Delivery Services 1.0

2013-08-11 04:36:48 UTC

Contents

Delivery Services 1.0

Delivery Services authenticates users of Citrix Receiver with the Citrix Self-service Plug-in to XenDesktop sites and XenApp farms. The resources available are enumerated and aggregated by Delivery Services into stores that are displayed in the self-service view of Citrix Receiver. The Delivery Services database records details of users' subscriptions and resource shortcuts to enable application synchronization.

In This Section

This section of the library provides up-to-date product information about deploying, configuring, and managing Delivery Services. These task-based topics help you to set up Delivery Services quickly and easily. Readers are assumed to have some knowledge of XenDesktop and XenApp.

Features of Delivery Services	Installing and Setting Up Delivery Services
Known Issues in Delivery Services 1.0	Managing Your Delivery Services Deployment
System Requirements for Delivery Services 1.0	Securing Your Delivery Services Deployment

About Delivery Services

Delivery Services consists of three services that provide authentication and resource delivery infrastructure for Citrix Receiver and the Citrix Self-service Plug-in:

- The Authentication Service authenticates users to Citrix servers. Once a user's credentials have been validated, the Authentication Service handles all subsequent interactions with the servers to ensure that users do not need to log on again.
- Delivery Services stores enumerate the resources currently available from Citrix servers, sending the results to the Self-service Plug-in so the resources can be displayed to users.
- The Delivery Services database records details of users' subscriptions, plus associated shortcut names and locations. When a user accesses a store with application synchronization enabled, the subscribed resources on the user device are automatically reconfigured so that the configuration is the same as that stored in the Delivery Services database.

You manage the Delivery Services components with the Citrix Delivery Services Management console. If you want to perform certain advanced administration tasks, you may also need to edit the Delivery Services configuration files.

Features of Delivery Services

Authentication Service. The Delivery Services Authentication Service communicates with XenDesktop sites and XenApp farms to authenticate users. Once a user's credentials have been validated, the Authentication Service handles all subsequent interactions with the servers to ensure that users do not need to log on again.

Stores. Delivery Services stores enumerate the resources available to each authenticated user from XenDesktop sites and XenApp farms and send the results to the Citrix Receiver self-service view. Stores are also responsible for recording and retrieving users' application synchronization data, and passing this information to the self-service view so that any differences can be resolved.

Application synchronization. Subscribed resources now follow users from one Windows computer to the next, so that they do not need repeatedly to make the same changes each time they use a different Windows computer. When a user adds, removes, renames, or moves a resource in a store with application synchronization enabled, details of the change are recorded in the store. Subsequently, whenever the user accesses the store from a different device running Citrix Receiver with the Citrix Self-service Plug-in for Windows, the same changes are automatically applied to the new device.

Integration with Citrix Online products. Delivery Services stores can be configured to include Citrix Online products, such as GoToMeeting, GoToWebinar, and GoToTraining, along with the other resources. When users subscribe to a Citrix Online product, the associated client application is installed locally. Where Citrix Online accounts are not already available, users can be prompted to set up a trial account or to request an account from the IT department.

Citrix Delivery Services Management console. The Citrix Delivery Services Management console is a Microsoft Management Console (MMC) 3.0 snap-in that enables you to create and configure stores and the Authentication Service hosted on Delivery Services. The Citrix Delivery Services Management console enables you to perform day-to-day administration tasks quickly and easily.

How Delivery Services Works

Delivery Services employs Microsoft .NET technology running on Internet Information Services (IIS) and, optionally, Microsoft SQL Server to provide authentication and resource delivery infrastructure for Citrix Receiver and the Citrix Self-service Plug-in. Delivery Services integrates with your existing XenDesktop and XenApp infrastructure. An example of a typical deployment is shown below. This environment consists of the following components.

Authentication Service—authenticates users to the Citrix servers using explicit authentication and stores user credentials.

Stores—retrieve user credentials from the Authentication Service to authenticate users to the Citrix servers. Enumerate the resources currently available from the configured servers and send the details to the Self-service Plug-in.

Database—stores details of user subscriptions plus associated shortcut names and locations.

Citrix Delivery Services Management console—enables administrators to create and manage stores and the Authentication Service.

Citrix servers—provide desktops, content, and online and offline applications.

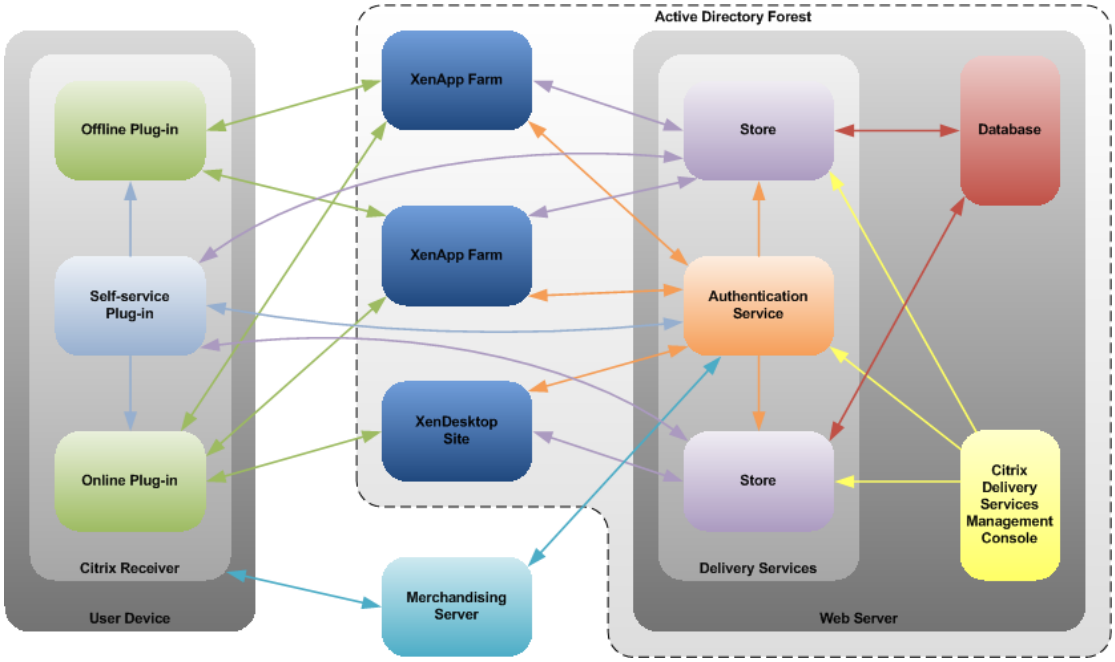
Self-service Plug-in—presents the resources and services available across the configured stores. Enables users to subscribe to and organize their resources. Integrated into and managed by Citrix Receiver.

Online Plug-in/Offline Plug-in—enable users to access their subscribed resources. Integrated into and managed by Citrix Receiver.

Citrix Receiver—manages plug-ins, including the Self-service Plug-in, on the user device.

Merchandising Server—delivers plug-ins and configuration updates to Citrix Receiver. Uses the Authentication Service to identify users.

The figure shows the architecture of Delivery Services and the interactions between the components in a typical environment.



The interactions that take place between the components in the environment shown above are described below.

- A user logs on to a device; Citrix Receiver starts automatically.
- If the user has not yet subscribed to any resources or if the user opens Citrix Receiver, the self-service view is displayed.
- The user logs on to the stores that the Self-service Plug-in is configured to contact.
- The Self-service Plug-in sends the user's credentials to the Authentication Service.
- Merchandising Server uses the Authentication Service to identify the user and sends any configuration updates specified by the administrator to Citrix Receiver.
- The Authentication Service authenticates the user to the Citrix servers that provide the resources in the stores.
- Using the Authentication Service to provide the user's credentials, the stores contact the Citrix servers, obtain details of the available resources, and send this information to the Self-service Plug-in.
- The Self-service Plug-in aggregates the resources from all the stores, but only those resources that the administrator has made available for this particular user are displayed in Citrix Receiver.
- When application synchronization is enabled for a store, the store queries the Delivery Services database and sends details of the user's subscribed resources and associated shortcuts to the Self-service Plug-in as part of the resource enumeration process.
- The Self-service Plug-in compares the configuration received from the store with the configuration of the current device to determine whether the user has subscribed or unsubscribed from any resources, or modified any shortcuts on any other devices.

- If any differences are detected between the user's subscriptions on the current device and the configuration stored in the database, the Self-service Plug-in automatically adds and removes resources and moves or renames shortcuts to resolve the differences.
- The user subscribes to and organizes resources in the self-service view of Citrix Receiver.
- Shortcuts to the subscribed resources are added to the user's device.
- Any offline applications to which the user subscribes are downloaded from the XenApp farm to the user device by the Offline Plug-in. Once downloading is complete, the applications are available for use.
- If the user subscribes to a Citrix Online product, the associated client application is installed locally on the device. If configured by the administrator, the user may also be prompted to create a Citrix Online account or request an account from the IT department.
- When application synchronization is enabled for a store, the Self-service Plug-in notifies the store of any changes to the user's subscribed resources and associated shortcuts. The store updates the database with the new configuration.
- The user clicks on a shortcut to a subscribed resource.
- For offline applications, the application starts and runs locally within an isolation environment.

  For desktops, content, and online applications, the Online Plug-in initiates a session with a XenDesktop or XenApp server providing the selected resource.

Known Issues in Delivery Services 1.0

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

Delivery Services cannot be removed when the Citrix Delivery Services Management console is open

Attempting to remove Delivery Services while the Citrix Delivery Services Management console is open may cause the removal process to stop responding. [#253363]

Delivery Services installer does not enable the IIS Management Console role service

The role service that installs the Internet Information Services (IIS) Manager console is not enabled by default when Delivery Services is installed. To access the console, manually enable the **Management Tools** > **IIS Management Console** role service for the **Web Server (IIS)** role on your Delivery Services server. [#253746]

System Requirements for Delivery Services 1.0

This topic lists the supported Citrix product versions and platform requirements for installing Delivery Services. It is assumed that your servers meet the minimum hardware requirements for the installed operating system.

Citrix Server Requirements

Delivery Services supports the following product versions.

- Citrix XenDesktop 5.0
- Citrix XenDesktop 4.0
- Citrix XenDesktop 3.0
- 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

- Citrix XenApp 4.0, with Feature Pack 2, for UNIX Operating Systems
- Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems

Delivery Services operates with these products on all of their supported platforms. For a list of supported platforms, see the documentation for your Citrix product. Citrix recommends that you install the latest service pack for the operating system on your servers.

If you plan to enable Merchandising Server to use the Authentication Service to identify users when delivering configurations for Citrix Receiver, Citrix Merchandising Server 2.1 is required.

Web Server Requirements

Delivery Services is only supported for installation on Windows Server 2008 R2. The components listed below are also required on the Web server. If any of these prerequisites are not already present, the Delivery Service installer adds them before installing the product.

- Microsoft Internet Information Services 7.5
- Microsoft .NET Framework 3.5 with Service Pack 1
- Microsoft Visual J#.NET 2.0 Second Edition

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 Delivery Services can be installed.

Delivery Services requires a Microsoft SQL Server 2008 R2 database to provide the application synchronization feature. If a suitable database is not installed on the Web server, application synchronization cannot be enabled.

User Device Requirements

Delivery Services requires that, at minimum, Citrix Receiver 2.1 and the Citrix Self-service Plug-in for Windows 2.0 is installed on the user device, plus a compatible version of the Citrix Online Plug-in. If you plan to deliver offline applications to users, the Citrix Offline Plug-in 6.0 is required. If you want to deliver Microsoft Application Virtualization (App-V) sequences to users, a supported version of the Microsoft Application Virtualization Desktop Client is required. For more information, see System Requirements for the Citrix Self-service Plug-in for Windows 2.0.

Planning Your Delivery Services Deployment

When determining how best to deploy Delivery Services within your existing Citrix environment, consider the following requirements and limitations.

- Delivery Services is currently only supported for single-server deployments, with one Authentication Service per server. In the current release, Delivery Services does not support parallel deployments for load balancing and failover.

- The number of Citrix Receiver users supported by a single Delivery Services deployment depends on the specifications of the Delivery Services server and on the level of user activity. Based on tests using a server with twin 2 GHz quad-core CPUs and 8 GB RAM, Delivery Services supports up to 25,000 users per hour in a light usage scenario (users log on, enumerate their resources, and access existing subscribed resources) or up to 6000 users per hour in an intensive usage scenario (users log on, enumerate their resources, and then subscribe and unsubscribe to a resource.)

- The Citrix Delivery Services Management console must be installed locally on the Delivery Services server and cannot be used for management of remote Delivery Services instances.

- The Delivery Services server must reside within the same Active Directory forest as the XenDesktop and XenApp servers hosting users' resources. To use application synchronization with XenDesktop 3.0, XenApp 5.0, or XenApp for UNIX, the Delivery Services server must reside within the same domain as the XenDesktop or XenApp servers.

- To use the application synchronization feature, a local Microsoft SQL Server database is required on the Delivery Services server. This means that you cannot use high availability configurations of SQL Server, such as mirroring and failover clustering. If you decide to enable application synchronization, Citrix recommends that you back up the database regularly so that you can restore from the backup if the database fails.

- XenDesktop servers must be members of a site and XenApp servers must be members of a farm. The servers must have resources (applications, content, and desktops) available to users. For more information about grouping servers and making resources available, see the documentation for your Citrix server.

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

- In a production environment, Citrix recommends installing a Secure Sockets Layer (SSL) certificate on the IIS site hosting Delivery Services and using HTTPS to secure communications between Delivery Services and users' devices.

- To enable single sign-on to multiple stores for users, all the stores must use the same Authentication Service. Since, in the current release, stores are automatically

- In the current release, Delivery Services supports only explicit authentication of users. Two-factor authentication and smart card authentication are not supported.

- To access their resources through Delivery Services, users of Windows devices require, at minimum, Citrix Receiver and the Self-service Plug-in, plus a compatible version of the Online Plug-in. If you plan to deliver offline applications to your users, the Offline Plug-in is also required.

Installing and Setting Up Delivery Services

To install Delivery Services, Citrix recommends that you carry out the following steps in order.

1. Join the Delivery Services server to a domain within the Active Directory forest that contains your XenDesktop sites and XenApp farms.

2. Optionally, install the **Web Server (IIS)** role on the Delivery Services server and then enable 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** > **Security** > **Windows Authentication**, **Request Filtering**

   - **Management Tools** > **IIS Management Scripts and Tools**

   - **Management Tools** > **IIS 6 Management Compatibility** > **IIS 6 Metabase Compatibility**, **IIS 6 WMI Compatibility**, **IIS 6 Scripting Tools**

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

3. Optionally, use the Internet Information Services (IIS) Manager console on the Delivery Services 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.

4. If you installed a server certificate on the Delivery Services server, configure HTTPS binding on port 443 for the default Web site. For more information, see http://technet.microsoft.com/en-us/library/cc731692(WS.10).aspx.

5. If you plan to enable application synchronization, install Microsoft SQL Server 2008 R2 on the Delivery Services server. For more information, see http://technet.microsoft.com/en-us/library/bb500469.aspx.

6. Install Delivery Services.

7. Use the Citrix Delivery Services Management Console to configure the Authentication Service and create your first store.

To install Delivery Services

Before starting the installation, ensure that the Delivery Services server is joined to a domain within the Active Directory forest containing your Citrix servers. If you plan to enable the application synchronization feature, install Microsoft SQL Server 2008 R2 on the Delivery Services server.

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

2. Browse your installation media or download package, locate CitrixDeliveryServices-x64.exe, and run the file as an administrator.

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 Delivery Services components are listed for installation and click **Install**.

   Before the components are installed, the following prerequisites are deployed if they are not already configured on the server.

   - Microsoft Internet Information Services

     The Web Server (IIS) role is installed, if necessary, and any of the following role services that are missing are enabled.

     - Static Content
     - Default Document
     - HTTP Errors
     - HTTP Redirection
     - ASP.NET
     - .NET Extensibility
     - ISAPI Extensions
     - ISAPI Filters
     - Windows Authentication
     - Request Filtering
     - IIS Management Scripts and Tools
     - IIS 6 Metabase Compatibility

- IIS 6 WMI Compatibility
- IIS 6 Scripting Tools

- Microsoft Visual J#.NET 2.0 Second Edition

6. When the installation is complete, click **Finish**.

   The Citrix Delivery Services Management console starts automatically so that you can configure the Authentication Service and create your first store.

To install Delivery Services from a command prompt

Before starting the installation, ensure that the Delivery Services server is joined to a domain within the Active Directory forest containing your Citrix servers. If you plan to enable the application synchronization feature, install Microsoft SQL Server 2008 R2 on the Delivery Services server.

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

2. Copy the file CitrixDeliveryServices-x64.exe 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.

   ```
   CitrixDeliveryServices-x64.exe [-s] [-unpack custominstallationlocation]
   ```

   Use the -s or -silent argument to perform a silent installation of Delivery Services and all the prerequisites. The -unpack argument enables you to install Delivery Services in the specified directory rather than the default installation location.

To configure the Authentication Service and create your first store

After installing Delivery Services, set up the Authentication Service that will authenticate users to your Citrix servers. Once the Authentication Service is configured, you create a store to enumerate the resources currently available for users.

1. If the Citrix Delivery Services Management console is not already open after installation of Delivery Services, click **Start** > **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. In the results pane of the Citrix Delivery Services Management console, click **Quick Start**.

3. On the **Authentication Service Location** page, specify a name for the Authentication Service.

4. Select a Microsoft Internet Information Services (IIS) site to host the Authentication Service and specify a location within that site for the service. Click **Next**.

   If the specified IIS site does not have a Secure Sockets Layer (SSL) certificate installed, Delivery Services generates a self-signed certificate for token management and uses HTTP for communications. Self-signed certificates generated by Delivery Services should not be used for any other purpose. In a production environment, Citrix recommends using SSL certificates for token management and securing Delivery Services communications with HTTPS.

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

5. On the **Authentication Points** page, add to the **Servers** list the name or IP address of at least one server running the Citrix XML Service for each of your XenDesktop sites and XenApp farms to perform user authentication. Specify more than one server to enable fault tolerance for a site or farm, listing the servers in order of priority to set the failover order.

   If you use XenDesktop 3.0, XenApp 5.0, or XenApp for UNIX servers for user authentication and you plan to enable application synchronization, further configuration of Delivery Services is required. For more information, see Configuring Delivery Services Using the Configuration Files.

6. Select from the **Transport type** list the type of connections that Delivery Services will use for communications with the Authentication Service.

   - To send data over unencrypted connections, select **HTTP**. If you select this option, you will need to make your own arrangements to secure connections to the Authentication Service.

- To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select **HTTPS**. If you select this option, ensure that the Citrix XML Service on your XenDesktop and XenApp servers is set to share a port with 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 Delivery Services and your XenDesktop sites and XenApp farms, ensure the server names you specified in the **Servers** list match exactly (including the case) the names on the certificates for the servers running XenDesktop and XenApp.

7. Specify the port that Delivery Services will use for connections to your XenDesktop sites and XenApp farms in the **XML Service port** box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service in your XenDesktop sites and XenApp farms.

8. If you are using the SSL Relay to secure the connections between Delivery Services and your XenApp farms, specify the TCP port of the SSL Relay in the **SSL Relay port** box. The default port is 443. Ensure all the servers running the SSL Relay are configured to listen on the same port. Click **Next**.

9. On the **Merchandising Servers** page, list the names or IP addresses of any Merchandising Server appliances that you want to use this Authentication Service to identify users when delivering configurations for Citrix Receiver. Click **Next**.

10. On the **Store Service Location** page, specify a name for your first store. Select an IIS site to host the store and specify a location within that site for the store. Click **Next**.

    If the specified IIS site does not have an SSL certificate installed, Delivery Services generates a self-signed certificate for token management and uses HTTP for communications. Delivery Services registers the certificate for the new store with the Authentication Service you created in the preceding steps and, similarly, registers the certificate for the Authentication Service with the new store. The Authentication Service is configured to trust the new store.

11. On the **Server Farm** page, specify in the **Farm name** box a name for a XenDesktop site or XenApp farm providing the resources that you want to make available through the store. In the **Servers** list, enter the name or IP address of at least one server running the Citrix XML Service for the site or farm. Specify more than one server to enable fault tolerance for the site or farm, listing the servers in order of priority to set the failover order.

12. Select from the **Transport type** list the type of connections that Delivery Services will use for communications with the store.

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

    - To send data over secure HTTP connections using SSL or TLS, select **HTTPS**. If you select this option, ensure that the Citrix XML Service on your XenDesktop or XenApp servers is set to share its port with 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 Delivery Services and your XenDesktop site or XenApp farm, ensure the server names you specified in the **Servers** list match exactly (including the case) the names on the certificate for the server running XenDesktop or XenApp.

13. Specify the port that Delivery Services will use for connections to your XenDesktop site or XenApp farm in the **XML Service port** box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service in your site or farm.

14. If you are using the SSL Relay to secure the connections between Delivery Services and your XenApp farms, specify the TCP port of the SSL Relay in the **SSL Relay port** box. The default port is 443. Ensure all the servers running the SSL Relay are configured to listen on the same port. Click **Next**.

15. 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. Click **Next**.

    - 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**.

    Click **Try it Free** to visit the Citrix Web site and set up a free corporate trial of GoToMeeting.

16. On the **Synchronize Applications** page, specify whether or not to enable application synchronization in the store for users of Citrix Receiver with the Citrix Self-service Plug-in for Windows and click **Next**.

    When a Windows device user subscribes to or unsubscribes from a resource, or moves or renames shortcuts, in a store with application synchronization enabled, details of the change are recorded. Subsequently, whenever the user accesses the store from a different Windows device, the same changes are automatically applied to the new device.

    A locally installed Microsoft SQL Server 2008 R2 database is required to provide the application synchronization feature. To use application synchronization with XenDesktop 3.0, XenApp 5.0, and XenApp for UNIX, further configuration of Delivery Services is required. For more information, see Configuring Delivery Services Using the Configuration Files.

17. On the **Review Settings** page, check that the details are correct and click **Create**.

18. Once the Authentication Service and the store have been created, click **Finish**.

    The URLs to enable Merchandising Server to access the Authentication Service and for users to access the new store are displayed. Details of the certificates to be used by the Authentication Service and the store for token management are also shown.

If you are using HTTPS for communications with the Authentication Service, ensure that you install an SSL certificate on the Merchandising Server appliance.

After configuring the Authentication Service and creating a store, further tasks become available in the Citrix Delivery Services Management console. For example, you can modify the Authentication Service and the store, or create more stores. For more information, see Managing Your Delivery Services Deployment.

Uninstalling Delivery Services

1. Log on to the Delivery Services server using an account with local administrator permissions.
2. On the Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.
3. Using the Citrix Delivery Services Management console, remove all the stores and then remove the Authentication Service. For more information, see Repairing and Removing the Authentication Service and Stores.
4. On the Windows **Start** menu, click **Control Panel** > **Programs and Features**.
5. Select **Citrix Delivery Services** and click **Uninstall** to remove all Delivery Services components from the server.

The prerequisites and the application synchronization database, if installed, are not removed from the server.

Managing Your Delivery Services Deployment

After configuring the Authentication Service and creating a store, further tasks that enable you to manage your deployment become available in the Citrix Delivery Services Management console.

The topics in this section describe:

- Configuring the Authentication Service
- Modifying Authentication Service settings
- Creating stores
- Modifying store settings
- Managing certificates for stores and the Authentication Service
- Repairing and removing stores and the Authentication Service
- Configuring Delivery Services using the configuration files

To configure the Authentication Service

Use the **Create Authentication Service** task to configure the Delivery Services Authentication Service. You can only configure one Authentication Service per Delivery Services installation. This task is only available when the Authentication Service on the Delivery Services server has been removed.

1. On the Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. Select the **Authentication** node in the left pane of the Citrix Delivery Services Management console and, in the **Actions** pane, click **Create Authentication Service**.

3. On the **Authentication Service Location** page, specify a name for the Authentication Service.

4. Select a Microsoft Internet Information Services (IIS) site to host the Authentication Service and specify a location within that site for the service. Click **Next**.

   If the specified IIS site does not have a Secure Sockets Layer (SSL) certificate installed, Delivery Services generates a self-signed certificate for token management and uses HTTP for communications.

   Citrix recommends hosting Delivery Services on a dedicated instance of IIS. Installing other Web applications on the same IIS instance as Delivery Services could have security implications for the overall Delivery Services infrastructure. Self-signed certificates generated by Delivery Services should not be used for any other purpose. In a production environment, Citrix recommends using SSL certificates for token management and securing Delivery Services communications with HTTPS.

5. On the **Authentication Points** page, add to the **Servers** list the name or IP address of at least one server running the Citrix XML Service for each of your XenDesktop sites and XenApp farms to perform user authentication. Specify more than one server to enable fault tolerance for a site or farm, listing the servers in order of priority to set the failover order.

   If you use XenDesktop 3.0, XenApp 5.0, or XenApp for UNIX servers for user authentication and you plan to enable application synchronization, further configuration of Delivery Services is required. For more information, see Configuring Delivery Services Using the Configuration Files.

6. Select from the **Transport type** list the type of connections that Delivery Services will use for communications with the Authentication Service.

   - To send data over unencrypted connections, select **HTTP**. If you select this option, you will need to make your own arrangements to secure connections to the Authentication Service.

   - To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select **HTTPS**. If you select this option, ensure that the Citrix XML Service on your XenDesktop and XenApp servers is set to share a port with 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 Delivery Services and your XenDesktop sites and XenApp farms, ensure the server names you specified in the **Servers** list match exactly (including the case) the names on the certificates for the servers running XenDesktop and XenApp.

7. Specify the port that Delivery Services will use for connections to your XenDesktop sites and XenApp farms in the **XML Service port** box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service in your XenDesktop sites and XenApp farms.

8. If you are using the SSL Relay to secure the connections between Delivery Services and your XenApp farms, specify the TCP port of the SSL Relay in the **SSL Relay port** box. The default port is 443. Ensure all the servers running the SSL Relay are configured to listen on the same port. Click **Next**.

9. On the **Merchandising Servers** page, list the names or IP addresses of any Merchandising Server appliances that you want to use this Authentication Service to identify users when delivering configurations for Citrix Receiver. Click **Next**.

10. On the **Review Settings** page, check that the details are correct and click **Create**.

11. Once the Authentication Service has been created, click **Finish**.

    The URL to enable Merchandising Server to access the Authentication Service is displayed, along with details of the certificate to be used for token management. If you are using HTTPS for communications with the Authentication Service, ensure that you install an SSL certificate on the Merchandising Server appliance.

Managing the Authentication Service

The tasks described below enable you to configure the Authentication Service. You can also manage the certificate installed on the Microsoft Internet Information Services (IIS) site for the Authentication Service and repair or remove the service.

To manage authentication points

Use the **Manage Authentication Points** task to specify the servers running the Citrix XML Service that authenticate users to your XenDesktop sites and XenApp farms for the Authentication Service, and to configure communication with these servers.

1. On the Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. Select the **Authentication** node in the left pane of the Citrix Delivery Services Management console and, in the **Actions** pane, click **Manage Authentication Points**.

3. Click **Add** to enter the name or IP address of another server running the Citrix XML Service and performing user authentication for a XenDesktop site or XenApp farm. To modify a server name or IP address, select the entry in the **Servers** list and click **Edit**. Select a server name or IP address in the list and click **Remove** to stop the server performing user authentication.

   Specify more than one server to enable fault tolerance for a site or farm, listing the servers in order of priority to set the failover order.

   If you use XenDesktop 3.0, XenApp 5.0, or XenApp for UNIX servers for user authentication and you plan to enable application synchronization, further configuration of Delivery Services is required. For more information, see Configuring Delivery Services Using the Configuration Files.

4. Select from the **Transport type** list the type of connections that Delivery Services will use for communications with the Authentication Service.

   - To send data over unencrypted connections, select **HTTP**. If you select this option, you will need to make your own arrangements to secure connections to the Authentication Service.

   - To send data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), select **HTTPS**. If you select this option, ensure that the Citrix XML Service on your XenDesktop and XenApp servers is set to share a port with 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 Delivery Services and your XenDesktop sites and XenApp farms, ensure the server names you specified in the **Servers** list match exactly (including the case) the names

on the certificates for the servers running XenDesktop and XenApp.

5. Specify the port that Delivery Services will use for connections to your XenDesktop sites and XenApp farms in the **XML Service port** box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service in your XenDesktop sites and XenApp farms.

6. If you are using the SSL Relay to secure the connections between Delivery Services and your XenApp farms, specify the TCP port of the SSL Relay in the **SSL Relay port** box. The default port is 443. Ensure all the servers running the SSL Relay are configured to listen on the same port. Click **Next**.

Enabling Users to Change Expired Passwords

Use the **Manage Password Options** task to enable users to reset expired passwords when logging on to the stores that use the Authentication Service. When this setting is enabled, users who cannot log on because their passwords have expired are redirected to the **Change Password** dialog box. Delivery Services contacts XenDesktop sites and XenApp farms in the order in which they are defined in the **Farms** list in the **Manage Server Farms** dialog box. If the password reset request fails, the next site or farm in the sequence is issued the password reset request. Delivery Services works through the list until a site or farm reports that the user's password has been reset successfully, at which point the process stops.

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. In stores that aggregate XenApp for UNIX farms with XenDesktop sites or XenApp for Windows farms, only the Windows password can be changed. For mixed XenApp farm deployments, use suitable password replication mechanisms between your farms to ensure that user passwords remain consistent.

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.

To manage the 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 Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. Select the **Authentication** node in the left pane of the Citrix Delivery Services Management console and, in the **Actions** pane, click **Manage Merchandising Servers**.

3. Click **Add** to enter the name or IP address of a Merchandising Server appliance that you want to use this Authentication Service. To modify a server name or IP address, select

the entry in the **Servers** list and click **Edit**. Select a server name or IP address in the list and click **Remove** to stop the 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 SSL certificates on the Merchandising Server appliances.

To create a store

Use the **Create Store Service** task to add stores. You can create as many stores as you need; for example, you may want to create a store for a particular group of users or to aggregate a specific set of resources. All the stores in a Delivery Services installation use the same Authentication Service.

1. On the Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. Select the **Stores** node in the left pane of the Citrix Delivery Services Management console and, in the **Actions** pane, click **Create Store Service**.

3. On the **Store Service Location** page, specify a name for the store. Select a Microsoft Internet Information Services (IIS) site to host the store and specify a location within that site for the store. Click **Next**.

   If the specified IIS site does not have a Secure Sockets Layer (SSL) certificate installed, Delivery Services generates a self-signed certificate for token management and uses HTTP for communications. Delivery Services registers the certificate for the new store with the Authentication Service and, similarly, registers the certificate for the Authentication Service with the new store. The Authentication Service is configured to trust the new store.

   Self-signed certificates generated by Delivery Services should not be used for any other purpose. In a production environment, Citrix recommends using SSL certificates for token management and securing Delivery Services communications with HTTPS.

4. On the **Server Farm** page, specify in the **Farm name** box a name for a XenDesktop site or XenApp farm providing the resources that you want to make available through the store. In the **Servers** list, enter the name or IP address of at least one server running the Citrix XML Service for the site or farm. Specify more than one server to enable fault tolerance for the site or farm, listing the servers in order of priority to set the failover order.

5. Select from the **Transport type** list the type of connections that Delivery Services will use for communications with the store.

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

   - To send data over secure HTTP connections using SSL or Transport Layer Security (TLS), select **HTTPS**. If you select this option, ensure that the Citrix XML Service on your XenDesktop or XenApp servers is set to share its port with 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 Delivery Services and your XenDesktop site or XenApp farm, ensure the server names you specified in the **Servers** list match exactly (including the case) the names on the

certificate for the server running XenDesktop or XenApp.

6. Specify the port that Delivery Services will use for connections to your XenDesktop site or XenApp farm in the **XML Service port** box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service in your site or farm.

7. If you are using the SSL Relay to secure the connections between Delivery Services and your XenApp farms, specify the TCP port of the SSL Relay in the **SSL Relay port** box. The default port is 443. Ensure all the servers running the SSL Relay are configured to listen on the same port. Click **Next**.

8. 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. Click **Next**.

   - 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**.

   Click **Try it Free** to visit the Citrix Web site and set up a free corporate trial of GoToMeeting.

9. On the **Synchronize Applications** page, specify whether or not to enable application synchronization in the store for users of Citrix Receiver with the Citrix Self-service Plug-in for Windows and click **Next**.

   When a Windows device user subscribes to or unsubscribes from a resource, or moves or renames shortcuts, in a store with application synchronization enabled, details of the change are recorded. Subsequently, whenever the user accesses the store from a different Windows device, the same changes are automatically applied to the new device.

   A locally installed Microsoft SQL Server 2008 R2 database is required to provide the application synchronization feature. To use application synchronization with XenDesktop 3.0, XenApp 5.0, and XenApp for UNIX, further configuration of Delivery Services is required. For more information, see Configuring Delivery Services Using the Configuration Files.

10. On the **Review Settings** page, check that the details are correct and click **Create**.

11. Once the store has been created, click **Finish**.

    The URL for users to access the new store is displayed, along with details of the certificates to be used for token management by the Authentication Service and the store.

Managing Stores

The tasks described below enable you to configure stores. You can also manage the certificates installed on the Microsoft Internet Information Services (IIS) site for the stores and repair or remove stores.

To manage server farms

Use the **Manage Server Farms** task to add and remove XenDesktop sites and XenApp farms from stores, and to modify the details of these sites and farms.

1. On the Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. Select the **Stores** node in the left pane of the Citrix Delivery Services Management console and, in the results pane, select a store. In the **Actions** pane, click **Manage Server Farms**.

3. Click **Add** to include the resources from another XenDesktop site or XenApp farm in the store. To modify the settings for a site or farm, select the entry in the **Farms** list and click **Edit**. Select a site or farm in the list and click **Remove** to remove the resources provided by the site or farm from the store.

   The order in which sites and farms are defined in the list determines the order in which user password reset requests are issued when the password reset feature is enabled.

4. In the **Edit Server Farm** dialog box, specify in the **Farm name** box a name for the XenDesktop site or XenApp farm providing the resources made available through the store. Click **Add** to enter the name or IP address of a server running the Citrix XML Service for the site or farm. To modify a server name or IP address, select the entry in the **Servers** list and click **Edit**. Select a server name or IP address in the list and click **Remove** to stop Delivery Services contacting the server to enumerate the resources available from the site or farm.

   Specify more than one server to enable fault tolerance for the site or farm, listing the servers in order of priority to set the failover order.

5. Select from the **Transport type** list the type of connections that Delivery Services will use for communications with the store.

   - To send data over unencrypted connections, select **HTTP**. If you select this option, you will need to 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, ensure that the Citrix XML Service on your XenDesktop or XenApp servers is set to share its port with 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 Delivery Services and your XenDesktop site or XenApp farm, ensure the server names you specified in the **Servers** list match exactly (including the case) the names on the certificate for the server running XenDesktop or XenApp.

6. Specify the port that Delivery Services will use for connections to your XenDesktop site or XenApp farm in the **XML Service port** box. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. This port must match the port used by the Citrix XML Service in your site or farm.

7. If you are using the SSL Relay to secure the connections between Delivery Services and your XenApp farms, specify the TCP port of the SSL Relay in the **SSL Relay port** box. The default port is 443. Ensure all the servers running the SSL Relay are configured to listen on the same port. Click **Next**.

Configuring Application Synchronization

Use the **Synchronize Applications** task to specify whether or not application synchronization is enabled in a store for users of Citrix Receiver with the Citrix Self-service Plug-in for Windows. When a Windows device user subscribes to or unsubscribes from a resource, or moves or renames the shortcuts, in a store with application synchronization enabled, details of the change are recorded. Subsequently, whenever the user accesses the store from a different Windows device, the same changes are automatically applied to the new device.

A locally installed Microsoft SQL Server 2008 R2 database is required to provide the application synchronization feature. To use application synchronization with XenDesktop 3.0, XenApp 5.0, and XenApp for UNIX, further configuration of Delivery Services is required. For more information, see Configuring Delivery Services Using the Configuration Files.

To manage Citrix Online application integration

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 Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

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

3. Select the 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**.

Click **Try it Free** to visit the Citrix Web site and set up a free corporate trial of GoToMeeting.

To manage certificates

Use the **Change Certificates** task to manage the certificates installed on the IIS site for the Authentication Service and stores.

1. On the Windows **Start** menu, click **All Programs** > **Citrix** > **Citrix Delivery Services Management**.

2. Select the appropriate node in the left pane of the Citrix Delivery Services Management console and, if necessary, select a service in the results pane. In the **Actions** pane, click **Change Certificates**.

3. Select from the list a certificate to use from the certificate store on the Delivery Services server. Click **View** to see information about the selected certificate.

4. Alternatively, to have Delivery Services generate a new self-signed certificate for the service, click **Create Self-Signed Certificate** and specify a name for the new certificate.

Delivery Services registers the new certificate with any other services that depend on the service that you modified. Previous certificates are retained on the IIS site. Self-signed certificates generated by Delivery Services should not be used for any other purpose.

Repairing and Removing the Authentication Service and Stores

Use the **Remove Service** task to delete the Authentication Service and stores. To remove the Authentication Service, first remove all the stores using the Authentication Service. 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 to deliver configurations for Citrix Receiver. When you remove a service that uses a self-signed certificate generated by Delivery Services, the certificate is retained on the IIS site.

Use the **Repair Service** task to remove and recreate fresh instances of the Authentication Service and stores. When you repair the Authentication Service or a store, Delivery Services saves the configuration, removes the old service, creates a new service, and reapplies the saved configuration. For stores with application synchronization enabled, the database is also deleted and recreated. When you repair a service that uses a self-signed certificate generated by Delivery Services, the repaired service is updated to use a new certificate generated by Delivery Services. The previous certificate is retained on the IIS site. In the case of services that use an SSL certificate, the repaired service is configured to use the same certificate.

Configuring Delivery Services Using the Configuration Files

This topic describes additional configuration tasks that involve editing the Delivery Services configuration files.

To configure application synchronization for earlier versions of XenApp and XenDesktop

If you use XenDesktop 3.0, XenApp 5.0, or XenApp for UNIX servers for user authentication and you enable application synchronization, manual configuration of Delivery Services is required to enable enumeration of user account security identifiers. To do this, you edit the Authentication Service configuration file.

1. Join the Delivery Services server to the domain that contains your XenDesktop or XenApp servers.

2. Using a text editor, open the Authentication Service web.config file, which is typically located in the c:\inetpub\wwwroot\Citrix\Authentication\ directory on the Delivery Services server.

3. Locate the following parameter in the file.

   ```
   requireAccountSIDs="FarmLookup"
   ```

4. Change the setting to LocalLookup.

   ```
   requireAccountSIDs="LocalLookup"
   ```

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

By default, contact between Delivery Services and the Citrix XML Service times out after 100 seconds and the service is considered failed after two unsuccessful attempts are made to communicate with it. You can change these default settings by editing the configuration file for the Authentication Service or store.

1. Using a text editor, open the web.config file for the Authentication Service or the store, which are typically located in the c:\inetpub\wwwroot\Citrix\Authentication\ and c:\inetpub\wwwroot\Citrix\Store\ directories, respectively, on the Delivery Services server.

2. Locate the following parameters in the file.

   ```
   serverCommunicationAttempts="2" timeout="100"
   ```

3. Update the settings as required, specifying the time-out value in seconds.

Securing Your Delivery Services Deployment

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

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

Use of certificates in Delivery Services. Server certificates are used for two different purposes in Delivery Services: token management and transport security.

The Authentication Service and stores each require certificates for token management. In the absence of a suitable certificate, Delivery Services generates a self-signed certificate when the Authentication Service or store is created. Self-signed certificates generated by Delivery Services should not be used for any other purpose. Although you can also use your existing self-signed certificates for token management in the Authentication Service and stores, in a production environment, Citrix recommends using Secure Sockets Layer (SSL) certificates from a trusted certificate authority.

To use HTTPS to protect communications, Delivery Services requires that the IIS instance hosting the Authentication Service and stores is configured for HTTPS and has an SSL certificate installed. In the absence of a suitable certificate and the appropriate IIS configuration, Delivery Services uses HTTP for communications.

Securing Delivery Services communications. In a production environment, Citrix recommends using the SSL Relay to secure data traffic between the Delivery Services server and your 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 HTTPS protocol to secure data passing between Delivery Services and your Citrix servers. HTTPS uses the SSL and Transport Layer Security (TLS) protocols to provide strong data encryption. Citrix recommends securing user connections to stores using HTTPS.

Password reset. You can enable users who cannot log on to a store because their passwords have expired to reset those passwords when they log on. 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 configure the Authentication Service.

Integrating Delivery Services into Your Environment

You can configure Delivery Services 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.

To manage user access to Citrix Online applications with XenApp

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

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

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

3. When you are prompted for a description of the application for users, include a description of the Citrix Online product that you want to publish. Append the string KEYWORDS:IsGoToMeeting | IsGoToWebinar | IsGoToTraining CitrixOnlinePromptMode=FreeTrial | None | Corporate at the end of the description.

   The FreeTrial option specifies that users without an account for the selected application will be prompted to visit the Citrix Web site and set up personal trial accounts. Use None if you want to prompt users to contact the system administrator to obtain an account for the selected application. Set the parameter to Corporate if accounts for all users are already in place for the selected application.

4. Ensure that you enable the appropriate Citrix Online product in the Delivery Services 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 Delivery Services

Delivery Services supports Windows event logging. Any events that are generated are written to the Delivery Services application log, which can be viewed using Event Viewer.

Delivery Services uses Microsoft .NET tracing to provide a tracing facility, which is disabled by default. You enable and configure tracing by editing the configuration file for the Authentication Service or store.

To enable tracing for Delivery Services

1. Using a text editor, open the web.config file for the Authentication Service or the store, which are typically located in the c:\inetpub\wwwroot\Citrix\Authentication\ and c:\inetpub\wwwroot\Citrix\Store\ directories, respectively, on the Delivery Services server.

2. Locate the <system.diagnostics> section in the file.

3. In the <switches> section, enable the tracing sources that you want to use by setting the value parameter to the required level of severity.

    - Set the parameter to Critical to trace only events that lead to serious, irrecoverable errors.

    - Set the parameter to Error to trace events that lead to any error.

    - Set the parameter to Warning to trace events that lead to errors or to unusual activity.

    - Set the parameter to Information to trace events that lead to errors, unusual activity, or changes in the system.

    - Set the parameter to Verbose to trace all events.

After enabling the required tracing, use a trace viewer capable of capturing Win32 output to see the Delivery Services traces.