when delivering configurations for Citrix Receiver.

To configure trusted user domains

Use the Configure Trusted Domains task to restrict access to stores that use the authentication service for users logging on with explicit domain credentials, either directly or through Access Gateway.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > Citrix StoreFront.

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

3. Select Trusted domains. Click Add to enter the name of a trusted domain. Users with domain accounts will be able to log on to all stores that use this authentication service. To modify a domain name, select the entry in the list and click Edit. Select a domain in the list and click Remove to prevent users from logging on to stores using accounts from 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 StoreFront.

Enabling Users to Change Expired Passwords

Use the Manage Password Options task to enable users accessing stores with explicit domain credentials to reset expired passwords when logging on. When this setting is enabled, users who cannot log on because their passwords have expired are redirected to the Change Password dialog box. StoreFront contacts the domain controller to reset users' passwords.

If you decide to enable this feature, ensure that the policies for the domains containing your Citrix servers do not prevent users from resetting their passwords. You must also ensure that there is sufficient disk space on your StoreFront server to store profiles for all your users. By default, StoreFront warns users if their passwords are due to expire. To perform the password expiry check, StoreFront creates local user profiles on the server.

Enabling users to reset expired passwords exposes sensitive security functions to anyone who can access any of the stores that use this authentication service. If your organization has a security policy that restricts user password reset functions for internal use only, ensure that none of the stores that use this authentication service are accessible from outside your internal network. User resetting of expired passwords is disabled by default when the authentication service is created.

To create a store

Use the Create Store task to add stores. StoreFront stores enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users.

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

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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.

4. On the Delivery Controllers page, list the XenDesktop, XenApp, and CloudGateway Enterprise deployments 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 through the store are provided by CloudGateway Enterprise (through AppController), XenApp, or XenDesktop.

6. If you are configuring a XenDesktop site or XenApp farm, continue to Step 8. To make applications managed by CloudGateway Enterprise available in the store, enter the name or IP address of an AppController virtual appliance in the Server box and specify the port for StoreFront to use for connections to AppController. The default port is 443.

7. If you manage user access to ShareFile through AppController, select the Data provisioning check box to enable synchronization of users' ShareFile data and documents across all their devices. Continue to Step 12.

8. To make desktops and applications provided by a XenDesktop site or XenApp farm available in the store, add the names or IP addresses of XenDesktop controllers or XenApp servers running the Citrix XML Service to the Servers list. Specify multiple servers in a site or farm to enable fault tolerance, listing the entries in order of priority to set the failover sequence.

9. 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 the XenDesktop site or XenApp farm.

    - To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select HTTPS. If you select this option, ensure that the Citrix XML Service on your servers is set to share its port with IIS and that IIS is configured to support

HTTPS.

- To send data over secure connections to XenApp servers only, 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 XenDesktop sites or XenApp farms, ensure that the server names you specify in the Servers list match exactly (including the case) the names on the certificates for the servers.

10. Specify the port for StoreFront to use for connections to the XenDesktop site or XenApp farm. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service.

11. If you are using the SSL Relay to secure connections between StoreFront and a XenApp farm, 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.

12. Click OK. Repeat Steps 4 to 12, as necessary, to list additional XenDesktop, XenApp, and CloudGateway Enterprise deployments on the Delivery Controllers page. Click Next.

13. If you are creating a store for a single-server deployment, continue to Step 15. For multiple server deployments, on the Database page, provide details of the SQL Server instance to be used to record details of users' application subscriptions. Enter the fully qualified domain name of the database server and the name of the database.

    A separate database is required for each store you create. If you are using a mirrored database, enter details for one of the database servers, create the store, and then edit the store configuration file to include details of the failover partner.

14. Click Test Connection to ensure that StoreFront can access the specified database. If the database details you provide cannot be verified, select the Specify connection string check box to manually compose the database connection string. Click Next.

    Note: The credentials with which you log on to the StoreFront server are used to test the database connection. Ensure that this user account has permissions to access the database to enable StoreFront to validate the connection details.

15. On the Remote Access page, specify whether and how users connecting from public networks can access the store through Access 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. If you select this option, continue to Step 27.

    - To make only resources available through the store available to users on public networks through Access Gateway, select No VPN tunnel. Users log on directly to Access Gateway and do not need to use the Access Gateway Plug-in.

    - To make the store and other resources on the internal network available to users on public networks through an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the Access Gateway Plug-in to establish the VPN tunnel.

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

logged on when they access their stores.

16. If you enabled remote access, list the Access Gateway deployments through which users access the store. Any appliances you configured previously for this and other stores are available for selection in the Access Gateways list. If you want to add a further appliance to the list, click Add. Otherwise, continue to Step 26.

17. On the Gateway Settings page, specify a name for the Access Gateway deployment that will help users to identify it.

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

18. Enter the URL of the user logon point or virtual server for your Access Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone Access Gateway appliance or an Access Controller server that is part of an Access Gateway cluster.

19. Unless you are configuring remote access through an Access Gateway Enterprise Edition deployment, click Next and continue to Step 21. For Access Gateway Enterprise Edition deployments, select the Set server as Access Gateway Enterprise Edition check box and specify the subnet IP address of the Access Gateway appliance.

    The subnet address is the IP address that Access Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Access Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

20. Select from the Logon type list the authentication method used for Citrix Receiver users accessing their desktops and applications through Access Gateway Enterprise Edition. Click Next.

    - If users are not required to authenticate, select No Authentication.
    - If users are required to enter their domain credentials, select Domain only.
    - If users are required to enter a tokencode obtained from a security token, select Security token only.
    - 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.

21. If you are configuring StoreFront for an Access Gateway cluster, list on the Appliances page the IP addresses or fully qualified domain names of the Access Gateway appliances in the cluster and click Next.

22. On the Enable Silent Authentication page, specify the URL for an appliance running the Access Gateway authentication service. For Access Gateway clusters, enter URLs for multiple Access Controller servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

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

23. On the Secure Ticket Authority (STA) page, specify the URL for a server running the STA. Enter URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

    The STA can be hosted by the Citrix XML Service and issues session tickets in response to requests for connections to XenDesktop sites and XenApp farms. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.

24. If you want XenDesktop and XenApp 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.

25. Click Create to configure remote user access to the store through your Access Gateway deployment.

26. Repeat Steps 16 to 25, as necessary, to list additional Access Gateway deployments on the Remote Access page. If you selected multiple deployments in the Access Gateways list, specify a default Access Gateway appliance to be used to access the store.

27. On the Remote Access page, click Create and then, once the store has been created, click Finish.

    StoreFront automatically establishes a trust relationship between the new store and the authentication service.

    The URL for users to access the Receiver for Web site for the new store is displayed. The Receiver for Web site enables users to access their desktops and applications through a Web page.

Your store is now available for users to access with Citrix Receiver and through the Receiver for Web site. For more information about modifying settings for stores, see Configuring Stores.

By default, the store is configured to specify that Citrix Receiver Updater for Windows and Citrix Receiver Updater for Mac users accessing the store receive plug-in updates directly from the Citrix Update Service on the Citrix Web site. The specific plug-ins included depend on the configuration of the store. For more information about configuring plug-in update settings, see To manage Citrix Receiver updates.

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.

Configuring Stores

StoreFront stores enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users. The tasks in this section enable you to modify settings for your stores. Some advanced settings can only be changed by editing the store configuration files. For more information, see Configuring 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.

The topics in this section describe:

- Exporting store provisioning files for users
- Hiding and advertising stores to users
- Managing the resources made available through stores
- Managing remote access to stores through Access Gateway
- Managing Citrix Receiver updates
- Integrating Citrix Online applications with stores
- Changing the application subscription database used by a store
- Configuring support for legacy clients
- Generating security keys for stores
- Removing 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 Access Gateway deployments and beacons configured for the stores. Make these files available to your users to enable them to configure Citrix Receiver automatically with details of your stores. If you configure Receiver for Web sites for your stores, users can also obtain Citrix Receiver provisioning files from the sites.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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.

Hiding and Advertising Stores to Users

Use the Hide Store task to prevent stores being made available automatically for Citrix Receiver users to add to their configurations. By default, when you create a store it is advertised and becomes available for all users to add to their Citrix Receiver configurations. Hiding a store does not make it inaccessible, instead users must know the connection details for the store in order to add it in Citrix Receiver. To restore the general availability of a hidden store, use the Advertise Store task.

To manage the resources made available through stores

Use the Manage Delivery Controllers task to add and remove from stores resources provided by XenDesktop, XenApp, and AppController, and to modify the details of the deployments providing these resources.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 site, XenApp farm, or AppController virtual appliance in the store. To modify the settings for a site, farm, or virtual appliance, select the entry in the Farms list and click Edit. Select an entry in the list and click Remove to remove the resources provided by the site, farm, or virtual appliance from 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 through the store are provided by CloudGateway Enterprise (through AppController), XenApp, or XenDesktop.

5. If you are configuring a XenDesktop site or XenApp farm, continue to Step 7. To make applications managed by CloudGateway Enterprise available in the store, enter the name or IP address of an AppController virtual appliance in the Server box and specify the port for StoreFront to use for connections to AppController. The default port is 443.

6. If you manage user access to ShareFile through AppController, select the Data provisioning check box to enable synchronization of users' ShareFile data and documents across all their devices. Continue to Step 11.

7. To make desktops and applications provided by a XenDesktop site or XenApp farm available in the store, click Add to enter the name or IP address of XenDesktop controllers or XenApp servers running the Citrix XML Service. To modify the name or IP address of a controller or 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 controller or server to enumerate the resources available.

   Specify multiple servers in a site or farm to enable fault tolerance, listing the entries in order of priority to set the failover sequence.

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 the XenDesktop site or XenApp farm.

- To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select HTTPS. If you select this option, ensure that the Citrix XML Service on your servers is set to share its port with IIS and that IIS is configured to support HTTPS.

- To send data over secure connections to XenApp servers only, 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 XenDesktop sites or XenApp farms, ensure that the server names you specify in the Servers list match exactly (including the case) the names on the certificates for the servers.

9. Specify the port for StoreFront to use for connections to the XenDesktop site or XenApp farm. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service.

10. If you are using the SSL Relay to secure connections between StoreFront and a XenApp farm, 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. Repeat Steps 3 to 11, as necessary, to add or modify further XenDesktop, XenApp, and CloudGateway Enterprise deployments in the Delivery Controllers list.

To manage remote access to stores through Access Gateway

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

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 Access 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 available through the store available to users on public networks through Access Gateway, select No VPN tunnel. Users log on directly to Access Gateway and do not need to use the Access Gateway Plug-in.

   - To make the store and other resources on the internal network available to users on public networks through an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the Access Gateway Plug-in to establish the VPN tunnel.

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

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

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

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

6. Enter the URL of the user logon point or virtual server for your Access Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone Access Gateway appliance or an Access Controller server that is part of an Access Gateway cluster.

7. Unless you are configuring remote access through an Access Gateway Enterprise Edition deployment, click Next and continue to Step 9. For Access Gateway Enterprise Edition deployments, select the Set server as Access Gateway Enterprise Edition check box and specify the subnet IP address of the Access Gateway appliance.

   The subnet address is the IP address that Access Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Access Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

8. Select from the Logon type list the authentication method used for Citrix Receiver users accessing their desktops and applications through Access Gateway Enterprise Edition. Click Next.

   - If users are not required to authenticate, select No Authentication.
   - If users are required to enter their domain credentials, select Domain only.
   - If users are required to enter a tokencode obtained from a security token, select Security token only.
   - 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.

9. If you are configuring StoreFront for an Access Gateway cluster, list on the Appliances page the IP addresses or fully qualified domain names of the Access Gateway appliances in the cluster and click Next.

10. On the Enable Silent Authentication page, specify the URL for an appliance running the Access Gateway authentication service. For Access Gateway clusters, enter URLs for multiple Access Controller servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

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

11. On the Secure Ticket Authority (STA) page, specify the URL for a server running the STA. Enter URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

    The STA can be hosted by the Citrix XML Service and issues session tickets in response to requests for connections to XenDesktop sites and XenApp farms. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.

12. If you want XenDesktop and XenApp 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 configure remote user access to the store through your Access Gateway deployment.

14. Repeat Steps 4 to 13, as necessary, to list additional Access Gateway deployments in the Enable Remote Access dialog box. If you selected multiple deployments in the Access Gateways list, specify a default Access Gateway appliance to be used to access the store.

To manage Citrix Receiver updates

Use the Manage Receiver Updates task to specify the mechanism for delivery of plug-in updates to Citrix Receiver Updater for Windows and Citrix Receiver Updater for Mac users accessing the store.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 Receiver Updates.

3. Specify how Citrix Receiver Updater users accessing the store receive plug-in updates.

    - If you want users to receive plug-in updates directly from the Citrix Update Service, select Citrix Update (citrix.com). Users receive the latest plug-ins from the Citrix Web site, provided they are connected to the Internet.

    - If you are using Merchandising Server to manage plug-in updates for Citrix Receiver users, select Citrix Merchandising Server and specify the URL 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 authentication service to enable Merchandising Server to identify users, see Configuring Authentication.

    - If you have an alternative strategy for managing plug-in updates, such as using a third-party electronic software distribution tool, select None.
4. If you are using the Citrix Update Service to deliver plug-in updates to Citrix Receiver Updater users, specify the plug-ins to include.

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

    - Select ShareFile Sync to enable users to access ShareFile data through Citrix Receiver. If the store provides users with access to ShareFile data through AppController and you enabled ShareFile data provisioning for the store, ShareFile Sync is included by default and cannot be removed.

    - Select ShareFile for Outlook to enable users to access ShareFile data through Microsoft Outlook. If the store provides users with access to ShareFile data through AppController and you enabled ShareFile data provisioning for the store, ShareFile for Outlook is included by default and cannot be removed.

    - Include the 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 Secure Access Plug-in is included by default and cannot be removed.

- Include the HDX Real Time Media Engine to enable Citrix Receiver Updater for Windows users to access audio and video communications provided by XenDesktop and XenApp resources.

To integrate Citrix Online applications with stores

Use the Integrate with Citrix Online task to specify 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 primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 Web site 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 application immediately.

To change the application subscription database used by a store

Use the Change Database task to switch the SQL Server instance used to record details of users' application subscriptions by stores in multiple server deployments. Enter the fully qualified domain name of the database server and the name of the database.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 Change Database.
3. Enter the fully qualified domain name of the database server and the name of the new database.

   A separate database is required for each store you create. If you are using a mirrored database, enter details for one of the database servers and then edit the store configuration file to include details of the failover partner.
4. Click Test Connection to ensure that StoreFront can access the specified database. If the database details you provide cannot be verified, select the Specify connection string check box to manually compose the database connection string.

   Note: The credentials with which you log on to the StoreFront server are used to test the database connection. Ensure that this user account has permissions to access the database to enable StoreFront to validate the connection details.

To configure support for legacy clients

Use the Configure Legacy Support task to configure access to your stores for users with older clients that support Web Interface XenApp Services sites. When you create a new store, access through a XenApp Services URL is enabled by default.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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.

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

   The online plug-in enables you to specify a default URL for each server or group of servers providing a XenApp Services site.

Generating 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. Generating new security keys requires that all users reauthenticate to their stores, so this task is best carried out during periods of low user activity.

Removing Stores

Use the Remove Store task to delete a store. Before removing a store, first delete any associated Receiver for Web sites.

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 Web page. To access their desktops and applications, users also require a compatible version of Citrix Receiver.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 that users will use 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 Configuring 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.

Configuring Receiver for Web Sites

Receiver for Web sites enable users to access stores through a Web page. To access their desktops and applications, users require a compatible version of Citrix Receiver. 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 Configuring Receiver for Web 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.

Changing 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.

Removing 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 access the Web page for the store. Users must access the store directly from Citrix Receiver or through the XenApp Services URL, if configured.

To add an Access Gateway connection

Use the Add Gateway Server task to add Access Gateway deployments through which users can access your stores. You must enable the pass-through from Access Gateway authentication method before you can configure remote access to your stores through Access Gateway.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > Citrix StoreFront.

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

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

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

4. Enter the URL of the user logon point or virtual server for your Access Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone Access Gateway appliance or an Access Controller server that is part of an Access Gateway cluster.

5. Unless you are configuring remote access through an Access Gateway Enterprise Edition deployment, click Next and continue to Step 7. For Access Gateway Enterprise Edition deployments, select the Set server as Access Gateway Enterprise Edition check box and specify the subnet IP address of the Access Gateway appliance.

   The subnet address is the IP address that Access Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Access Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

6. Select from the Logon type list the authentication method used for Citrix Receiver users accessing their desktops and applications through Access Gateway Enterprise Edition. Click Next.

   - If users are not required to authenticate, select No Authentication.
   - If users are required to enter their domain credentials, select Domain only.
   - If users are required to enter a tokencode obtained from a security token, select Security token only.
   - 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.

7. If you are configuring StoreFront for an Access Gateway cluster, list on the Appliances page the IP addresses or fully qualified domain names of the Access Gateway appliances in the cluster and click Next.

8. On the Enable Silent Authentication page, specify the URL for an appliance running the Access Gateway authentication service. For Access Gateway clusters, enter URLs for multiple Access Controller servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

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

9. On the Secure Ticket Authority (STA) page, specify the URL for a server running the STA. Enter URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

   The STA can be hosted by the Citrix XML Service and issues session tickets in response to requests for connections to XenDesktop sites and XenApp farms. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.

10. If you want XenDesktop and XenApp 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.

11. Click Create to configure user access to StoreFront through your Access Gateway deployment. Once the configuration has been updated, click Finish.

    For more information about updating the StoreFront configuration with changes to the details of your Access Gateway deployments, see Configuring Access Gateway Connection Settings.

When you add an Access Gateway deployment, at least two external beacon points are required to enable Citrix Receiver to determine whether users are connected to local or public networks and select the appropriate access method. For more information, see To configure beacon points. To enable users to access your stores through Access Gateway, ensure that you configure remote user access.

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.

Configuring Access Gateway Connection Settings

The tasks described below enable you to update the StoreFront configuration with changes to the details of the Access Gateway deployments through which users access your stores.

If you change any Access Gateway details in the StoreFront configuration, ensure that users who access stores through that Access Gateway deployment 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 Access Gateway settings

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

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > Citrix StoreFront.

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

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

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

4. Enter the URL of the user logon point or virtual server for your Access Gateway deployment in the Gateway URL box. Specify whether the logon point or virtual server is hosted on a standalone Access Gateway appliance or an Access Controller server that is part of an Access Gateway cluster.

5. If you are configuring StoreFront for an Access Gateway Enterprise Edition deployment, select the Set server as Access Gateway Enterprise Edition check box and specify the subnet IP address of the Access Gateway appliance.

   The subnet address is the IP address that Access Gateway Enterprise Edition uses to represent the user device when communicating with servers on the internal network.

This can also be the mapped IP address of the Access Gateway appliance. StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

6. For Access Gateway Enterprise Edition deployments only, select from the Logon type list the authentication method used for Citrix Receiver users accessing their desktops and applications through Access Gateway Enterprise Edition.

   - If users are not required to authenticate, select No Authentication.
   - If users are required to enter their domain credentials, select Domain only.
   - If users are required to enter a tokencode obtained from a security token, select Security token only.
   - 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.

Managing Access Gateway Appliances

Use the Manage Appliances task to add, edit, or remove from the StoreFront configuration IP addresses or fully qualified domain names for appliances in your Access Gateway cluster.

Enabling Silent User Authentication Through Access Gateway

Use the Enable Silent Authentication task to update the location of the Access Gateway authentication service that StoreFront uses to authenticate remote users so that they do not need to re-enter their credentials when accessing stores. For Access Gateway clusters, enter URLs for multiple Access Controller servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

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.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > Citrix StoreFront.
2. Select the Gateways node in the left pane of the Citrix StoreFront management console and, in the results pane, select an Access 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.

Specify URLs for multiple STA servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

4. If you want XenDesktop and XenApp 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.

Removing Access Gateway Deployments

Use the Remove Gateway Server task to delete an Access Gateway deployment from the StoreFront configuration. Once an Access Gateway appliance is removed, users are no longer be able to access stores through that deployment.

To configure beacon points

Use the Manage Beacons task to update the StoreFront configuration with URLs outside of your internal network to be used as beacon points. Citrix Receiver uses beacon points to determine whether users are connected to local or public networks and then selects the appropriate access method.

If you enabled remote access when you created your stores, StoreFront uses the logon points or virtual servers of your Access Gateway deployments as external beacon points by default.

If you change any beacon points in the StoreFront configuration, 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.

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.

1. On the primary StoreFront server in your deployment, click Start > All Programs > Citrix > 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 URLs for at least two beacon points outside your internal network.

   The base URL you specified when you installed StoreFront is used as a beacon point within your internal network.

   Including at least two highly available external beacons that can be resolved from public networks enables Citrix Receiver to determine whether users are located behind an Internet paywall, such as in a hotel or Internet café.

Configuring Server Groups

The tasks described below enable you to modify settings for your multiple server StoreFront deployments. To manage your 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.

Adding 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 joining new servers to existing StoreFront deployments, see To join an existing server group.

Removing 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.

Propagating 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 configuration changes made on other servers in the group are discarded. While running this task, you cannot make any further configuration 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.

Synchronizing Local Settings with a Server Group

Use the Sync Settings with Server Group task to update the configuration of the current server to match the configuration of all the other servers in a multiple server StoreFront deployment.

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 synchronize the server configuration with the other servers in the deployment.

Configuring StoreFront Using the Configuration Files

This topic describes additional configuration tasks that involve editing the StoreFront 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 enable ICA file signing

StoreFront provides the option to digitally sign ICA files so that Citrix Receiver can verify that the file originates from a trusted source. When file signing is enabled on 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, then 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, edit the store configuration file. For more information about enabling ICA file signing in Citrix Receiver, see ICA File Signing - Protection 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 StoreFront server, 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 any string that you want to use 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 string with which you chose 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.

To configure Citrix XML Service time-out duration and retry attempts

By default, contact between StoreFront and the Citrix XML Service for a XenDesktop site or XenApp farm times out after 30 seconds and the service is considered unavailable after two unsuccessful communication attempts. To change these settings, edit the configuration file for the authentication service and store.

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

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

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

To configure a store to use a mirrored database

When you create a store in a multiple server deployment, StoreFront uses the database server and database name that you enter to create a connection string for the application subscription database. If you are using mirroring to provide high availability for the application subscription database, you must add details of the failover partner to the database connection string. To do this, edit the store configuration file.

1. On the StoreFront server, 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.

   ```
   <add ... connectionString="Integrated Security=SSPI;
     Server=firstservername;
     Database=databasename" ... />
   ```

   Where *firstservername* is the fully qualified domain name of one of the mirrored database servers and *databasename* is the name of the database that you specified when you created the store.

3. Add the failover partner to the database connection string as shown below.

   ```
   <add ... connectionString="Integrated Security=SSPI;
     Server=firstservername;
   ```

Database=*databasename*;
Failover Partner=*secondservername*" ... />

Where *secondservername* is the fully qualified domain name of the failover partner database server.

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, edit the store configuration file.

1. On the StoreFront server, 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.

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 SSL connections. Socket pooling should not be used for stores that contain applications hosted on XenApp for UNIX. To enable socket pooling, edit the store configuration file.

1. On the StoreFront server, 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.

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, edit the files for the authentication service.

1. On the StoreFront server, 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 versions of the ExplicitAuth.resx file.

Configuring Receiver for Web Using the Configuration Files

This topic describes additional configuration tasks for Receiver for Web sites that involve editing 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 configure how resources are displayed for users

When both desktops and applications are available from a site, Receiver for Web 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 site, if only a single desktop is available for a user, Receiver for Web attempts to automatically start that desktop when the user logs on.

Note: To enable Receiver for Web to automatically start their desktops, users accessing the site through Internet Explorer must add the site to the Local intranet or Trusted sites zones.

To change these default settings, edit the site configuration file.

1. 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.

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 from automatically starting and accessing a desktop when a user logs on to the site and only a single desktop is available for that user.

To configure 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 or if a more recent version is available, the user is prompted to download and install the appropriate Citrix Receiver for their platform, installation files for which are automatically stored on the server when you install StoreFront. To disable detection and deployment of Citrix Receiver, edit the site configuration file.

1. 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.

2. Locate the following element in the file.

   <pluginAssistant enabled="true" upgradeAtLogin="true">

3. Change the value of the enabled attribute to false to disable detection and deployment of Citrix Receiver for the site. Set the value of the upgradeAtLogin attribute to false to stop offering users with older clients the option to upgrade.

4. To update the versions of Citrix Receiver for Windows and Citrix Receiver for Mac stored on the StoreFront server and offered to users, replace the Citrix Receiver installation files in the \Receiver Clients\Windows\ and \Receiver Clients\Mac\ directories of the StoreFront installation, typically located at C:\Program Files\Citrix\Receiver StoreFront\.

5. Using an account with local administrator permissions, start Windows PowerShell and, at a command prompt, type the following commands to update StoreFront with the new versions of Citrix Receiver.

   ```
   > C:\Program Files\Citrix\Receiver StoreFront\Scripts\
     UpdateWindowsReceiverLocation.ps1 -ClientLocation "Windows\filename"
   > C:\Program Files\Citrix\Receiver StoreFront\Scripts\
     UpdateMacOSReceiverLocation.ps1 -ClientLocation "Mac\filename"
   ```

   Where *filename* is the name of the updated Citrix Receiver installation file.

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, edit the site configuration file.

1. 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.

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 logging on to the site 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 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 automatically disconnected when the user logs off from that site, provided that the same browser is used to log on, start the resources, and log off.

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

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

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

To stop offering provisioning files to users

By default, users can obtain from Receiver for Web sites provisioning files that enable them to configure Citrix Receiver automatically with connection details, including any Access Gateway deployments and beacons, for the store providing the desktops and applications for the site. To stop offering Citrix Receiver provisioning files to users, edit the site configuration file.

1. 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.

2. Locate the following element in the file.

<receiverConfiguration enabled="true" ... />

3. Change the value of the enabled attribute to false to remove the Citrix Receiver provisioning file button from the site.

To configure store time-out duration and retry attempts

By default, contact between the Receiver for Web site and the associated store times out after one minute and the store is considered unavailable after two unsuccessful communication attempts. To change these settings, edit the site configuration file.

1. 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.

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.

To configure session durations

Once authenticated to XenDesktop, XenApp, or AppController, users can, by default, access resources provided by the site, farm, or virtual appliance 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, edit the site configuration file.

1. 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.

2. Locate the following element in the file.

   <authentication tokenLifeTime="08:00:00" ... />

3. Change the value of the tokenLifeTime attribute to set the time in hours, minutes, and seconds for which users, once authenticated to XenDesktop, XenApp, or AppController, can continue to use resources provided by the site, farm, or virtual appliance.

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.

Securing Your StoreFront Deployment

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

Use of 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 local users connecting directly to StoreFront, 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 Configuring 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.

Securing StoreFront communications. In a production environment, Citrix recommends using the SSL Relay to secure data traffic between StoreFront servers and XenApp farms. The SSL Relay is a default component of XenApp that performs host authentication and data encryption.

For XenDesktop sites and other deployments that do not support the SSL Relay, use 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 SSL and Transport Layer Security (TLS) protocols to provide strong data encryption.

Citrix recommends securing communications between StoreFront and users' devices using Access Gateway and HTTPS. To use HTTPS, StoreFront requires that the IIS instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.

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.

Hosting StoreFront. 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 Citrix Receiver 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 about enabling ICA file signing in StoreFront, see Configuring StoreFront Using the Configuration Files.

Password reset. You can enable users whose passwords have expired to reset their passwords when they log on to StoreFront. However, this exposes sensitive security functions to anyone who can access any of the stores that use the authentication service for which this setting is enabled. If your organization has a security policy that restricts user password reset functions for internal use only, ensure that none of the stores that use this authentication service are accessible outside of your internal network. User resetting of expired passwords is disabled by default when you create an authentication service.

Integrating StoreFront into Your Environment

When publishing applications on your XenApp farms, consider the following options to enhance the experience for users accessing the applications through StoreFront stores.

- Consider organizing 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 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. For more information about application folders, see To configure shortcuts for user devices.

- Ensure that you include meaningful descriptions for published applications, as these descriptions are visible to users in Citrix Receiver. For more information about including descriptions when publishing applications on your XenApp farms, see To publish a resource using the Publish Application wizard.

- 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 publish the application in XenApp. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.

- To automatically subscribe all users of a store to a Web or software-as-a-service (SaaS) application managed by AppController, select the App is available in Receiver to all users automatically check box when you configure the application settings. For more information, see To configure settings to create user accounts.

- Advertise 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; for example, KEYWORDS:Auto Featured.

- By default, shared XenApp server desktops are treated like other virtual desktops by Receiver for Web. To change this behavior, append the string KEYWORDS:TreatAsApp to the desktop description. The desktop is displayed in the application view rather than the desktop view and users must subscribe to the desktop before they can access it. In addition, the desktop is not automatically started when the user logs on to the site and is not accessed with the Desktop Viewer, even if Receiver for Web is configured to do this for other desktops.

To manage user access to Citrix Online applications with XenApp

You can configure StoreFront stores to include Citrix Online products, such as GoToMeeting, GoToWebinar, and GoToTraining, along with the other resources. However, the Citrix Online applications that you include in a store are available to all users of the store. If you want to manage user access to Citrix Online applications, use AppController to automatically provision and manage user accounts. Alternatively, you can make Citrix Online products available as hosted applications and use the access controls available in XenApp.

1. Using XenApp, publish any application; for example, Notepad.

   This application is a placeholder and will not be accessed by users.

2. When you are prompted to specify a name for the application, give it the name of the Citrix Online product that you want to publish and set the icon to the appropriate Citrix Online application icon.

3. When you are prompted for a description of the application for users, include a description of the Citrix Online product that you want to publish. Append the string KEYWORDS:IsGoToMeeting , KEYWORDS:IsGoToWebinar, or KEYWORDS:IsGoToTraining, as appropriate, to the description.

4. Ensure that you enable the appropriate Citrix Online product in the StoreFront store that enumerates resources from the XenApp server.

When users subscribe to the Citrix Online product, the appropriate client application is still installed locally. However, the XenApp policies and settings applied to the placeholder application now determine the users to which the application is made available in the store.

Troubleshooting StoreFront

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 to files in the \Admin\logs\ directory of the StoreFront installation, typically located at C:\Program Files\Citrix\Receiver StoreFront\. By default, tracing for other operations is disabled and must be enabled manually.

To configure log throttling

1. On the StoreFront server, use a text editor to open the web.config file for the authentication service, store, or Receiver for Web site, which is 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. Using an account with local administrator permissions on the StoreFront server, start Windows PowerShell and, at a command prompt, type the following commands.

   ```
   > Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
   > Set-DSTraceLevel -All -TraceLevel Verbose
   ```

2. 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 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\.