Receiver Storefront 1.1

2013-08-11 04:36:40 UTC

Contents

Receiver Storefront 1.1

Receiver 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 Receiver Storefront database records details of resource subscriptions and shortcuts to enable synchronization of users' desktops and applications across their devices.

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

About Receiver Storefront

Receiver Storefront provides authentication and resource delivery services for Citrix Receiver.

- The Receiver 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.
- Receiver 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 Receiver 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 Receiver Storefront database records details of users' resource subscriptions, plus associated shortcut names and locations. When a user accesses a store, the application synchronization feature automatically updates the subscribed desktops and applications on the user device to match the configuration stored in the Receiver Storefront database, ensuring users have a consistent experience across all their devices.

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

What's New

Pass-through authentication to AppController. Once logged on to Citrix Receiver or Access Gateway, users can access Web and software-as-a-service (SaaS) applications through AppController without needing to authenticate again. For more information, see Planning Your Receiver Storefront Deployment.

Default support for legacy clients. When you create a new store, access for older clients that support Web Interface XenApp Services sites is enabled by default. For more information, see Configuring Stores.

Installation alongside Web Interface. Receiver Storefront can be hosted on the same Microsoft Internet Information Services (IIS) instance as Web Interface. For more information, see Installing and Setting Up Receiver Storefront.

Other Features

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

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

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

One-click client configuration. You can configure Citrix Receiver for your users by making provisioning files available. For more information, see Configuring Stores.

Known Issues in Receiver Storefront 1.1

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]

AppController Logon screen is not localized

When users access Web and SaaS applications through Receiver Storefront stores and Receiver for Web sites, the AppController Logon screen appears in English regardless of users' operating system and Web browser locales. [#291987]

System Requirements for Receiver Storefront 1.1

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

Citrix Server Requirements

Receiver Storefront can be used with the following product versions.

AppController

- Citrix AppController 1.0
- Citrix AppController 1.1

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

If you plan to configure Merchandising Server to use the authentication service to identify users when delivering Citrix Receiver configurations, Receiver 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

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

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

Web Server Requirements

Receiver 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 Receiver 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 Receiver Storefront.

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

Database Requirements

Receiver 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 Receiver Storefront stores. Receiver Storefront supports the following versions of SQL Server.

- 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 Receiver Storefront stores directly.

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

The following client, operating system, and Web browser combinations are recommended for users to access Receiver for Web sites.

Client	Operating system	Browser	Connection

Citrix Receiver for Windows 3.2	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 10 Mozilla Firefox 9 Google Chrome 17 Google Chrome 16	Local network and Access Gateway
	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 11.5	Mac OS X 10.7 Lion	Safari 5.1 Mozilla Firefox 10	Local network and Access Gateway
	Mac OS X 10.6 Snow Leopard	Safari 5.0	
Citrix Receiver for Linux 12.1	Red Hat Enterprise Linux 6 Desktop Ubuntu 11.1 32-bit	Mozilla Firefox 10 Mozilla Firefox 9	Local network only
Citrix Receiver for Chromebook 1.0	Google Chrome OS 17	Google Chrome OS 17	Local network and Access Gateway

The following clients can be used to access Receiver Storefront stores with reduced functionality through XenApp Services URLs. For more information, see User Access Options.

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

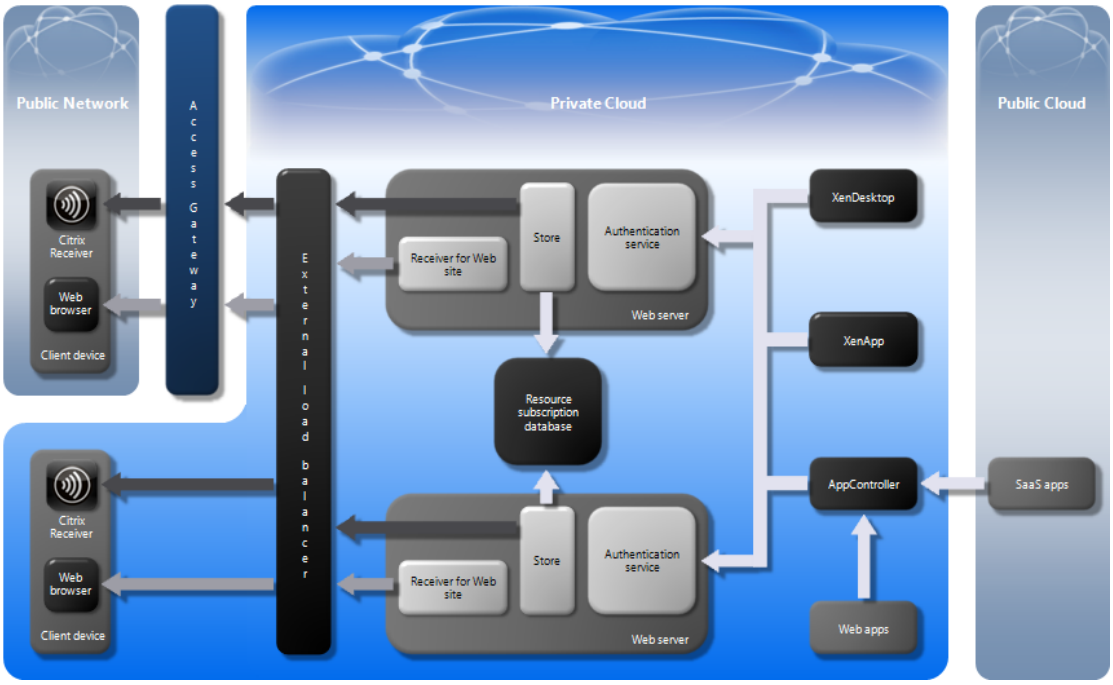
Citrix Receiver for Mac 11.4	Yes	Yes
Citrix Online Plug-in for Macintosh 11.2	Yes	Yes
Citrix Receiver for Linux 12.1	Yes	No
Citrix Receiver for Linux 12.0	Yes	No
Citrix Receiver for iOS 5.0.2	Yes	Yes

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 Receiver Storefront Deployment

Receiver 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. Receiver Storefront integrates with your existing XenDesktop and XenApp deployment.

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



Receiver Storefront Components

The following services provide the functionality of Receiver 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.
- **Resource subscription database**—stores details of user subscriptions, plus associated shortcut names and locations.

Three of the core components of Receiver Storefront, the authentication service, the stores, and the Receiver for Web sites, run on IIS. The other main component, the resource subscription database, requires SQL Server. Receiver 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 Receiver Storefront server. In multiple server environments, the resource subscription database can be hosted on one of the Receiver Storefront servers or on a dedicated database server.

Receiver Storefront servers and the resource 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 Receiver Storefront servers in the group must reside within the same domain.

Other Citrix Components

The following Citrix products and technologies integrate with Receiver Storefront to enable you to deliver desktops and applications to your users.

- **Citrix Receiver**—enables users to access their desktops and applications.
- **Access Gateway**—secures access to resources over public networks for remote users.
- **XenDesktop/XenApp**—provide desktops, content, and online and offline applications.
- **AppController**—enables pass-through authentication to both internal Web applications and third-party SaaS solutions. Provides centralized user account provisioning and reporting.

Include AppController in your deployment to provide pass-through authentication for Receiver Storefront users to Web applications hosted on your internal network and to software-as-a-service (SaaS) applications provided by third parties over public networks. This enables you to deliver Web applications seamlessly alongside XenDesktop and XenApp resources through Receiver Storefront stores.

Deploy Access Gateway to secure user connections to Receiver Storefront stores and Receiver for Web sites over public networks. This provides remote users with a single secure point of access to their desktops and applications while enabling you to control access to internal resources.

Third-Party Components

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

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

To configure a multiple server deployment for high availability, install your Receiver Storefront servers within a load-balanced environment. Configure the external load balancer for failover between servers to provide a fault-tolerant deployment. Consider implementing database mirroring or clustering to enable automatic failover and provide high availability of the resource subscription database.

Recommendations

When planning your Receiver Storefront deployment, consider the following recommendations.

- Citrix recommends hosting Receiver Storefront on a dedicated instance of IIS. Installing other Web applications on the same IIS instance as Receiver Storefront could have security implications for the overall Receiver Storefront infrastructure.

- In a production environment, Citrix recommends using HTTPS to secure communications between Receiver Storefront and users' devices. To use HTTPS, Receiver 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, Receiver Storefront uses HTTP for communications.

- Citrix recommends that you back up the resource subscription database regularly so that you can restore from the backup if the database fails.

User Access Options

Three different methods are available for users to access Receiver Storefront stores.

Direct Store Access

Users with compatible versions of Citrix Receiver can access Receiver Storefront stores directly by configuring Citrix Receiver with the store URL. For the Citrix Receiver versions that can be used to access stores directly, see System Requirements for Receiver Storefront 1.1.

Accessing stores directly from Citrix Receiver provides the best user experience and the greatest functionality. You can make the configuration process easier for users by making Citrix Receiver provisioning files available to them. By default, Receiver for Web sites offer users a provisioning file for the single store for which the site is configured. If you want to provide users with a provisioning file for multiple stores, you can manually export a file from Receiver Storefront that you can distribute. For more information on exporting provisioning files, see Configuring Stores.

Receiver for Web Sites

Users with compatible Web browsers can access Receiver Storefront stores by browsing to Receiver for Web sites. To access their desktops and applications, 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 Receiver Storefront 1.1.

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.

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 VPN connections, so users logging on through Access Gateway without a VPN connection cannot access Web applications for which AppController requires that a VPN connection is used.
- Subscribed desktops and 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 desktops and 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 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 Receiver Storefront 1.1.

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 Receiver Storefront authentication service.

User Authentication

Local Users

Receiver 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 Receiver Storefront, see Configuring the Authentication Service.

Remote Users

Deploy Access Gateway to secure connections to Receiver Storefront stores and Receiver for Web sites from remote users over public networks. Receiver Storefront supports pass-through authentication from Access Gateway. For more information about configuring pass-through authentication from Access Gateway, see Configuring the Authentication Service.

Depending on your Access Gateway configuration, users either log on to Citrix Receiver or directly to Access Gateway. Receiver 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 Receiver Storefront for Access Gateway, see To add an Access Gateway connection.

Distribute provisioning files to remote users make it easier for them to configure Citrix Receiver to access stores through Access Gateway. Provisioning files include connection details for any gateways and beacons configured for the stores for which the file was created. For more information on exporting provisioning files, see Configuring Stores.

When deployed with Access Gateway Enterprise Edition, Receiver Storefront supports the following authentication methods for remote users on public networks.

- **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.
- **Two-factor.** 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.

Pass-through Authentication to AppController

If you deploy Access Gateway and AppController, remote users can authenticate to Access Gateway and Citrix Receiver and then access their Web and software-as-a-service (SaaS) applications without needing to authenticate again. To access both Web and SaaS applications, remote users must use the Access Gateway Plug-in to log on to Access Gateway before logging on to Citrix Receiver.

For remote users who cannot install the Access Gateway Plug-in, you can enable clientless access with pass-through authentication to SaaS applications only. To do this, configure Access Gateway to act as a secure remote proxy and create a Receiver for Web site for the store containing the SaaS applications. Users log on to Access Gateway directly and use the Receiver for Web site to access their applications without needing to authenticate again.

Clientless access with pass-through authentication is supported with AppController 1.1 and Access Gateway 9.3, Enterprise Edition only. Users require one of the following supported client, operating system, and Web browser combinations.

Client	Operating system	Browser
Citrix Receiver for Windows 3.2	Windows 7 64-bit Editions with Service Pack 1	Internet Explorer 9 (32-bit mode) Google Chrome 17
	Windows 7 32-bit Editions with Service Pack 1	Internet Explorer 8 Mozilla Firefox 10
Citrix Receiver for Mac 11.5	Mac OS X 10.7 Lion	Safari 5.1
Citrix Receiver for Linux 12.1	Red Hat Enterprise Linux 6 Desktop Ubuntu 11.1 32-bit	Mozilla Firefox 9

Optimizing the User Experience

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

Content Redirection

Where users have subscribed to the appropriate application, content redirection enables local files on users' devices to be opened using subscribed applications. To enable redirection of local files, associate the application with the required file types in XenApp. File type association is enabled by default for Receiver Storefront stores. For more information about disabling file type association, see Configuring Receiver Storefront Using the Configuration Files.

Workspace Control

Workspace control lets desktops and 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 desktops and 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 desktops and applications that they left running. When users log off from the site, their desktops and applications are automatically shut down. This configuration enables a user to log on to a site, start their desktops and applications, and then, without logging off, log on to the same site using a different device and have those resources automatically transferred to the new device. All the desktops and applications that the user starts from a particular site are automatically shut down 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 sites are accessed from hosted desktops and applications.
- For users accessing sites through Internet Explorer, workspace control is only enabled if the site can detect that Citrix Receiver is installed on users' devices.
- Users must disconnect from their desktops and 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.
- To reconnect to disconnected desktops and applications, users accessing sites through Internet Explorer must add the site to the Local intranet or Trusted sites zones.

Additional Recommendations

In order that users do not have to log on separately to each store they access, ensure that all your stores use the same authentication service. This means that for a single-server deployment, all stores must be hosted on the same Receiver Storefront server. In multi-server deployments, all stores must use a single authentication service hosted on one of the servers in the deployment.

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

- 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.

  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.

- 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 move a published application to another folder.

Installing and Setting Up Receiver Storefront

To install and configure Receiver Storefront, carry out the following steps in order.

1. If you plan to use Receiver Storefront to deliver XenDesktop and XenApp resources to users, join the Receiver 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 Receiver Storefront server. In the case of multiple server deployments, SQL Server can either be installed on one of the Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver Storefront.

   Citrix recommends hosting Receiver Storefront on a dedicated instance of IIS. Installing other Web applications on the same IIS instance as Receiver Storefront could have security implications for the overall Receiver Storefront infrastructure.

8. Use the Citrix Receiver Storefront management console to configure your server.

To install Receiver Storefront

If you plan to use Receiver Storefront to deliver XenDesktop and XenApp resources to users, ensure that the Receiver 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 Receiver Storefront server. In the case of multiple server deployments, SQL Server can either be installed on one of the Receiver 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 Receiver Storefront servers.

Citrix recommends hosting Receiver Storefront on a dedicated instance of IIS. Installing other Web applications on the same IIS instance as Receiver Storefront could have security implications for the overall Receiver Storefront infrastructure.

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

2. Browse your installation media or download package, locate CitrixReceiverStorefront-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 Receiver 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 Receiver Storefront management console starts automatically so that you can configure your server.

To install Receiver Storefront from a command prompt

If you plan to use Receiver Storefront to deliver XenDesktop and XenApp resources to users, ensure that the Receiver 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 Receiver Storefront server. In the case of multiple server deployments, SQL Server can either be installed on one of the Receiver 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 Receiver Storefront servers.

Citrix recommends hosting Receiver Storefront on a dedicated instance of IIS. Installing other Web applications on the same IIS instance as Receiver Storefront could have security implications for the overall Receiver Storefront infrastructure.

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

2. Browse your installation media or download package, locate CitrixReceiverStorefront-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.

   CitrixReceiverStorefront-x64.exe [-silent]

   Use the -silent argument to perform a silent installation of Receiver 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-11/dws-first-auth-store.html

dws-deploy-single

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-11/dws-deploy-single.html

dws-deploy-multi

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-11/dws-deploy-multi.html

To set up a remote database

If you plan to use a remote database with a multiple server Receiver 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 Receiver 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.aspx.

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

   This service enables the Citrix Receiver 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.aspx.

4. To create the Receiver 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 = 4096KB ,
     MAXSIZE = UNLIMITED, FILEGROWTH = 10% )
   LOG ON
   ( NAME = N'MyApps_log', FILENAME = N'%%LOG_FILE%%' , SIZE = 560KB ,
     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 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 and add as members the computer accounts of the servers on which you plan to install Receiver Storefront.

   Creating a local group on the server hosting the database enables remote Receiver 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 domain name of the local group you created in the preceding step.

   ```
   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.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 Receiver 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 Receiver Storefront management console is not already open after installation of Receiver Storefront, click Start > All Programs > Citrix > Citrix Receiver Storefront.

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

3. Log on to the primary server in the Receiver Storefront deployment that you wish to join and open the Citrix Receiver 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 specify the name of the primary server in the existing server deployment that you wish to join. 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 Receiver Storefront management console, select the Server Group node. In the Actions pane, click Propagate Changes.

   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 Receiver 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 Receiver Storefront

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

The prerequisites and the resource subscription database, if installed, are not removed from the server.

Managing Your Receiver Storefront Deployment

After initial configuration of Receiver Storefront, further tasks that enable you to manage your deployment become available in the Citrix Receiver 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 Receiver 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 Receiver 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 Receiver Storefront deployment. This task is only available when the authentication service on the primary Receiver Storefront server has been removed.

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

2. Select the Authentication node in the left pane of the Citrix Receiver 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.

   Note: If you enable the pass-through from Access Gateway authentication method, configure gateways and beacons, and enable remote user access for your stores so that Citrix Receiver users can access Receiver Storefront through Access Gateway.

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 configuration of the secondary servers is 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 Receiver Storefront authentication service. Some advanced settings can only be changed by editing the authentication service configuration files. For more information, see Configuring Receiver 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 configuration of the secondary servers is 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 Receiver 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 Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront.

2. Select the Authentication node in the left pane of the Citrix Receiver 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.

   Note: If you enable the pass-through from Access Gateway authentication method, configure gateways and beacons, and enable remote user access for your stores so that Citrix Receiver users can access Receiver Storefront through Access Gateway.

To manage use of the authentication service by Merchandising Server appliances

Use the Manage Merchandising Servers task to specify any Merchandising Server appliances that you want to use the authentication service to identify users when delivering configurations for Citrix Receiver.

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

2. Select the Authentication node in the left pane of the Citrix Receiver Storefront management console and, in the Actions pane, click Manage Merchandising Servers.

3. Click Add to enter the URL of a Merchandising Server appliance that you want to use this authentication service. To modify a server URL, select the entry in the Server URLs list and click Edit. Select a URL in the list and click Remove to stop that Merchandising Server appliance using the authentication service for user identification.

   If you are using HTTPS for communications with the authentication service, ensure that you install Secure Sockets Layer (SSL) certificates on the Merchandising Server appliances.

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 for self-signed certificates generated by Receiver Storefront you periodically generate new security keys. 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 Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront.

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

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 Receiver 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. Receiver 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.

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 outside of your internal network. User resetting of expired passwords is disabled by default when you configure the authentication service.

dws-create-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-11/dws-create-store.html

Configuring Stores

Receiver Storefront stores enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users. The tasks described below 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 Receiver 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 configuration of the secondary servers is also updated.

To export 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 gateways 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 Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront. Select the Stores node in the left pane of the Citrix Receiver 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. Click Export.

3. Save the provisioning file with a .cr extension to a suitable location on your network.

To manage server farms

Use the Manage Server Farms task to add and remove XenDesktop, XenApp, and AppController resources from stores, and to modify the details of the infrastructure providing these resources.

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

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

3. 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

4. In the Add Server Farm or Edit Server Farm dialog box, specify a name and indicate whether the resources that you want to make available through the store are provided by a XenDesktop site, XenApp farm, or AppController virtual appliance. Click Add to enter the name or IP address of a XenDesktop or XenApp server running the Citrix XML Service, or of an AppController virtual appliance. To modify the name or IP address of a server or virtual appliance, select the entry in the Servers list and click Edit. Select an entry in the list and click Remove to stop Receiver Storefront contacting the server or virtual appliance to enumerate the resources available.

   Specify multiple servers or virtual appliances to enable fault tolerance, listing the entries in order of priority to set the failover order.

5. Select from the Transport type list the type of connections for Receiver Storefront to use for communications with the store.

   - To send data over unencrypted connections, select HTTP. If you select this option, you must make your own arrangements to secure connections to the store.

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

   - To send data over secure connections using the SSL Relay running on XenApp servers to perform host authentication and data encryption, select SSL Relay.

   Note: If you are using HTTPS or the SSL Relay to secure the connections between Receiver Storefront and XenDesktop sites or XenApp farms, ensure that the server name you specified in the Servers list matches exactly (including the case) the name on the certificate for the server running the Citrix XML Service.

6. Specify the port for Receiver Storefront to use for connections to XenDesktop sites, XenApp farms, and AppController in the XML Service port box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. For XenDesktop sites and XenApp farms, this port must match the port used by the Citrix XML Service.

7. If you are using the SSL Relay to secure the connections between Receiver Storefront and XenApp farms, 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.

Enabling Remote Access for Users

Use the Enable Remote Access task to specify the Access Gateway appliances that you want to use to enable users to access stores from public networks. If you add multiple gateways, specify a default gateway for the store. Before starting this task, ensure that you enable the pass-through from Access Gateway authentication method, add details of your Access Gateway appliances to Receiver Storefront, and configure beacon points to enable Citrix Receiver to determine whether users are connected to local or public networks.

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 Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront.

2. Select the Stores node in the left pane of the Citrix Receiver 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, select Ask users to contact their help desk for an account.

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

Changing the Database for a Store

Use the Change Database task to switch the SQL Server instance used by the store to record details of users' resource 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 and then edit the store configuration file to include details of the failover partner.

Click Test Connection to ensure that Receiver Storefront can access the database and that it is not already in use.

Note: The credentials with which you log on to the Receiver Storefront server are used to test the database connection. Ensure that this user account has permissions to access the database to enable Receiver 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 Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront.

2. Select the Stores node in the left pane of the Citrix Receiver 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 Receiver 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 for self-signed certificates generated by Receiver Storefront you periodically generate new security keys. 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 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 Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront.

2. Select the Receiver for Web node in the left pane of the Citrix Receiver 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 any changes that are required 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 configuration of the secondary servers is 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 also 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 configuration of the secondary servers is 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 provide Receiver Storefront with details of Access Gateway deployments through which users access your stores.

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

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

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

   Users see the display name you specify in the Citrix Receiver Preferences dialog box, so you should include relevant information in the name to help users decide whether to use the gateway. 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 gateway for their location.

4. Enter the URL of the user logon point for your Access Gateway deployment. Specify whether the logon point 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 Receiver Storefront for 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 gateway.

   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 gateway. Receiver Storefront uses the subnet IP address to verify that incoming requests originate from a trusted device.

6. If applicable, 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 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 Receiver 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 your deployment 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 order. Click Next.

   Receiver 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 order.

   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 multiple STAs are available and you 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, Receiver 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, Receiver Storefront is unable to contact two STAs, it falls back to using a single STA.

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

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

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 configuration of the secondary servers is also updated.

After adding details of your Access Gateway deployments, configure beacon points to enable Citrix Receiver to determine whether users are connected to local or public networks. To enable users to access stores from public networks, ensure that you also enable the pass-through from Access Gateway authentication method and enable remote user access for the store.

Configuring Access Gateway Connection Settings

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

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

If you change any Access Gateway details in the Receiver 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.

To change general Access Gateway settings

Use the Change General Settings task to modify the gateway name shown to users and to update the Receiver Storefront configuration if the logon point URL or deployment mode of your Access Gateway infrastructure changes.

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

2. Select the Gateways node in the left pane of the Citrix Receiver 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 gateway that will help users to identify it.

   Users see the display name you specify in the Citrix Receiver Preferences dialog box, so you should include relevant information in the name to help users decide whether to use the gateway. 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 gateway for their location.

4. Enter the URL of the user logon point for your Access Gateway deployment. Specify whether the logon point 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 Receiver 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 gateway.

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 gateway. Receiver Storefront uses the subnet IP address to verify that incoming requests originate from a trusted device.

6. If applicable, 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 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 update the Receiver Storefront configuration with the IP addresses or fully qualified domain names of the appliances in your Access Gateway cluster.

Enabling Silent User Authentication Through Access Gateway

Use the Enable Silent Authentication task to change the Access Gateway authentication service that Receiver 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 order.

To manage Secure Ticket Authorities

Use the Secure Ticket Authority task to update the list of Secure Ticket Authorities (STAs) from which Receiver Storefront obtains session tickets for users and to enable session reliability.

1. On the primary Receiver Storefront server in your deployment, click Start > All Programs > Citrix > Citrix Receiver Storefront.
2. Select the Gateways node in the left pane of the Citrix Receiver 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 Receiver Storefront obtaining session tickets from that STA.

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

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 multiple STAs are available and you 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, Receiver 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, Receiver 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 Receiver Storefront configuration. Once a gateway is removed, users are no longer be able to access the stores hosted on your Receiver Storefront deployment through that gateway.

To configure beacon points

Use the Manage Beacons task to update the Receiver 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.

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 configuration of the secondary servers is also updated.

If you change any beacon points in the Receiver 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.

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

2. Select the Beacons node in the left pane of the Citrix Receiver 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 Receiver Storefront is used as a beacon point within your internal network.

   Including at least two 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. For example, you could use your company's Web site and a highly available public Web site as external beacon points.

To enable users to access stores from public networks, enable the pass-through from Access Gateway authentication method, add details of your Access Gateway deployments to Receiver Storefront, and then enable remote user access for the store.

Configuring Server Groups

The tasks described below enable you to modify settings for your multiple server Receiver Storefront deployments. To manage your multiple server deployment, use only the Citrix Receiver 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 Receiver Storefront server to your existing deployment. For more information about joining new servers to existing Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver Storefront Using the Configuration Files

This topic describes additional configuration tasks that involve editing the Receiver 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 configuration of the secondary servers is also updated.

To enable ICA file signing

Receiver 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 Receiver Storefront, the ICA file generated when a user starts an application is signed using a certificate from the personal certificate store of the Receiver Storefront server. ICA files can be signed using any hash algorithm supported by the operating system running on the Receiver 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 Receiver 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.

1. Ensure that the certificate you want to use to sign ICA files is available in the Citrix Delivery Services certificate store on the Receiver Storefront server.

2. On the Receiver 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.

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

By default, contact between Receiver 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 Receiver 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 Receiver 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, Receiver Storefront uses the database server and database name that you enter to create a connection string for the resource subscription database. If you are using mirroring to provide high availability for the resource 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 Receiver 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 Receiver 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, Receiver 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 Receiver 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.

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 configuration of the secondary servers is also updated.

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, 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 Receiver Storefront. To disable detection and deployment of Citrix Receiver, edit the site configuration file. You can also configure the site to offer users with older clients the option to upgrade.

1. On the Receiver 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*sitepath*\ directory, where *sitepath* is the URL specified for the site when it was created.

2. Locate the following element in the file.

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

3. Change the value of the enabled attribute to false to disable detection and deployment of Citrix Receiver for the site. Alternatively, set the value of the upgradeAtLogin attribute to true to offer users with older clients the option to upgrade.

To configure workspace control

Workspace control lets desktops and 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 desktops and 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 Receiver 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*sitepath*\ directory, where *sitepath* is the URL specified for the site when it was created.

2. Locate the following element in the file.

   ```
   <workspaceControl enabled="true" autoReconnectAtLogon="true"
     terminateSessionsAtLogoff="true" 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 desktops and applications that they left running. To leave users' desktops and applications running after they log off from the site, set the value of the terminateSessionsAtLogoff attribute to false.

   By default, autoReconnectAtLogon and terminateSessionsAtLogoff are set to true. This configuration means that if a user logs on to a site, starts some desktops and applications, and then, without logging off, logs on to the same site using another device, those desktops and applications are automatically transferred to the new device. Additionally, all the desktops and applications that a user starts from a particular site are automatically shut down when the user logs off from the site, provided that the same browser is used to log on, start the desktops and applications, and log off.

   If you choose to disable automatic reconnection of desktops and applications at logon, enable the Reconnect link to provide users with a way to manually reconnect to desktops and applications that they left running.

4. Change the value of the showReconnectButton attribute to true to display on the site the Reconnect link, which enables users to manually reconnect to desktops and 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 desktops and applications without shutting them down.

   The Reconnect and Disconnect links do not appear on sites by default. Enable the links and disable automatic reconnection of desktops and applications at logon to enable users to choose whether they want their desktops and 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 gateways 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 Receiver 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*sitepath*\ directory, where *sitepath* is the URL specified for the site 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 Receiver 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*sitepath*\ directory, where *sitepath* is the URL specified for the site 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 desktops and applications. To change these settings, edit the site configuration file.

1. On the Receiver 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*sitepath*\ directory, where *sitepath* is the URL specified for the site 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 Receiver Storefront Deployment

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

Hosting Receiver Storefront. Citrix recommends hosting Receiver Storefront on a dedicated instance of Microsoft Internet Information Services (IIS). Installing other Web applications on the same IIS instance as Receiver Storefront could have security implications for the overall Receiver Storefront infrastructure.

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

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

Securing Receiver Storefront communications. In a production environment, Citrix recommends using the SSL Relay to secure data traffic between Receiver 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 Receiver 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 Receiver Storefront and users' devices using Access Gateway and HTTPS. To use HTTPS, Receiver 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, Receiver 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 Receiver Storefront servers. For more information about disabling protocols in IIS, see http://support.microsoft.com/kb/187498.

ICA file signing. Receiver 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 Receiver Storefront server, including SHA-1 and SHA-256. For more information about enabling ICA file signing in Receiver Storefront, see Configuring Receiver Storefront Using the Configuration Files.

Password reset. You can enable users whose passwords have expired to reset their passwords when they log on to Receiver 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 Receiver 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 Receiver Storefront stores.

- 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 configure shortcuts for user devices.

- 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.

  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.

- 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 move a published application to another folder.

To manage user access to Citrix Online applications with XenApp

You can configure Receiver 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 in a store, you can set up a separate store containing only those applications. Alternatively, you can use the fine-grained 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

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 Receiver 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 Receiver Storefront

Receiver Storefront supports Windows event logging for the authentication service, stores, and Receiver for Web sites. Any events that are generated are written to the Receiver 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 Receiver Storefront management console automatically records tracing information to files in the \Admin\logs\ directory of the Receiver 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 Receiver 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, Receiver Storefront is configured to limit the number of duplicate log entries to 10 per minute.

3. Change the value of the duplicateInterval parameter to the set the time period, in the format hh:mm:ss, over which duplicate log entries are monitored. Use the duplicateLimit parameter 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 Receiver 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 Receiver 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 Receiver Storefront installation, typically located at c:\Program Files\Citrix\Receiver Storefront\.