Merchandising Server 1.1

Contents

Merchandising Server 1.1

Citrix Receiver for Windows, Receiver for Mac, and Merchandising Server are components of the Citrix Delivery Center solution. While Citrix Delivery Center provides the application delivery infrastructure to the IT administrator, Citrix Merchandising Server and Citrix Receiver for Windows work together to streamline the installation and management of application delivery to the user desktops. Merchandising Server provides the administrative interface for configuring, delivering, and upgrading plug-ins for your users' computers.

Under this node, you will find the following resources for the Merchandising Server:

New Features	Contains a listing of new features released in this version.
Readme for Merchandising Server 1.1	Contains known issues and issues fixed in this release.
Installation	Contains server requirements, system requirements and compatibility, scalability, and supported plug-ins and components. The procedure for installing Merchandising Server is also included.
Administration	Contains the following administrative tasks and information:
Overview	Contains an overview of the components with which the Merchandising Server interacts.
Configuring the Merchandising Server	Contains an overview task list of the actions involved in configuring the server. The tasks and procedures can be viewed by expanding each topic.
Creating Deliveries	Contains tasks and procedures involved in creating deliveries. This includes preparing updates, creating recipient rules, getting the delivery status, and deploying other Citrix product plug-ins.
Managing Plug-ins and Deliveries	Contains tasks and procedures for removing plug-ins from a Merchandising Server or user's computer, getting plug-in updates, redelivering, suspending, and restoring deliveries.
Maintaining the Merchandising Server	Contains tasks and procedures for upgrading the Merchandising Server software, changing server settings, ensuring high availability and fault tolerance, backing up the Merchandising Server, and starting and stopping it.
Auditing Administrative Actions	Contains tasks and procedures for auditing the actions an administrator performs in the Administrator Console.
Troubleshooting	Contains tasks and procedures for troubleshooting the Merchandising Server through viewing different log files.

Metadata Reference	Contains the schema and descriptions of the metadata files used to define the properties for each of the applications present in the installer file. A sample file is included.

New Features in this Release

Features	Description
Targeted deliveries	Enables you to create rules-based deliveries (for contexts such as machine name, IP range, domain membership, operating system identity) to deliver IT Services to individually managed and unmanaged computers
Windows 7	Receiver and many of its components now fully support Windows 7
Reconfiguration	Plug-ins can now be reconfigured from the Merchandising Server
Reporting and auditing	Delivery reporting and a fulll audit trail has been added
Easier user experience	We have simplified the end user download and install experience
Smaller footprint	Only 1 processor and 1 GB of RAM needed for testing and small deployments
Proxy server support	You can now enter settings to allow the Merchandising Server to use a proxy server
Expanded certificate support	You can now use your own certificates, including wildcard and chain certificates, with the Merchandising Server

Readme for Citrix Merchandising Server 1.1

Version: Release 1.1

Download File Name: citrix-merchandising-server-1.1.0-1063.xva

Contents

Finding Documentation

To access complete and up-to-date product information, go to Citrix eDocs located at http://support.citrix.com/proddocs/index.jsp and expand **Receiver and Plug-ins** > **Merchandising Server**.

To access HTML-based help for the Merchandising Server, click the **Help** link at the top of every Administrator Console page.

To open Receiver for Windows help, right-click the Receiver icon in the notification tray and select **Help**.

Getting Support

Citrix provides an online user forum for technical support. This forum can be accessed at http://forums.citrix.com/category.jspa?categoryID=169 The Web site includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

Citrix provides technical support primarily through Citrix Solutions Advisor. Contact your supplier for first-line support or use Citrix Online Technical Support to find the nearest Citrix Solutions Advisor.

Citrix offers online technical support services on the Citrix Support Web site. The Support page includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

Upgrading the Merchandising Server and Plug-ins

To upgrade the Merchandising Server, Receiver for Windows, and plug-ins, follow these general guidelines:

- **Merchandising Server:** To upgrade the Merchandising Server, download the upgrade file and use the **Configuration** > **Upgrade Server** page in the Administrator Console. Upgrade steps are included in this topic.

- **Receiver for Windows:** The upgraded Merchandising Server automatically handles the Receiver for Windows upgrade. The first time that Receiver for Windows synchronizes with an upgraded Merchandising Server, Receiver either prompts the user to upgrade or upgrades automatically, depending on a user's upgrade settings. When you upgrade the Merchandising Server, the upgraded Receiver for Windows client is automatically added to the download page.

- **Plug-ins:** To upgrade plug-ins or to add new plug-ins to Merchandising Server, download the plug-in and metadata files to the Merchandising Server from the **Plug-ins** > **Get New** page, then create and schedule a delivery. You can also use that page to obtain plug-ins that run in standalone mode. Although the 1.0 version plug-ins are compatible with Merchandising Server 1.1, it is recommended that you upgrade to benefit from new functionality.

To upgrade your installation of Merchandising Server 1.1:

1. Download the Merchandising Server 1.1 RPM file. Upgrade files are available at Citrix.com.

2. In the Administrator Console, select **Configuration** > **Upgrade Server**.

3. Click **Browse** to locate the downloaded file and then click **Upgrade**.

4. Click **Yes** in the confirmation popup to start the software upload.

5. When the progress bar closes, wait a few minutes for the installation to complete before you refresh the page and log on.

After you upgrade the Merchandising Server, perform the following tasks.

- Required: Review the information about new SSL certificate functionality in this release and then consult your security department about certificate requirements. For more information, search for the topic “Installing SSL Certificates” in eDocs.

- Recommended: Use the XenCenter console to set the Appliance Terminal password.

Known Issues

Cannot update Xen Tools from the Merchandising Server [1356]

You currently cannot update the Xen Tools from the Merchandising Server.

"#" ignored in group sorting [1762]

On the **Rule Create/Edit** page, a "#" in a group name is ignored when groups are sorted. To locate a group name that includes a "#", look for the characters following the symbol.

Evaluation order numbers are incorrect after creation of a 1.0 to 1.1 upgrade delivery [1863]

On the Deliveries page, the delivery for the 1.0 release is labeled "PRODUCTION" and it has an evaluation order of 2. After you create and schedule your first delivery after the 1.1 upgrade, the delivery list shows the new delivery with an evaluation order of 2 and the "PRODUCTION" delivery has an evaluation order of 3. Be sure to change the evaluation order as needed for your deliveries.

Spaces in some search strings result in a row of ellipses [1870]

In some of the Reporting and Logging pages, a search string that includes a space results in a row containing only an ellipsis in each cell. Unless otherwise indicated, this issue applies to search strings with a space in any position: Leading (" name"), trailing ("name "), space only (" "), between names ("name1 name2").

- From the **Delivery Reporting** page, searches by delivery name, user name, or machine name.
- From the **Enable / Disable Logging** page, searches by user name if the space is between names. (Leading and trailing spaces, as well as searches by a space only, are handled correctly.)
- From the **View Log Files** page, searches by user name if the space is between names. (Leading and trailing spaces, as well as searches by a space only, are handled correctly.)

Cannot search by domain on some pages [1871]

On the **Reporting and Logging** > **Enable/Disable Logging** page and the **Reporting and Logging** > **Delivery Reporting** page, a search string containing a full or partial domain name results in an empty table. A search string that is left empty returns results for one domain.

Some events are omitted from the audit log [1892]

The audit log generated from the **Reporting and Logging** > **View Audit Trail** page does not contain the following events:

- Active Directory synchronizations
- Administrator Console user logins
- Citrix Update Service update checks

- Enable/disable user logging and system logging changes
- Trigger Client Log Collection button clicks

HTML code appears on Receiver Plug-in status page when server restart is needed [1908]

The Receiver **Preferences** > **Advanced** > **Plug-in status** page will contain HTML code if Receiver is unable to check for updates. To re-enable updates, restart the Merchandising Server.

Issue with creating a delivery rule for domains [1944]

If you define a delivery rule that includes the "Is Not" operator with Machine Domain Membership, the resulting delivery might not work. Until this issue is resolved, use the "Is" operator for rules based on Machine Domain Membership.

Also, the "Creating Delivery Recipient Rules" topic available from the Administrator Console Help and from eDocs should include the following information:

Rules can be defined by User Name, User Group, User Domain, Machine Domain Membership, Machine Name, IP Address or Range, or Operating System.

Spaces not permitted in delivery rules based on IP address range [1956]

When defining a delivery rule based on an IP address range, do not include spaces in the range. For example, an error occurs if the IP address range string is "10.10.10.10 - 10.20.10.10" but not if the string is "10.10.10.10-10.20.10.10".

Upload of certificate file sometimes fails [1961]

After an initial installation (not an upgrade) of the Merchandising Server, the upload of a certificate file will occasionally fail and result in an error message about an invalid SSL certificate. If this occurs, wait a few minutes and try again.

Spaces not permitted in delivery rules containing a comma-separated list [1981]

When defining a delivery rule containing a comma-separated list of user domains, machine domain membership, or machine names, do not include spaces in the list. For example, an error occurs if the list is "name1, name2" but not if the list is "name1,name2".

Issues Fixed in this Release

The following issues were fixed since the last release.

- Merchandising Server does not support plug-in installer file name changes [1031]
- User searches with non-English characters do not return correct results with Internet Explorer 7 [1362]
- Suspended Default deliveries do not get delivered after being resumed [1526]

- Cannot save edits to rule based on user or group name if more than one rule exists on Internet Explorer 7 [1529]
- Unable to change a delivery that is scheduled for delivery in the future to "deliver now" [1594]
- OS Rules will not work in a delivery [1612]

http://www.citrix.com

Administrator's Quick Start

This quick start is intended to provide tips to returning users. For complete instructions, refer to the appropriate topics under Receiver and Plug-ins > Merchandising Server > Administration.

Installing Merchandising Server Software

The Merchandising Server software is delivered as a virtual appliance image that contains all of the software necessary for running the Merchandising Server.

Getting the Merchandising Server Software

1. The Merchandising Server virtual appliance (.xva) image is available for download from the Citrix support site. The image name is similar to: citrix-merchandising-server-[*releaseNumber*].bz2.

   Where *releaseNumber* is a numeric value representing the release version

2. Unpack the zip file using bz2, winzip, or other archive utility.

Importing the VM into XenCenter

Verify that you have a minimum of 8 GB of available hard disk space before proceeding.

1. Start Citrix XenCenter.
2. Select **File > Import VM**.
3. Click **Browse**, navigate to the .xva file, and click **Open**.
4. Select **Exported VM** as the Import Type and then click **Next**.
5. In the **Home** server screen of the wizard, select the XenServer instance where this VM should be imported and then click **Next**.
6. In the **Storage** screen, select the XenServer where the storage repository resides and then click **Import**.

   The import begins and the Network screen opens.

7. In the **Network** screen, select the appropriate network designation. If you only have one network, select **Network 0** and click **Next**.
8. In the **Finish** screen, clear the checkbox for **Start VM after Import** and then click **Finish**.
9. After the import process completes, right-click the VM and choose **Properties**.
10. Click the **Memory and VCPUs** tab, choose the amount of memory for the VM, and choose the number of VCPUs. We recommend allocating at least 4GB of memory and configuring 2 VCPUs.
11. Click **OK**.
12. Select the VM and click the **Network** tab.
13. Click the **Properties** button, select **Auto-generate**, and click **OK**.
14. Right-click the VM and choose **Start**.
15. Open the **Console** tab, configure network settings, enter a root password, and then save the settings.

Configuring Your Administrator Users

1. Open a browser window and enter the Administrator Console URL. The URL is similar to https://[*server_address*]/appliance, where *server_address* is your Merchandising Server host name or IP address.
2. Enter `root` for username, `C1trix321` for the password, and click **Log on**.
3. Select **Configuration > Configure AD**.
    a. Provide the Active Directory server information.
    b. Click **Save Changes and Sync** to load your users into the Merchandising Server database.
4. Select **Configuration > Permissions**.
    a. Enter your first or last name in the Search text box and click **Search**.
    b. Select your name in the search results list and click **Edit**.
    c. Select **Administrator** permissions and click **Save**.
    d. Repeat the process for each of the users who will need Administrator and Auditor permissions.
5. Log out of the Administrator Console.

Configuring the Administrator Console

1. Log in to the Administrator Console with the administrator user administration credentials you just configured (above).
2. Optionally, select **Configuration > SSL Certificate Management**.
    a. Select **Export certificate signing request** to produce the request.
    b. Enter your company information and click **Export** and send this to your preferred signing authority.
    c. Upon receipt of the certificate from your system administrator, select **Import certificate from certificate authority** from the dropdown list.
    d. Click **Browse** to locate the certificate.cer file and click **Submit**.
3. Select **Configuration** > **Options**.
    a. Enter support information for your users.
    b. Enter your Active Directory domain name.
    c. Enter the polling frequency to the Citrix Update Service.
    d. Enter the user authentication token expiration date.
4. Optionally, select **Configuration** > **Network Settings**.

    If you are using a proxy server, enter the configuration and authentication settings here.

Preparing Your System

Before creating a delivery, download your plug-ins and create delivery rules.

To download plug-ins

1. In the Administrator Console, select **Plug-ins** > **Get New**.
2. Select the plug-in from the list and click **Download to Server** or click **Download All to Server**.
3. Click **Close** in the Success pop-up.
4. Continue this process until you have downloaded all the plug-ins you want to deliver.

To create recipient rules

1. In the Administrator Console, select **Deliveries** > **Rules**.

2. Click **Create** at the bottom of the page.

3. Enter the rule name and description.

4. Select the rule type from the menu in the Type field. Possible values are Machine Name, User Domain Membership, Machine Domain Membership, Operating System, IP Address Range, LDAP User, and LDAP Group.

    - If you select LDAP User or Groups for the type, the screen shows the Search functionality.

    - If you select User Domain membership, Machine Domain Membership, Operating System, or IP Address Range for the type, select Is or Is Not for the Operator field and enter the appropriate value.

    - If you select Machine Name for the type, select either Begins With, Is Exactly, or Contains and enter the appropriate value.
5. Click **Save** to save your rule.

Creating Deliveries

To create a delivery

1. In the Administrator Console, select **Deliveries** > **Deliveries**.

2. Click **Create** at the bottom of the page.

3. In the **General** tab, enter the general information for the delivery.

4. In the **Plug-ins** tab, click **Add** and select the checkboxes for the plug-ins to deliver; click **Add** again.

5. Click the **Config** tab and enter the plug-in specific values.

6. Click the **Rules** tab.

    a. With **Basic** link enabled, select the operator type (ADD or OR) and click **Add**.

    b. Select the checkbox for the rules to add and click **Add**. The selected items are added to the delivery.
7. Click the **Schedule** tab.

    - Define the delivery schedule time and date or click **Now**.

    - Click **Schedule** to complete the process.

Your system is now ready for your users to download Citrix Receiver at your internal site address. Once they have download the Receiver, it will automatically fetch your scheduled delivery and install the plug-ins.

Installation

The Merchandising Server software is packaged as a virtual appliance image. The virtual appliance image when imported onto XenServer, creates a fully functional virtual server.

System Requirements

Before you install the Merchandising Server virtual image, verify that the following requirements are met:

Contents

Server Requirements

- XenServer 5.x — The instructions in this section describe the installation process using XenCenter on a XenServer 5.x server. To download a free version of XenServer Express, go to http://www.citrix.com and select **Products & Solutions > Products > XenServer**.
- Active Directory — Your corporate directory must be accessible through Active Directory.

System Requirements and Compatibility

- Citrix XenServer™ 5.x with 8 GB of available disk space and 1 GB available RAM.

  You can download the XenServer free of cost from http://www.citrix.com.

One of the following browser versions is required to use the Citrix Merchandising Server Administrator Console:

- Internet Explorer version 7.x.
- Firefox version 2.x and later

Scalability

The Merchandising Server capacity depends on the amount of RAM and number of CPUs configured for the virtual appliance. The frequency of plug-in updates is the primary driver of the Merchandising Server performance and bandwidth requirements. Based on simulated user traffic load, concurrent users requests, the number of plug-in installations in the busy hour, and recommended maximum number of Receivers are shown below for three sample configurations. Contact Citrix if you require a higher capacity.

Merchandising Server Configuration	Maximum Simultaneous Concurrent User Requests*	Maximum Number of Plug-ins Delivered Per Hour	Recommended Maximum Number of Receiver Users	Maximum Busy Hour Bandwidth Consumption (Mbps)
4 GB/2 CPU	600	30000	15000	125
2 GB/1 CPU	100	20000	10000	83
1 GB/1 CPU	8	6500	500	27

*****Based on a test where each request involved downloading four plug-ins.

Supported Citrix Plug-ins

The following table lists the plug-ins that are compatible with Merchandising Server Release 1.1, as well as the operating systems supported by those plug-ins:

Plug-in	Compatible Operating Systems
Acceleration plug-in 5.5.0.128	Windows XP Professional, Vista (32-bit)
EasyCall 2.2.1.872	Windows XP Professional, Vista, Windows Server 2000 and 2003
EasyCall 3.0.0.0950	Windows 7, XP Professional, Vista, Windows Server 2003 and 2008 (32- and 64-bit)
Online plug-in 11.2.0.31560	Windows 7, XP Professional, Vista, Windows Server 2003 and 2008 (32- and 64-bit)
Offline plug-in 5.2.0.1227	Windows 7, XP Professional, Vista, Windows Server 2003 and 2008 (32- and 64-bit)
Profile Management plug-in 2.0.1.48	Windows XP Professional, Vista, Windows Server 2003 and 2008 (32- and 64-bit)
Secure access plug-in 4.6.1.27	Windows 7 and Vista (32- and 64-bit), XP Professional (32-bit)
Secure access plug-in 9.1.96.4	Windows XP Professional, Vista (32-bit)

Service monitoring plug-in 5.2.3012.0	Windows 7, XP Professional, Vista (32- and 64-bit)

Documentation for the Citrix components supported by Citrix Merchandising Server is available at http://support.citrix.com/proddocs/index.jsp and through the **Plug-ins** > **Get New** page in the Merchandising Server Administrator Console.

Importing the Virtual Appliance

You install the Merchandising Server virtual appliance using Citrix XenCenter for XenServer 5.0 (Express, Standard, Enterprise, or Platinum Edition). For information on upgrading the Merchandising Server software, see Upgrading the Merchandising Server.

1. The Merchandising Server virtual appliance (.xva) image is available for download from the Citrix download site. The image name is similar to citrix-merchandising-server-[*releaseNumber*].bz2. Where [*releaseNumber*] is a numerical value representing the release.

2. Unpack the zip file using Bz2 or another archive utility.

3. Start Citrix XenCenter.

   Important: Verify that you have a minimum of 20 gigabytes of available hard disk space before proceeding.

4. In XenCenter, choose **File > Import VM**.

5. Click **Browse**, navigate to the .xva file, and click **Open**.

6. Select **Exported VM** as the **Import Type** and then click **Next**.

7. In the Home server screen of the wizard, select the XenServer instance where this VM should be imported and then click **Next**.

8. In the Storage screen, select the XenServer where the storage repository resides and then click **Import**. The import begins and the Network screen opens.

9. In the Network screen, select the appropriate network designation. If you only have one network, select **Network 0**.

10. Click **Next**.

11. In the Finish screen, clear the checkbox for **Start VM after Import** and then click **Finish**.

    The import progress is displayed in the status bar at the bottom of the XenCenter window and also on the Logs tab. The import process may take some time, depending on the size of the VM and the speed and bandwidth of the network connection between XenCenter and the server where you are installing the new VM. Under optimum conditions this could take as little as 5 minutes.

    After the import process completes, you can specify the amount of memory to be allocated to this VM before starting the VM.

12. Right-click the VM in the XenCenter window and choose **Properties** to allocate memory and number of VCPUs for the VM.

    a. Click the **Memory** tab and **VCPUs** tab and choose the amount of memory for the VM.

Note: We recommend that you allocate at least 4Gb of memory.

b. Click the **VCPUs** tab and choose the number of VCPUs.

Note: We recommend that you allocate at least 2 VCPUs.

13. Configure the VM for an auto-generated MAC address. (The VM does not function properly without a unique MAC address.)

    a. In the XenCenter window, select the VM and click the **Network** tab.

    b. Click the **Properties** button and select **Auto-generate**.

    c. Click **OK**.
14. In the XenCenter window, right-click the VM and select **Start**. The VM starts and the **Network Configuration Utility** opens.

15. Enter the numerical values as directed on the screen to establish the IP address, netmask, default gateway, and a DNS server for this server.

    Note: The Merchandising Server does not support DHCP.

    Note: An asterisk is displayed by each setting that you have changed but not saved.

16. Enter 9 to save your settings as directed on the screen.

    Note: There is one more option available in this utility that is not displayed on the screen. Entering an uppercase 'R' resets all the values, including the root password, to the factory defaults. Use caution when using this feature.

You have completed the installation and configuration of the virtual machine.

Want More Information?

- Changing Server Network Setting
- Configuring the Administrator Console

Administration

The Merchandising Server is administered through the Administrator Console.

Overview

Merchandising Server is the head-end infrastructure component – used in conjunction with Receiver – that allows you to create, deliver and manage a high quality end user experience on laptops, desktops, and smart phones.

With Merchandising Server, you can easily “merchandise” your IT services in a convenient, simple way that seamlessly connects users to virtual applications, desktops, and other services – in the same way retail merchandising managers create a compelling shopping experience for their customers.

About Merchandising Server

Easily “Merchandise” Virtual Apps and Desktops

With centralized management, the Merchandising Server allows you to “merchandise” virtual applications and desktops across the entire organization. The Merchandising Server sits in front of the XenApp and XenDesktop infrastructure and facilitates not only the delivery of virtual apps and desktops but more importantly also allows you to provide a simple and intuitive end user experience.

Simplifies Setup and Distribution

The Merchandising Server provides easy management, setup, and distribution to your end users of the Citrix Receiver, plug-in software, and updates. For users, Receiver’s one-time setup is simple, fast, and easy. Users simply point any browser to the setup site included with Merchandising Server. Two clicks and the setup process starts. From a fresh PC or laptop to fully provisioned with the broad range of IT services – from applications to virtual desktops - anywhere in the world in less than 15 minutes (depending upon network connection).

Citrix Merchandising Server comes packaged as a virtual appliance that:

- Manages the setup of Citrix Receiver
- Enables “plug-ins” to support multiple types of delivery services
- Centralizes management of all updates
- Enables access to web-based user support services
- Offers robust management reporting features

Receiver supports 32-/64-bit of Windows XP, Vista, Server 2003, and Server 2008.

It is strongly recommended that Citrix Receiver for Windows be used with the Citrix Merchandising Server. For specialized applications, Receiver for Windows may be installed with compatible plug-ins independent of the Merchandising Server.

Once installed, the Receiver fetches the delivery information from the Merchandising Srever and installs the plug-ins.

After installation is complete, the Receiver starts its plug-ins in the correct order ensuring that connectivity services are available for plug-ins that require it.

Use the Merchandising Server and Receiver for Windows in combination to simplify desktop and application delivery. The Receiver infrastructure provides:

Seamless installation

Your users install Receiver for Windows on their devices. If a download is interrupted, the Receiver silently resumes the action when the connection is restored. When installation is complete, the Receiver immediately installs the scheduled plug-ins without requiring the user to enter any information. The Receiver can even be installed from outside of the company firewall. Upgrades are pushed down and run automatically.

Managed connections to delivery services

The Receiver uses the Citrix secure access plug-in to supply secure connectivity, enabling users access to business-related applications from anywhere.

Simplified administration

Use the Merchandising Server to deliver plug-ins in one action. The Merchandising Server retrieves plug-in updates from the Citrix Update Service and presents the update list to you through the Administrator Console.

Simplified installation and upgrade

Import the Merchandising Server virtual appliance through Citrix XenServer. Upgrades to the Merchandising Server are imported directly through the Administrator Console.

Administrator Console

Use the Administrator Console to configure and update the Merchandising Server, synchronize with Active Directory, and create and manage plug-in deliveries.

Use the console to configure and manage the following components:

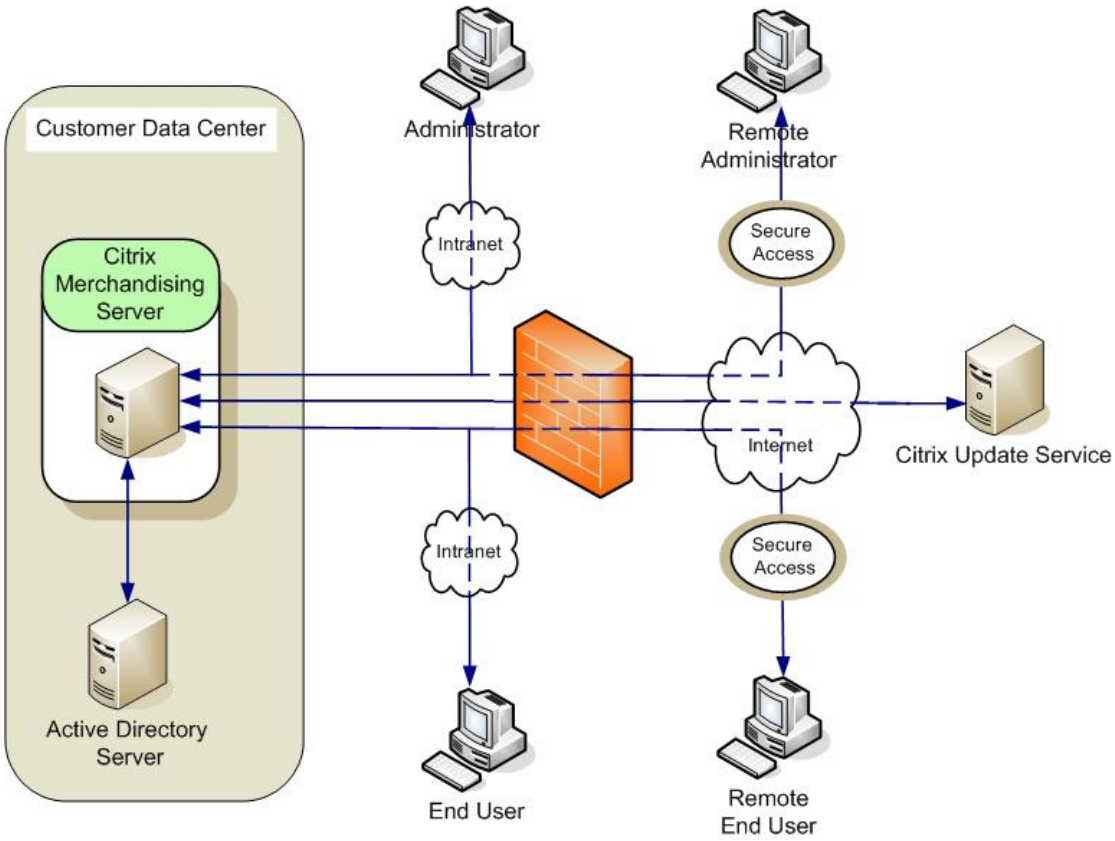
- Plug-ins — Prepare and process plug-ins for creating a delivery. See Preparing Updates.
- Deliveries — Create and maintain deliveries and recipient rules. See Scheduling Deliveries.
    - Rules — Create rules to define the recipients list for the delivery. The recipients can be defined by machine name, IP address, and domain names.
    - Deliveries — Deliveries contain plug-ins, configurations, rules, and a schedule.
- Reporting and Logging — Check the status of your deliveries. See Getting Delivery Status and Triggering Client Log Collection.
- Configure the following features:
    - Grant user permissions — Granting Administrator and Auditor Permissions.
    - Configure and Sync Active Directory — Connecting to Active Directory.
    - Install SSL Certificates — Installing SSL Certificates.
    - Update Service Polling Frequency — Citrix Update Service.
    - Token Expiration Frequency — User Authentication.
    - Default domain name — Configuring Default Domain Name.
    - HTTPs redirection — Disabling HTTPS Redirection.
    - Support Contact Information — Configuring Support Contact Information.
    - Proxy Server — Configuring the Proxy Server
    - Upgrade Merchandising Server — Upgrading the Merchandising Server Software.

Components

The Citrix Receiver end-to-end infrastructure consists of four components:

- Citrix Merchandising Server
- Citrix Receiver Client
- Citrix Update Service
- Software Development Kit

Citrix Merchandising Server



The Merchandising Server resides in your data center and requires the connectivity shown in the following diagram. The Merchandising Server is managed using the administrator console and is delivered as a virtual appliance ready to import into your XenServer environment.

Configure the Merchandising Server to connect to:

- Microsoft Active Directory server

  The Merchandising Server acquires user and group information from your Active Directory.

  The Merchandising Server uses the imported user and group information to:

  - Display the list of users you can grant Administrator and Auditor permissions — See Granting Administrator and Auditor Permissions.
  - Display the list of user and group names that you use to create the distribution list for plug-in deliveries — See Creating Deliveries.
- Receiver for Windows

The Receiver for Windows software, installed on end user devices, connects to the Merchandising Server through HTTPS.

The Merchandising Server uses Secure Sockets Layer (SSL) on port 443 to communicate with the Receiver.

- Citrix Update Service

  Citrix posts new and updated plug-ins to the Citrix Update Service. For more information, see Preparing Updates.

Administrator Console

Use the Administrator Console to configure and update the Merchandising Server, synchronize with Active Directory, and create and manage plug-in deliveries.

Use the console to configure and manage the following components:

- Plug-ins — Prepare and process plug-ins for creating a delivery. See Preparing Updates.
- Deliveries — Create and maintain deliveries and recipient rules. See Scheduling Deliveries.
    - Rules — Create rules to define the recipients list for the delivery. The recipients can be defined by machine name, IP address, and domain names.
    - Deliveries — Deliveries contain plug-ins, configurations, rules, and a schedule.
- Reporting and Logging — Check the status of your deliveries. See Getting Delivery Status and Triggering Client Log Collection.
- Configure the following features:
    - Grant user permissions — Granting Administrator and Auditor Permissions.
    - Configure and Sync Active Directory — Connecting to Active Directory.
    - Install SSL Certificates — Installing SSL Certificates.
    - Update Service Polling Frequency — Citrix Update Service.
    - Token Expiration Frequency — User Authentication.
    - Default domain name — Configuring Default Domain Name.
    - HTTPs redirection — Disabling HTTPS Redirection.
    - Support Contact Information — Configuring Support Contact Information.
    - Proxy Server — Configuring the Proxy Server
    - Upgrade Merchandising Server — Upgrading the Merchandising Server Software.

Receiver Client

The Receiver installation can be pushed using your standard ESD process, or installed by your users through the Citrix Receiver Download page deployed either inside or outside of your company's firewall.

Once installed, Receiver downloads, updates, and starts its managed plug-ins without user interaction.

For more information about Receiver, see Receiver Overview.

Citrix Update Service

The Citrix Update Service web site contains all the latest updates to the Citrix plug-ins.

Software Development Kit

Citrix Receiver has an extensive set of APIs which provide the functionality required to integrate applications with the Citrix Receiver. For a complete list of the APIs, their descriptions, and other useful information such as integration tips and the metadata required to install your applications, contact receiversdk@citrix.com.

Security

Security is ensured through:

- User Authentication
- Secure Data Transfer

User Authentication

To ensure that only registered users can access the Merchandising Server for updates, users are authenticated each time they access the Merchandising Server.

When users install the Receiver, they are prompted to log on to the Merchandising Server. The Merchandising Server verifies the credentials against Active Directory accounts. If the user is authenticated, the Merchandising Server creates a client token for future user authentication. The token is downloaded and installed on the client device. When the Receiver subsequently communicates with the Merchandising Server, it uses the token for authentication.

Configure token expiry in the administrator console.

Data Transfer

All data transfers are handled using HTTPS protocol to ensure secure data transfer.

Configuring the Merchandising Server

Use the administrator console to configure the Merchandising Server.

To configure the Merchandising Server, you must:

1. Log on to the Administrator Console with root permissions.
2. Synchronize the Merchandising Server with Active Directory.
3. Grant your user name Administrator permissions.
4. Log off the Administrator Console and log back on with your user name.
5. Optionally, install SSL certificates.
6. Configure server options.
7. Optionally, configure proxy server.

When you have completed these configurations, you are ready to create deliveries.

This section contains the following topics.

Configuring your Administrator Account

To set up your administrator account you need to:

- Log on to the Administrator Console with root — Logging on as Root.
- Configure your corporate Active Directory — Connecting to Active Directory.
- Grant Administrator administrator permission to your Active Directory user account — Granting Administrator and Auditor Permissions.

Logging on as Root

Log on using the root user credentials. Once you are successfully logged on you can grant administrator permissions to user accounts, including your own.

To log on to the Administrator Console with root username

1. In a web browser, enter the URL for the Administrator Console. It is similar to https://[*serverAddress*]/appliance. Where the *serverAddress* is either the IP address or the host name of the Merchandising Server.

2. Enter the 'root' user name and password and then click **Log on**. The root user log on credentials are:

   - User name: root
   - Password: C1trix321

   Note: User login credentials are case-sensitive.

   The Administrator Console opens to the Set Up page.

The **Configurations** > **Permissions**, **Configure AD**, and **Change Root Password** nodes are displayed with root logon to the Administrator Console.

Next Steps?

- Resetting the Root Password
- Connecting to your Active Directory Server
- Granting Administrator and Auditor Permissions

Resetting Root Password

We recommend that you reset the root user password immediately.

1. In the Administrator Console, click **Change Root Password**.
2. Enter the current password in the **Old Password** field and enter the new password in both the **New Password** and **Confirm Password** fields. The new password must be at least 8 characters, include both alphabetic and numeric characters, and contain at least one upper case character.
3. Click **Change Password**.

Want More Information?

- Connecting to Active Directory
- Granting Administrator and Auditor Permissions

Connecting to Active Directory

The Merchandising Server connects to your Active Directory (AD) server to retrieve user and group information. In the Administrator Console, you use this information to assign user permissions, and define the recipients list for your deliveries.

By default, the Merchandising Server imports information from the configured directory source daily. You can change the frequency as described below. You can also force a synchronization to occur immediately. When you first configure the system, you must force a synchronization to complete the configuration tasks by using the **Save Changes and Sync** button.

If you change the AD server configuration, the Merchandising Server automatically deletes, updates, and adds the user information from the new server.

1. Log on to the Administrator Console with root credentials and select **Configure AD**.

2. Enter the settings as described in the following table:

Setting	Description
Source Name	A descriptive name for the directory source.
Server Address Server Port	The IP address or host name for the AD server to be used to import directory information. The AD Server Port for some AD directories is typically 389. If you are using an indexed database, changing the AD Server Port to 3268 significantly speeds up AD queries. If your directory is not indexed, we recommend that you use an administrative connection, rather than an anonymous connection, from the Merchandising Server to the database. Download performance improves when you use an administrative connection.
Bind DN Bind Password	The Administrator Bind DN and password for queries to your AD directory. Example syntax for Bind DN: "Administrator@adServer.com"
Base DN	The Base DN used as a starting point for directory searches. Example syntax for Base DN: "cn=Users,dc=ace,dc=com")

3. Enter the frequency for your AD synchronization. Available options are **Daily**, **Weekly**, **Monthly**, or **Quarterly**.

4. Click **Save Changes and Sync** to have the directory synchronized with the Merchandising Server immediately. The Administrator Console informs you when the synchronization is complete in the status bar.

Next Steps?

- Granting Administrator and Auditor Permissions
- Logging on as the Administrator

Granting Administrator and Auditor Permissions

You must first grant administrator permissions to your Active Directory user account before you can complete the Administrator Console configuration tasks. Only users logged in with administrators permissions or logged in as root can grant administrative permissions.

There are three levels of permissions in the Administrator Console as shown in the following table:

Permission	Access	Grantee
Administrator	All Admin Console functionality except the Audit Trail Reports	Other Administrators and root
Auditor	Audit Trail Reports and Permissions	Other Auditors and root
root	Permissions and Active Directory Synchronization.	N/A

To grant Administrator permissions to your user account

1. Log on to the Administrator Console with root credentials and select **Configurations > Permissions**. When you first access this page, the user list is blank, you must locate your user name and give yourself (and others) Administrator or Auditor permissions before this page contains data.

2. Enter the first few characters of your user's first or last name in the search text field and click **Search**. The list of all user names that match your search string is displayed.

3. Select the checkbox for your user name and click **Edit**.

4. Select the appropriate permission level in the **Edit User Permissions** popup and click **Save**. You can set the permissions to give all of your administrator access to the Administrator Console now or come back and do this later. You have completed the process for setting up your user account. Repeat the process to give Auditor permission to at least one user. If you do not do this now, you will have to log on to the Administrator Console with root credentials again to grant Auditor permissions. After you have finished this, log out of the root user session.

5. Close the search popup by clicking the top-right corner.

6. Click **Log off** in the top-right of the Administrator Console to log out. The remaining configuration tasks are completed when you log back in with your administrator user account.

Next Steps?

- Installing SSL Certificates
- Configuring Server Options
- Configuring the Proxy Server

Logging on as Administrator

Once you have configured the permissions for your administrator account, you can log on to the Administrator Console with your administrator account credentials to complete the configuration items:

- Installing SSL Certificates
- Configuring Server Options
- Configuring the Proxy Server

To log on as an administrator

1. In a web browser, enter the URL for the Administrator Console. It is similar to https://[*serverAddress*]/appliance.
   - Where *serverAddress* is the Merchandising Server IP address or the host name.
2. Enter the your user name and password and then click **Log on**. Your user name is the Active Directory user account with domain name that you configured in Granting Administrator and Auditor Permissions.
   - User name: Enter the user name in the form of domain\username.
   - Password: Your Active Directory user name password.

   Note: The credentials are case sensitive.

   The Administrator Console opens.

You can now complete the configuration process.

Next Steps?

- Configuring Server Options
- Installing SSL Certificates
- Configuring the Proxy Server

Configuring Server Options

The **Configurations > Options** page in the Administrator Console contains the following Merchandising Server and Receiver for Windows configuration parameters:

- Support Contact information — The support contact information presented to the user through the Receiver Preference panel, see Configuring Support Contact Information.
- Default Domain Name — The default domain name for user credentials, see Configuring Default Domain Name for more information.
- HTTP Redirection — Enable or disable automatically redirected to HTTPS, see Disabling HTTPS Redirection for more information.
- Citrix Update Service Polling Frequency — The frequency for poling the Update Service for plug-in updates, see Defining Update Service Polling Frequency.
- Token Expiration Frequency — The expiration interval for the unique token used to authenticate users, see Defining Token Expiration Frequency.

Configuring Support Contact Information

The **Configurations > Options** page contains the features for configuring the support contact information that populates the Preference panel **Help and Support** tab in the Receiver. You can define the support email address, web site, phone number, and if you have GoToAssist, you can define the server location for your users.

To define support contact information

1. Log on to the Administrator Console as administrator and select **Configurations > Options**. The first four fields are used to populate the Receiver Preference panel **Help and Support** page.

2. Enter the support contact information as shown in the following table.

Field	Description
Support email address	The email address for your end users to contact support. The value in this field must be in a valid email address form such as support@acme.com.
Support website	If you have a support web site for your end users to access, enter the http or https address here. The value should be in the form of http(s)://support.acme.com.
Support phone number	The value for this field is not validated, you can enter an extension or include international dialing numbers.
GoToAssist server	This is the fully qualified address for you GoToAssist server in the form of http(s)://www.gotoassist.acme.com.

   Field names for which you have not entered values in the **Options** page are not displayed in the Receiver.

3. Click **Save Changes**.

Want More Information?

- Defining Token Expiration Frequency
- Disabling HTTPS Redirection
- Configuring the Proxy Server

Configuring Default Domain Name

You can make the user experience a little easier by including your Active Directory domain name in the **Default Domain** field on the **Configurations > Options** page. If you configure this option, when your users log on the Merchandising Server or the Administrator Console, they only need to enter their Active Directory user name.

To define the default domain name

1. Log on to the Administrator Console as administrator and select **Configurations > Options**.
2. Enter your Active Directory server domain name in the **Default Domain** field.
3. Click **Save Changes**.

Want More Information?

- Defining Token Expiration Frequency
- Defining the Citrix Update Service Polling Frequency
- Disabling HTTPS Redirection
- Configuring the Proxy Server

Disabling HTTPS Redirection

By default, any attempt to access the Merchandising Server through http protocol is automatically redirected to https. If you are deploying several Merchandising Servers behind one address and deploying a commercial SSL certificate, you may want to disable this feature. The disable feature is designed for a system deployment that includes multiple server machines in different geographical areas. As each Merchandising Server uses a different SSL private key, it's not possible to purchase a single commercial SSL certificate that can be installed on all those machines. Instead, you can use NetScaler in 'Transparent SSL' or 'SSL Offload' mode.

In this configuration, Receiver for Windows appears to communicate in SSL to the https address of the Merchandising Server, but this is actually the NetScaler box. The Netscaler sends geo-load balance commands using HTTP protocol to the appropriate server.

1. Log on to the Administrator Console as administrator and select **Configurations > Options**.
2. For the **Https Redirection** field, click **Disabled** to stop the automatic redirection.
3. Click **Save Changes**.

The Merchandising Server restarts to reset this property. You can log back on to the Administrator Console in a few minutes.

Want More Information?

- Defining Token Expiration Frequency
- Defining the Citrix Update Service Polling Frequency
- Configuring Default Domain Name
- Configuring the Proxy Server

Defining Update Service Polling Frequency

The Polling Frequency settings in **Configurations > Options** allows you to specify how often the Merchandising Server requests update information from the Citrix Update Service. The Citrix Update Service contains the latest plug-in updates and is used to populate the list of new plug-ins ready for download at **Plug-ins > Get New**.

1. Log on to the Administrator Console as administrator and select **Configurations > Options**.
2. Select a value from the **Polling Frequency** dropdown menu to define how often the Merchandising Server checks for plugin updates. The possible options are Week, 2 Weeks, and 4 Weeks. By default, the Merchandising Server checks the Citrix Update Service for updates daily at 12:01am.
3. Click **Save Changes**.

Want More Information?

- Defining Token Expiration Frequency
- Disabling HTTPS Redirection
- Configuring the Proxy Server

Defining Token Expiration Frequency

The first time Receiver for Windows requests a delivery from the Merchandising Server, the user enters their user credentials for access. As soon as the user is authenticated, a unique token is generated and installed on the user's computer. Subsequent requests from the Receiver to the Merchandising Server are validated with this token, eliminating the need for repeated logons.

The **Token Expiration** field in the **Configurations > Options** page allows you to specify the expiration interval. When the token expires, the user will be required to to re-enter his credentials before the Receiver can access the Merchandising Server for delivery updates. Once the credentials have been authenticated again by the Merchandising Server, a new token is generated and affective for the interval you specify here.

1. Log on to the Administrator Console as administrator and select **Configurations > Options**.
2. Select a value from the **Token Expiration** dropdown menu to define the interval for token expiration. The default value for token expiration is 6 months.
3. Click **Save Changes**.

Want More Information?

- Defining the Citrix Update Service Polling Frequency
- Disabling HTTPS Redirection
- Configuring the Proxy Server

Installing SSL Certificates

Important: All communications between the Merchandising Server and the Receiver client are encrypted with SSL. The Merchandising Server contains a temporary 30-day certificate. You are required to replace or renew this certificate within 30 days to ensure uninterrupted communication.

You can replace the temporary SSL certificate on the Merchandising Server with the following certificate types:

- An existing SSL certificate, such as a wildcard certificate. Your existing certificate has a private key file that was generated by a server other than the Merchandising Server. The private key file for the certificate must have an associated password (also known as a pass phrase). When you import an existing certificate, you must also import the private key file.

- An SSL certificate that you obtain by generating a certificate signing request from the Merchandising Server. You provide the certificate signing request to an internal or public certificate authority. Consult your security department to find out the CA required by your company and the procedure for obtaining server certificates.

If your company generates custom certificates using Microsoft Certificate Services, you may wish to use that process to obtain a signed certificate. See Creating a Certificate Signing Request for instructions on how to generate the certificate signing request. Once the certificate is issued, you download the signed certificate with Base 64 encoding method and use the instructions to import the certificate to your Merchandising Server, see Importing Certificates and Creating Signing Request for Microsoft Certificate Services for instructions on obtaining a certificate using Microsoft Certificate Services.

Want More Information?

- Generating a Self-signed SSL Certificate
- Importing Certificates
- Creating Signing Request for Microsoft Certificate Services
- Installing Local Or Customized SSL Root Certificates on Client Devices

Generating a Self-signed SSL Certificate

A self-signed certificate is already installed on the Merchandising Server. A self-signed certificate is only valid for 30 days and requires that users accept a security exception for a certificate that was not issued by a trusted certificate authority. If you choose to use the self-signed certificate, you must renew it every 30 days by generating it again, as follows.

1. Log on to the Administrator Console as administrator and select **Configurations > SSL Certificate Management**.
2. Select **Generate a self-signed certificate** from the **Select an action dropdown**.
3. In **Common Name**, enter the host name or IP address for the Merchandising Server. The value you enter in **Common Name** must be the same value you use to access the Merchandising Server.
4. Complete the rest of the fields. Use the on-screen hints to guide your input. If you have questions about completing these fields, contact your company's certificate expert.
5. Click **Submit** to generate a self-signed certificate for this Merchandising Server.

The certificate fingerprint appears in the Certificate Status area and the Merchandising Server restarts.

Want More Information?

- Creating a Certificate Signing Request
- Importing the Root Certificate
- Creating a Signing Request for Microsoft Certificate Services
- Installing Local Or Customized SSL Root Certificates on Client Devices

Creating a Certificate Signing Request

To obtain an SSL certificate from a certificate authority, you can use the Administrator Console to generate a Certificate Signing Request (CSR) required by the CA. You can then purchase a certificate from the CA by providing the completed CSR. The Merchandising Server also supports certificates whose CSR was generated by other servers.

1. Log on to the Administrator Console as administrator and select **Configurations > SSL Certificate Management**.

2. Select **Export certificate signing request** from the **Select an action** dropdown to create the certificate signing request.

3. In **Common Name**, enter the host name or IP address for the Merchandising Server and complete the rest of the fields. Use the on-screen hints to guide your input. If you have questions about completing these fields, contact your company's certificate expert.

4. Click the **Export** button to download the server.csr file that you provide to the CA to obtain a certificate.

5. Follow your company's procedure for contacting the appropriate CA to obtain a certificate. Have the following information available:

   - The CSR that you exported in the previous step.

   - Server platform information: The server platform is Apache and the certificate usage is Web Server. Not all CAs require this information.

   The CA provides an SSL server certificate as well as the root certificate.

Want More Information?

- Generating a Self-signed SSL Certificate
- Creating a Certificate Signing Request
- Importing Root Certificate
- Creating a Signing Request for Microsoft Certificate Services
- Installing Local Or Customized SSL Root Certificates on Client Devices

Importing Certificates

To replace the temporary certificate, you must import a server certificate into the Merchandising Server. The following procedure explains how to import server, intermediate, and chain certificates as well as private key files.

1. Log on to the Administrator Console as administrator and select **Configurations** > **SSL Certificate Management**.

2. Select **Import certificate from a certificate authority** from the **Select an action** dropdown.

3. Specify the files to be imported, based on the type of certificates you are using, as follows. **To import certificates generated from the Merchandising Server**

   a. Across from Public cert file, click **Browse** to locate the certificate file on your local computer.

   b. If you have an intermediate certificate file, click **Browse** to locate the intermediate file. The Merchandising Server already has the private key file needed for the certificate requests that it generates. Do not upload a private key file for this type of certificate.

   c. Click **Submit** to upload the certificate(s).

      The Certificate Status text box displays information about the certificate upon successful completion.

   To import certificates generated from other servers

   a. Across from Public cert file, click **Browse** to locate the certificate file on your local computer.

   b. If you have an intermediate certificate file, click **Browse** to locate the intermediate file.

   c. Across from Private key file, click **Browse** to locate the private key file for the certificate.

   d. Enter the Private key password (also referred to as the pass phrase) for the private key file.

   e. Click **Submit** to upload the certificate(s) and private key file.

      The Certificate Status text box displays information about the certificate upon successful completion.

   To import chain certificates

   a. Prepare the chain certificate file for import. First use a text editor to separate the server certificate into a separate file. The resulting intermediate certificate file will then contain the remaining certificates, with the root certificate at the end and the next intermediate certificate authority certificate above it, as follows.

```
----BEGIN CERTIFICATE----
[intermediate certificate B goes here]
----END  CERTIFICATE----
----BEGIN CERTIFICATE----
[intermediate certificate A goes here]
----END  CERTIFICATE----
----BEGIN CERTIFICATE----
[root certificate goes here]
----END  CERTIFICATE----
```

In rare cases, you will need to assemble the intermediate certificate file from several files. If so, just make sure that its order is as shown above. Use a text editor to make changes to certificate files.

b. Across from Public cert file, click **Browse** to locate the certificate file on your local computer.

c. Across from Intermediate certificate file, click **Browse** to locate the intermediate file.

d. If the request for the chain certificate was not generated by the Merchandising Server, click **Browse** to locate the private key file for the certificate.

e. If you specified a private key file, enter the Private key password (also referred to as the pass phrase) for the private key file.

f. Click **Submit** to upload the certificates and, if applicable, private key file.

The Certificate Status text box displays information about the certificate upon successful completion.

The Merchandising Server restarts.

Want More Information?

- Creating a Certificate Signing Request
- Creating a Signing Request for Microsoft Certificate Services
- Installing Local Or Customized SSL Root Certificates on Client Devices

Creating Signing Request for Microsoft Certificate Services

The following describes a generic process for requesting and downloading signed certificate from your internal signing authority.

1. Open a browser and enter your company's certificate services URL.
2. Select the link to request a certificate.
3. Select the link to submit a request using a base 64 encoded CMC or PKS #10 file or a renewal request by using a base-64 encoded PKSCS #7 file.
4. Paste the contents of your signed certificate request into the Saved Request field, see Creating a Certificate Signing Request.
5. Select Web Server in the certificate template field.
6. Click **Submit**.
7. When the certificate is issued, select the Base 64 encoding method and download the signed certificate.

Follow the instructions at Importing the Root Certificate to import the certificate to your Merchandising Server.

Want More Information?

- Creating a Certificate Signing Request
- Importing the Root Certificate
- Installing Local Or Customized SSL Root Certificates on Client Devices

Installing Local or Customized Certificates on Client Devices

Communications between the Receiver and the Merchandising Server are SSL encrypted. As a result of this, you need a root certificate on the client device that can verify the signature of the Certificate Authority on the Merchandising Server certificate.

If you are using SSL certificates from a local or custom Certificate Authority, you must distribute the root certificates so that they are available for all users in the centralized local computer certificate store, not just the main desktop user. If the root certificates are not available in the centralized local computer certificate store, Receiver for Windows cannot receive updates from the Merchandising Server.

The plug-ins installed on your users' computers support the Certificate Authorities that are supported by the Windows, Windows 7, or Vista operating system. The root certificates for these Certificate Authorities are installed with Windows and managed using Windows utilities. They are the same root certificates that are used by Microsoft Internet Explorer.

Configuring the Proxy Server

Note: If you are not using a proxy server, skip this configuration step. You are now ready to start creating deliveries, see Creating Deliveries.

If you are using a proxy server for external internet access, your proxy server configuration parameters are needed by the Merchandising Server to access the Update Service for plug-in updates. If you are using a proxy server and have not provided your configuration parameters, plug-in updates will not be available.

1. Log on to the Administrator Console as administrator and select **Configurations > Network Settings**.
2. Select the **Enable Proxy Server** checkbox. The Server Address and Server Port fields are displayed.
3. Enter your proxy server IP address or domain name and port number.
4. If user authentication is required, select the **Enable Authentication** checkbox. (Note: If user authentication is required, users need https access only.) The User Name and Password fields display.
5. Enter the user name and password for proxy server authentication.
6. Click **Save Changes**.

Want More Information?

- Defining Token Expiration Frequency
- Defining the Citrix Update Service Polling Frequency
- Disabling HTTPS Redirection

Creating Deliveries

Before creating a delivery you must upload the plug-in installation and metadata files to the Merchandising Server and create delivery recipient rules. Plug-ins available for delivery are posted to the Citrix Update Service and are viewed and downloaded from the **Plug-ins > Get New** in the Administrator Console. The readme and Eula files for each of the plug-ins can also be viewed from this location and from **Plug-ins > Uploaded Plug-ins**.

This section contains the following topics.

Preparing Updates

The Merchandising Server uses metadata files to ensure that plug-in deliveries to your users are silent and seamless. Metadata files are XML files that are paired with the plug-in install files to define the requirements for install, upgrade, and uninstall on your end users' computers.

You can upload the plug-in files directly from **Plug-ins > Get New** to the Merchandising Server.

The **Plug-ins > Uploaded Plug-ins** page contains the list of the plug-ins that you have uploaded to the Merchandising Server. You can remove plug-ins from the Merchandising Server and view plug-in readme and licensing files from this area.

Want More Information?

- Downloading Plug-ins to the Merchandising Server

Downloading Plug-ins to the Merchandising Server

To download plug-in files to the Merchandising Server

1. In the Administrator Console, select **Plug-ins > Get-New**.
2. Select the plug-in from the listing and click **Download to Server**.
3. When the download is complete, click **Close** in the status popup. The plug-in is now available to include in a delivery.

   The list of plug-ins ready for delivery is always available through **Plug-ins > Uploaded Plug-ins**.

Want More Information?

- Scheduling Deliveries

Uploading Plug-ins into Merchandising Server

Note: This is an optional procedure that is only necessary if you have used the alternate download method to download plug-ins to your desktop for evaluation.

To upload an installer and metadata file

1. In the Administrator Console, select **Plug-ins > Upload**.
2. Enter the plug-in **Display Name**. This is the name that is displayed in the **Plug-ins** tab when you schedule a delivery. If you enter a name that you have used previously, the previous installer and metadata files is overwritten.
3. Click **Browse** to navigate to the location for the plug-in installer and metadata files.
4. Click **Upload**. When the upload is complete, the list of plug-ins uploaded to Merchandising Server is displayed in the **Plug-ins > Uploaded Plug-ins**.

Creating Delivery Recipient Rules

Delivery recipients are defined based on the rules you create. Rules can be defined by User Name, User Group, User Domain, Machine Name, IP Address, or Operating System. You can create as many rules as you need and use them individually or in combination to define a set of delivery recipients.

Note: One delivery can be defined as the default delivery. The default delivery cannot contain rules. For more information on the default delivery, see Defining General and Installation Delivery Information.

To create a recipient rule

1. In the Administrator Console, click **Deliveries** > **Rules**.
2. Click **Create** at the bottom of the page.
3. Enter the rule name and description.
4. Select the rule type from the dropdown menu and complete the steps as described in the following table.

If you select ...	Do the following ...
LDAP User Name	a. Enter the user name in the **Search** field. b. Select user name checkbox from search results. c. Click **Add**.
User Domain membership	a. Select the Operator from the dropdown list. The possible options are **Is** and **Is Not** b. Enter the domain membership name in the Value field.
LDAP Group Name	a. Enter the group name in the **Search** field. b. Select group name checkbox from search results. c. Click **Add**.
Operating System	a. Select the Operator from the dropdown list. The possible options are **Is** and **Is Not** b. Select operating system value from the dropdown menu.

IP Address Range	a. Select the Operator from the dropdown list. The possible options are **Is** and **Is Not** b. Enter the IP address in the Value field.
Machine Name	a. Select the Operator from the dropdown list. The possible options are **Begins With**, **Contains**, and **Is Exactly** b. Enter the machine name in the Value field.
Machine Domain membership	a. Select the Operator from the dropdown list. The possible options are **Is** and **Is Not** b. Enter the domain membership name in the Value field.

5. Click **Save** to save your rule. You can now use this rule when creating new deliveries.

Want More Information?

- Adding Rules to Deliveries
- Creating Deliveries

Rules: Use Case Scenario for Creating Targeted Deliveries

Targeted deliveries allow different types of users and computers to have specific plug-in deliveries and configurations. Targeted deliveries use a rules-based system. The first step is to create rules based on the items below; the second step is to apply the rules, along with other parameters, to a delivery.

The following scenario provides an example of how a university IT department might use rule types to serve the specific needs of staff, faculty, students, offices, labs, home computers, and more.

Rule Type	Used For...
User Domain	Delivering plug-ins and/or configurations based upon user-domain membership. For example, a university could use this type of rule to deliver certain services and applications to students, others to staff, and still different services to faculty where each group belonged to a different domain.
Computer Domain	Delivering plug-ins and/or configurations based upon a machine-domain membership. For example, a university could use this type of rule to deliver specific services and applications to office, lab, personal, and student computers that below to different machine domains.
Operating System	Delivering plug-ins and/or configurations based upon operating system type. For example, a university could use this type of rule to deliver a plug-in that works on Windows XP and Windows Vista, but not on Windows 7, or only users of Windows XP and Windows Vista computers.
LDAP User	Delivering plug-ins and/or configurations to specific users (no matter which computer they are on), and not to the computer itself. For example, a university could use this rule type to deliver specific capabilities to staff who user their personal computers in a BYOC program.
LDAP Group	Delivering plug-ins and/or configurations to groups of users (no matter which computer they are on), and not to the computer itself. For example a university could create an LDAP group for all students taking a Computer Aided Drafting course hosted on a specific XenApp farm and allow only those students access to that farm.

Machine Name	Delivering plug-ins and/or configurations where many people share the same machine and all need the same configuration to complete their tasks. For example, a university with different computer labs that cater to different educational programs, can use the machine name rule to deliver plug-ins to all machines that have a name that contains BLD200 so that all computers in the building 200 lab have the same capabilities.
IP Address Range	Delivering plug-ins and/or configurations based upon a computer's IP address. For example, a university can configure this type of rule to deliver a specific configuration to students on a specific subnet and a different configuration to a faculty on a different subnet.
Default Delivery	Delivering a default set of plug-ins and configurations where other more specific rules do not apply. For example, a university could deliver a limited set of services to any user of campus IT services who does not qualify for any extended or specialized services.

Creating Deliveries

Note: You must create recipient rules before creating a delivery, see Creating Delivery Recipient Rules. Additionally, you must load at least one plug-in onto your server before you can create a delivery. See Downloading Plug-ins to the Merchandising Server.

When you create a delivery, you define the following information:

- General — Define delivery name, description, server polling frequency for delivery updates. See Defining Installation Parameters.
- Plug-ins — Select plug-ins for delivery. You are actually selecting both the install and the metadata files for the given plug-in. The metadata files for each plug-in are preconfigured and don't require modification. However, if you wish to edit the metadata files, the metadata schema and a sample metadata file are provided for you in Metadata Reference.
- Configuration — Many of the plug-in configuration parameters are defined in its metadata file, but some parameters may change by delivery such as the location of its server. In this case, the server location is provided on this page, see Configuring Plug-in Parameters.
- Rules — Create rules based on machine name, machine domain membership, IP address, operating system, user name, user domain membership, or user group name. Rules can be combined within a delivery to create a complex recipients list, see Creating Rules and Adding Rules to the Delivery.
- Schedule — Define the date and time that the delivery is available for transmission to your users, see Scheduling a Delivery

Deliveries can also include the user support information defined in **Configuration > Options** in the Administrator Console, see Configuring Server Options. This information is the default data used to populate the Receiver for Windows Preference panel. If the delivery installation settings do not contain specific settings for these parameters.

You can copy an existing delivery and modify it accordingly or you can create a new delivery.

To create a new delivery

1. Select **Deliveries > Current Deliveries** in the Administrator Console. The list of current deliveries is displayed. If you have previously created one or more deliveries, the list of deliveries is displayed along with evaluation order, delivery status, and installation status. From this page you can create, copy, edit, delete, suspend, and resume deliveries.
2. Click **Create** at the bottom of the page.

   Create a Delivery is displayed with the **General** page activated.

3. The process for defining delivery information is described in the following sections:
    - Defining Installation and Installation Delivery Information
    - Adding Plug-ins to Deliveries
    - Configuring Plug-in Parameters
    - Adding Rules to Deliveries
    - Scheduling Deliveries

Next Steps?

- Defining General and Installation Delivery Information
- Adding Plug-ins to Deliveries
- Configuring Plug-ins
- Adding Rules to Deliveries
- Scheduling Deliveries

Defining General and Installation Delivery Information

The delivery **General** tab contains delivery information and installation properties.

To add or edit general and installation delivery information

1. Click the **General** tab from within a delivery creation or editing process.
2. Enter the values for the fields defined in the following table:

Field	Description
Delivery Name	This is a text field containing the delivery name.
Evaluation Order	A single user may be a recipient of more than one delivery. If this is the case, the Evaluation Order determines which delivery the user receives. The delivery with the lowest evaluation number is delivered to the user. All other deliveries are ignored. Select a value from the drop-down list.
Default Delivery	Selecting the Default Delivery checkbox designates the delivery as the default and as such, no rules can be defined. Users receiver the default delivery if they are not schedule to receiver any other delivery. Only one delivery can be designated as the default delivery.
Silent Install	If this is enabled, the Receiver does not give the end user the opportunity to cancel or pause any part of the installaton.
User Help URL	The URL to the user help system for the Receiver, which is accessed through the Receiver right-click menu or Preference panel. The default value, http://support.citrix.com/receiver/help/*release*/windows/en/User/Default.htm, is overwritten if a value is entered in this field.
Check for updates	The numerical value in days. This value defines the Receiver interval for polling the Merchandising Server for delivery updates. A value in this field overrides the **Polling Frequency** value set in the **Configurations > Options** page.
Secure connectivity	One of two options are available, always provide a secure connection or ask the user permission before providing a secure connection. This feature allows either the user to define connectivity through the Receiver Preferences or grays out the preference and makes it configured by the admin.
Completion text	Enter the message you want displayed to the end user at installation completion for this delivery. The following table contains recommended text for the various access methods.

For user application and desktop access through:	We recommend this text:

The Windows **Start** menu	Your applications can be found on the Windows Start menu.
A custom folder name, [MyWorldco Apps], in the Windows **Start** menu	Your applications can be found in the [MyWorldco Apps] Folder, on the Windows Start menu.
A XenApp icon on the user's desktop	Your programs can be found by clicking the blue applications icon on your desktop.
A web interface	* Your applications can be found by navigating to: [https:applications.worldco.com]
A URL (for XenDesktop virtual desktops)	* To start your virtual desktop, navigate to: [https://XenDesktop.worldco.com].
Dazzle	Use Dazzle to select your applications.

* URLs included in the Completion text for a delivery are not displayed to the user as hyperlinks.

3. Proceed to Adding Plug-ins to a Delivery.

Next Steps?

- Adding Plug-ins to Deliveries
- Configuring Plug-ins
- Adding Rules to Deliveries
- Scheduling Deliveries

Adding Plug-ins to a Delivery

The functionality for adding or removing plug-ins from a delivery is contained in the **Plug-ins** tab within the **Create a Delivery** or **Edit a Delivery** wizards, see Creating Deliveries.

To add plug-ins to a delivery

1. Click the **Plug-ins** tab In the **Create a Delivery** or **Edit a Delivery** page. The listing displays the name of the plugin, its version, the supported operating system and languages, and the plug-in action for this delivery.
2. Click **Add** at the bottom of the page.
3. Select the **Action** from the dropdown list at the top-right of the page. The possible options are **Install** and **Uninstall**
4. Select the checkbox for a each plugin you want added with this action.
5. Click **Add** at the top-left of the page (below the Action button).

   Note: To include plug-ins with the alternate action, repeat steps 3 and 4 with the alternate action selected.
6. The Plug-ins listing now contains the added plug-ins. Proceed to Configuring Plug-in Parameters.

Next Steps?

- Configuring Plug-in Parameters
- Adding Rules to Deliveries
- Scheduling Deliveries

Configuring Plug-in Parameters

The plug-in configuration information is different depending on the plug-ins that your have added to your delivery. For most plug-ins, the **Config** page contains fields to define each plug-in's server information.

To define the configuration parameters for your plug-ins

1. Click the **Config** tab.
    a. If you are delivering the communications plug-in, enter the EasyCall Gateway IP address.
    b. If you are delivering the online plug-in, enter the XenApp server IP address.
    c. If you are delivering secure access plug-in, coordinate the values you enter here with your Access Gateway Appliance.
        - Select either single or dual authentication by clicking **Single** or **Dual** and enter the field names to display in the log on page to your users.
        - Enter the Access Gateway Appliance host name and IP address. You can enter multiple host names here. The entries are added to the hosts file on your users' computers.
2. Proceed to Adding Rules to Deliveries.

Next Steps?

- Adding Rules to Deliveries
- Scheduling Deliveries

Adding Rules to the Delivery

Before adding rules to a new delivery, first create your rules as described in Creating Delivery Recipient Rules. You can add as many rules as you want to a delivery. Rules can be added using the **Basic** or **Advanced** functionality. In the Basic mode, rules can only be added using either the AND or OR operators, not both. With the Advanced mode, rules can be using both operators.

To add rules defining the recipients of a delivery

1. In the **Create a Delivery** (or Edit a Delivery) page, click the **Rules** tab.
2. To add rules in the basic mode:
    a. Select **Basic** above and to the left of the rule listing.
    b. Select the operator to use for combining your rules. The choices are AND or OR. In the basic mode, you can only select one type of operator.
    c. Click **Add** at the bottom of the page. The Add Rule to Delivery page displays.
    d. Select one or more of the rule checkboxes and click **Add**.

    Note: You can also use the Search box to find your rules.
3. To add rules in the advanced mode:
    a. Select the **Advanced** link. The advanced mode allows you to create blocks of rules. Rules within a block are AND'd and rule blocks are OR'd together, the combination of which defines the recipients for this delivery.
    b. Click the link to add a rule. The **Add Rule to Delivery** page displays. Follow the same process as in the basic mode to add one or more rules to this rule block.
    c. Click the link to add a new rule block. A new block in displayed in the Advanced page and the **Add Rule to Delivery** page again displays. Add the appropriate rule(s).

    When you are done adding rules to your rule blocks, the **Rules > Advanced page** appears similar to this:In the graphic above, the result of an AND operation on the two rules in the first block are OR'd with the rule in the second block.
4. Proceed to the **Schedule** tab to complete the final step in delivery creation.

Next Steps?

- Scheduling Deliveries

Scheduling Deliveries

Scheduling the delivery is the last step in the delivery creation process. From the **Schedule** tab, you can define when the delivery is available to your end users.

To schedule a delivery

1. Click the **Schedule** tab from within a delivery creation or editing process.
2. In **Schedule Delivery Start Time**, select **Now** or **Later**. If you select Later, specify the Date and select the Time from the drop down list and specify AM or PM for the delivery. tab.
3. Click **Schedule** to complete the process.

Want More Information?

Note: If you click **Cancel** on this page, none of your changes are saved. If you are in the process of editing an existing delivery, canceling will result in a roll back to the saved delivery configuration. If you are in the process of creating a new delivery, the new delivery is discarded and cannot be retrieved.

- Removing Plug-in Files from the Merchandising Server
- Updating Plug-ins
- Redelivering Plug-ins
- Removing Receiver for Windows and its Managed Plug-ins from your Client's Device

Getting Delivery Status

The **Reporting and Logging > Delivery Reporting** page contains reporting information at three levels: delivery, plug-in, and user. The Delivery Reporting page shows a listing of all deliveries with their status, success statistics, the list of users who have installed the delivery, the user's computer information, installation status, and the list of the plug-ins included in the delivery.

The plug-in report contains an entry for each plug-in in the delivery and displays the plug-in version, action performed, platforms supported, configuration values, and a link to the plug-in's readme file.

The user report contains user name, delivery name, machine name, IP address, domain name, list of plug-ins installed and installation status. The user report also contains the functionality to redelivery the latest delivery or uninstall the Receiver and the plug-ins installed with this delivery. For more information on redelivery and uninstall, see Managing Plug-ins.

To view delivery report

1. Click on **Reporting and Logging > Delivery Reporting** in the Administrator Console to view the delivery report listing.

2. To view the summary delivery information, select the checkbox for a delivery and click **View Delivery Report** at the bottom of the page.

3. To view the plug-in report, click the **View Full Details** link in the delivery report title. The plug-in report contains delivery success statistics and detailed information on each plug-in.

4. To view the user report, in the delivery report listing:

   a. Select **Name** from **Search By** dropdown list. The list of all users that have received a delivery is displayed.

   b. Select the checkbox for the desired user.

   c. Click **View User Report** at the bottom of the page.

   The user name, delivery name, machine name, IP address, domain name, and plug-in installation status are displayed. This page also contains the functionality to redeliver and to uninstall the delivery, see Redelivering Plug-ins and Removing the Receiver and its Plug-ins.

Want more Information?

- Redelivering Plug-ins
- Removing the Receiver and its Plug-ins

Deploying Other Citrix Products and Features

You can deploy the following Citrix products and features with Receiver by scheduling the associated plug-in in a Merchandising Server delivery:

- Access Gateway
- Other VPNs
- EasyCall
- Branch Repeater Acceleration
- EdgeSight Monitoring
- Profile Management

Deploying Access Gateway

The Access Gateway Enterprise Edition beginning with version 9.0 build 68.6 is closely integrated with Citrix Receiver. This is the same for the Access Gateway Standard and Advanced Edition client software beginning with version 4.6.1. When Citrix Receiver is deployed with the Access Gateway Secure Access Plug-in, Receiver automatically launches the logon page and prompts the user for credentials when it detects the need for secure communications.

To allow users to log on through Citrix Receiver, deploy Receiver and the Secure Access Plug-in by scheduling a delivery in the Merchandising Server Administrator Console or use the packager utility to create a bundled installer and place the installer on an external download page.

Note: Due to Access Gateway and plug-in compatibility requirements, after the Secure Access Plug-in is installed by Receiver, it continues to be automatically updated from the Access Gateway (not Receiver).

Tip: Beginning with the Access Gateway Standard and Enterprise Editions 4.6, users who do not have Receiver installed, can access the following link (after authenticating) to download the bundled Receiver and plug-ins:
http://ec2-75-101-182-218.compute-1.amazonaws.com/index.html

If multiple appliances are deployed in multiple locations, Receiver allows users who are traveling to select the nearest location. To define more than one location for an Access Gateway Plug-in, add it to a delivery in the Merchandising Server, and on the Configuration tab of the delivery wizard (click Add a New Location). The new locations appear in the Citrix Receiver for Windows client under Advanced/Network Settings.

Also, you can use the Merchandising Server to choose which fields to display to your users when they need to create a secure connection to delivery services. You can choose either single or double-source authentication and specify labels for the associated logon fields.

Using other VPNs with the Receiver

Citrix Receiver is fully integrated with the Access Gateway Enterprise Edition and will automatically detect when a remote user needs a secure connection to access a company's internal network. If your remote users employ another VPN product, they need to obtain a secure connection with their alternate VPN product before utilizing the full functionality of Citrix Receiver.

Deploying Easy Call with the Receiver

Once EasyCall Gateway is configured, there are several ways to deliver EasyCall services to end users. The EasyCall client software, now called the Citrix communications plug-in, may be downloaded and installed by the user, streamed to the user's desktop as an offline application through XenApp, published to users as an online application again through XenApp (refer to EasyCall documentation for limitations), and deployed through the Merchandising Server as a Citrix Receiver compatible plug-in.

To deploy Citrix communications plug-in using Citrix Receiver, schedule the Citrix communication plug-in in a delivery and configure it to point to the EasyCall Gateway you configured with your telephone system.

Note: The EasyCall communication plug-in is large and may take several minutes to install.

Deploying Branch Repeater Acceleration

Citrix Acceleration Plug-in works in conjunction with one or more Repeater appliances located in data centers. To deploy the Citrix Acceleration Plug-in using Citrix Receiver, schedule the Citrix Acceleration Plug-in in a Merchandising Server delivery and configure it to point to the appropriate Repeater appliances. After it is installed by Citrix Receiver, the Acceleration Plug-in offers transparent and always-on functionality – end-users do not need to enable or disable the Acceleration Plug-in as they will not even know it is there.

Deploying EdgeSight Monitoring

To deploy the Service monitoring plug-in using Citrix Receiver schedule the Service monitoring plug-in in a Merchandising Server delivery and configure it to point to the appropriate EdgeSight server.

Deploying Profile Management

Profiles are a critical component to a seamless and positive user experience. It is important to select, design and implement any profile solution while ensuring a proper match with the business and user needs. Citrix recommends consulting your Citrix Partner to properly plan for and implement any Profile management solution.

Recommendations:

- Leveraging mandatory or roaming profiles first (including the use of Folder Redirection
- If mandatory or roaming profiles do not fulfill your needs, evaluate and leverage Citrix Profile management
- If mandatory, roaming or Profile management do not meet your needs, evaluate third-party solutions such as AppSense and RES

For best practice guidelines, see the following articles in the Citrix Knowledge Center:

- Best Practices (ctx119036)
- User Profile Best Practices (XA5) (ctx120285)
- User Profile Best Practices (CPS 4.5 and prior) (

To deploy the Citrix Profile Management plug-in using Citrix Receiver schedule the Citrix Profile Management plug-in in a delivery.

Managing Plug-ins and Deliveries

The management tasks for plug-ins include:

- Removing plug-ins from the Merchandising Server.
- Removing a delivered plug-ins from your user's computer.
- Getting plug-ins updates.
- Redelivering, suspending, and restoring deliveries.

Updating Plug-ins

You download Citrix plug-in updates to the Merchandising Server from the **Plug-ins > Get New** page in the Administrator Console. Once the plug-in updates are loaded onto the Merchandising Server, they are available for inclusion in a delivery.

Note: If users are inside a firewall, the Merchandising Server updates the secure access plug-in. Remote users are updated the first time they encounter the Access Gateway directly from the Access Gateway.

To add an updated plug-in to a delivery:

1. Follow the process to download the latest updates from the Citrix Update Service, see Downloading Plug-ins to the Merchandising Server.
2. To add the plug-in update to an existing delivery:
    a. Select the delivery checkbox in the delivery listing at **Deliveries > Deliveries**.
    b. Click on the **Plug-ins** tab.
    c. Select the obsolete plug-in checkbox in the plug-in listing.
    d. Click **Delete**. Click **Add** and follow the process described in Adding Plug-ins to a Delivery to add the updated plug-in.
3. To create a new delivery with the updated plug-in, follow the process described in Creating Deliveries.

Want More Information?

- Removing Plug-in Files from the Merchandising Server
- Redelivering Plug-ins
- Removing Receiver for Windows and its Managed Plug-ins from your Client's Device

Redelivering Plug-ins

Redelivery is intended to fix any installation problems that may have occurred with the original delivery. The redelivery process first removes and then re-installs the plug-ins on the recipient's computer.

To redeliver the latest installation on a user's computer:

1. In the Administrator Console, select **Reporting and Logging > Delivery Reporting**.
2. Select **Name** in the **Search By** dropdown list. The list of user names is displayed.
    - You can also search by Machine Name. Domain name, or IP Address.
3. Select the checkbox for the desired user name in the user listing and click **View User Report**.

    Note: You only need to enter the first few letters of the criteria in the **Search** text box to retrieve viable results.
4. Click **Redeliver**. The originally delivered plug-ins are removed and re-installed on this user's device.

Want More Information?

- Removing Plug-in Files from the Merchandising Server
- Removing Receiver for Windows and its Managed Plug-ins from your Client’s Device

Removing Plug-in Files from the Merchandising Server

You remove plug-ins from the Merchandising Server through **Plug-ins > Uploaded Plug-ins** in the Administrator Console.

You cannot remove a plug-in that is part of an active delivery. If you attempt to delete a plug-in that is part of an active delivery, you receive a message stating that this plug-in cannot be removed because it is part of an active delivery and listing the active deliveries that contain this plug-in. See Creating Deliveries for more information on active deliveries.

To remove plug-in files from the Merchandising Server

1. In the Administrator Console, click **Plug-ins > Uploaded Plug-ins**.
2. Select the button for the plug-in you want to remove from the Merchandising Server.
3. Click **Delete**.

Want More Information?

- Updating Plug-ins
- Redelivering Plug-ins
- Removing Receiver for Windows and its Managed Plug-ins from your Client's Device

Removing the Receiver and its Plug-ins

You can completely remove an installation of Receiver and all of its managed plug-ins from a user's computer through the User Delivery Reports in **Reporting and Logging > Delivery Reporting**.

Important: The user will no longer have access to any plug-ins that were previously installed as they are uninstalled during this process.

1. In the Administrator Console, click **Reporting and Logging > Delivery Reporting**.
2. Select **User** from the **Search By** dropdown list.
3. Select the checkbox for the user’s name and click **View User Report**.
4. Click **Uninstall**.

Want More Information?

- Removing Plug-in Files from the Merchandising Server
- Redelivering Plug-ins
- Updating Plug-ins

Maintaining the Merchandising Server

Use the XenCenter console in XenServer to perform maintenance tasks on Merchandising Server.

To upgrade Merchandising Server, select**Configurations > Upgrade** on the administrator console.

Changing the Server Network Settings

XenCenter contains the functionality for changing your Merchandising Server IP address, the host name, netmask, gateway, and domain name system settings. It also contains the diagnostic capabilities to ping a server, traceroute, turn SSH on, and set the root password. If you are not familiar with using the XenCenter, refer to Importing the Virtual Appliance.

Note: The Merchandising Server does not support DHCP.

1. Start Citrix XenCenter.
2. In the XenCenter navigation frame, click your Merchandising Server VM.
3. Click the **Console** tab. The **Network Configuration Utility** opens.
4. Enter the numerical values as directed on the screen to establish the IP address, netmask, default gateway, and a DNS server for this server.
    a. Enter 1 to change the host name.
    b. Enter 2 to change the IP address.
    c. Enter 3 to change the netmask.
    d. Enter 4 to change the gateway.
    e. Enter 5 to change the domain name.
    f. Enter 9 to save your changes.

    Note: An asterisk is displayed by each setting that you have changed but not saved.

    The system reboots after saving the changes.
5. Enter 8 to troubleshoot the server with this utility. If you have not saved your changes, the changes will be discarded when you enter the diagnostic level. Enter 'y' to continue to the diagnostic menu.
    a. Enter 1 to ping an IP address.
    b. Enter 2 to perform a traceroute.
    c. Enter 3 to turn ssh on.
    d. Enter 4 to set the root password.
    e. Enter 8 to update XenTools - selecting this options will cause the system to reboot.
    f. Enter 0 to return to the main menu.
6. Enter uppercase 'R' to reset all of the settings to the original factory settings.

Important: Once you reset to the original settings, you have to reconfigure all of the network settings to access the Merchandising Server.

Want More Information?

- Importing the Virtual Appliance
- Configuring the Proxy Server

Ensuring Merchandising Server High Availability

The Merchandising Server may be deployed as a single server. If the Merchandizing Server becomes unavailable or is removed from service temporarily, users will be largely unaffected. However new users will not be able to download Receiver and have their computers configured and will not receive scheduled updates until the Merchandising Server is restored.

If your require higher availability, the simplest and easiest method is to use the capabilities provided by XenServer. XenServer can be configured with automated high-availability protection allowing virtual machines on a failed host to automatically restart on another physical server according to priority. Citrix Essentials for XenServer provides a range of high-availability capabilities, from automatic restart of hosts and virtual machines after a hardware failure to full fault tolerance of hardware and applications. A key advantage to this approach is that only a single Merchandizing Server needs to be configured. See How to Configure High Availability in XenServer 5.0 (CTX118545) in the Citrix Knowledge Center for more details.

Upgrading the Merchandising Server Software

Upgrade Merchandising Server through **Configurations > Upgrade Server** in the Administrator Console.

To upgrade your Merchandising Server

1. Download the Merchandising Server upgrade file from http://mycitrix.com to your local computer.

2. Log onto the Administrator Console with administrator permissions and select **Configuration > Upgrade Server**.

3. Click **Browse** to locate the upgrade file on your local computer and click **Upgrade**.

4. Click **Yes** in the confirmation popup to continue with the upgrade. While the upgrade file is copied to the server, the Administrator Console Upgrade Server page will display a spinning icon and the page will be grayed out.

5. Once the file is copied to the server, the upgrade process begins. The status window contains a message stating that the server is upgrading and to return later.

The upgrade process takes between 5 and 10 minutes to complete depending on your server configuration. The Merchandising Server is restarted when the upgrade is completed and you can log back into the Administrator Console.

Auditing Administrative Actions

The user with auditor permissions can view Audit Trail reports and grant Auditor permissions to other users. The Audit Trail report logs the actions that every administrators performs in the Administrator Console. The Audit Trail report file is a .csv file that can be downloaded or viewed from the Administrator Console. The .csv file contains Date, User name, Action type, Area affected, and Item affected columns.

For instructions on granting permissions, see Granting Administrator and Auditor Permissions.

Logging on as Auditor

Auditor permissions allow access two features within the Administrator Console: viewing audit trail and granting auditor permissions. Only a user logged in with Auditor or root permissions can grant Auditor permissions.

To log on as an auditor:

1. In a web browser, enter the URL for the Administrator Console. It is similar to http://[*serverAddress*]/appliance.
    - Where *serverAddress* is the Merchandising Server IP address or the host name.
2. Enter the your user name and password and then click **Log on**.
    - User name: Your Active Directory user account name. Enter the user name in the form of domain\username.
    - Password: Your Active Directory login password.

    Note: Your credentials are case sensitive.

    The Administrator Console opens. With the Audit Trail selection criteria active.

You can now view the audit trail and grant users auditor permissions.

Next Steps?

- Viewing the Audit Trail
- Granting Administrator and Auditor Permissions

Viewing the Audit Trail

The audit log captures all events that every administrator performs. This includes:

- All actions performed in the Plug-in node.
- All actions performed in the Deliveries node.
- All actions performed in the Configurations node.
- All changes to the root passwords.
- All logons to the Administrator Console.

1. Log in to the Administrator Console with auditor permissions.
2. Select **Reporting and Logging > View Audit Trail**.
3. Enter the dates that define the range of time you wish to view.
4. Click **Export to .csv**.
5. The **Opening Audit Trail** popup gives you the options to view the file or save it to your desktop. Select the appropriate option and click **OK**.

Next Steps?

- Logging on as Auditor
- Granting Auditor Permissions

Troubleshooting

There are six mechanisms within the Administrator Console to assist your troubleshooting efforts:

- Triggering the retrieval of client log files - Triggering Retrieval of Client Log.
- Enabling system debug logging - Enabling System Debug Logging.
- Enabling user debug logging - Enabling End User Debug Logging.
- Viewing debug log files - Viewing Debug Logs.
- View client log files - Viewing Client Logs.
- Changing the location of the Merchandising Server on the user client device - Changing Merchandising Server Location.

Enabling System Debug Logging

You can turn-on system level debugging, which logs all system background activities through **Reporting and Logging > Enable /Disable Logging** in the Administrator Console. Once you have enable system level debugging, you can view the debug log file through **Reporting and Logging > View Log Files**. The system activities are posted to the log file until you disable debugging.

To enable system debugging:

1. Select **Reporting and Logging > Enable / Disable Logging** in the Administrator Console.
2. Click **Enable System Logging** at the bottom of the page.
3. Click **Confirm** in the configuration popup to process the request.
4. Click **Close** in the operation completion popup to complete the process.

All system activities will be posted to the log file on the server until you disable system debugging. To view the debug log file, see Viewing Debug Files.

Want More Information?

- Changing Merchandising Server Location
- Triggering Collection of Client Log File
- Viewing Debug Files

Enable User Debug Logging

You can enable system debug logging at the user level through **Reporting and Logging > Enable / Disable** in the Administrator Console. If you enable this feature, all actions taken by the Receiver for the specified user are captured and logged. You can view the debug log files through **Reporting and Logging > View Log Files**, see Viewing Debug Log Files.

1. Select **Reporting and Logging > Enable / Disable Logging** in the Administrator Console.
2. Select the checkbox for the users for which you want to enable debug logging.
3. Click **Enable User Logging** at the bottom of the page.
4. Click **Confirm** in the configuration popup to process the request.
5. Click **Close** in the operation completion popup to complete the process.

All activities on behave of the specified end user are continually posted to the `appliance.log` file on the server until you disable end user debugging.

Want More Information?

- Changing Merchandising Server Location
- Triggering Collection of Client Log File
- Viewing Debug Log File

Triggering the Collection of Client Log Files

You can trigger the retrieval of a client's log file through **Reporting and Logging > Enable / Disable Logging**. Once you have triggered collection, the log file from the specified client device is retrieved the next time Receiver for Windows gets an update. This is a one time only action, meaning the log file that is on the user's client device at the time of the retrieval request is sent to the server; log files are not continuously sent.

To trigger the retrieval of log files from an client's device:

1. In the Administrator Console, select **Reporting and Logging > Enable / Disable Logging**.
2. Select the checkbox by the user's name. Alternatively, you can search for the user by name:
    a. Enter the first few characters of the user's first or last name in the **Search** field.
    b. Click **Search**.
    c. Select checkbox for user name.
3. Click **Trigger Client Log Collection**.
4. Click **Confirm** in the confirmation popup to process the request.
5. Click **Close** in the operation completion popup to complete the process.

The log files are retrieved the next time the user's Receiver for Windows gets an update from the Merchandising Server.

Want More Information?

- Viewing Client Log Files
- Changing Merchandising Server Location
- Enabling of System Debug Logging
- Viewing Debug Files

Viewing Client Log Files

Once you have triggered the retrieval of log files from a client's device, you can access the log files through **Reporting and Logging > View Log Files**.

To view the log files retrieved from a client's device

1. In the Administrator Console, click **Reporting and Logging > View Log Files**.
2. Select the checkbox for the user and click **Download Client Log**.
3. The Open file popup requests you to select whether you want to open the file or save it to your desktop. To view the ErrorLog.xml file, choose **Open** and select the application to open it. The `ErrorLog.xml` opens and look similar to the following image:

Want More Information?

- Changing Merchandising Server Location
- Enabling System Debug Logging
- Viewing Debug Files

Downloading the Debug Log Files

Once you have enabled debugging at either the user or system level, you can download the log files through **Reporting and Logging > View Log Files**.

To download the server log files

1. In the Administrator Console, click **Reporting and Logging > View Log Files**.
2. Click **Download Server Logs** at the bottom of the page.
3. Select the checkboxes for files you want to download from the **Download Server Logs** popup.
4. Click **Download Logs**.
5. Click **Save File**, provide file save location, and click **Save**. The compressed zip file is saved to the location you entered. Decompress the file for viewing.

Want More Information?

- Viewing Client Log Files
- Changing Merchandising Server Location
- Enabling System Debug Logging
- Triggering Collection of Client Log Files

Changing the Merchandising Server Location

Important: Changes to the server location can interrupt the delivery of plug-ins to your clients.

Receiver for Windows fetches updates from the Merchandising Server whose location is defined in the `Receiver.cfg` file located in the Receiver for Windows installation directory on the client's device. For a standard installation this is located at `C:\Program Files\Citrix\Receiver\Receiver.cfg`.

The `Receiver.cfg` contains only one line of text which is the Merchandising Server address, as an example:

https://[*ServerAddress*]/appliance/services/applianceService/

Where: *ServerAddress* is either the Merchandising Server domain name or IP address.

Metadata Reference

The metadata files are the means by which deliveries are made to your users without requiring user interaction. Each plug-in install file is paired with a metadata file that contains all of the properties and commands required to ensure proper installation while minimizing or eliminating user involvement.

When you select a plug-in for delivery, you are actually selecting both the install and the metadata files for the given plug-in. The metadata files for each plug-in come preconfigured for you and don't require modification. However, if you wish to edit the metadata files, the metadata schema and a sample metadata file are provided in this section.

Metadata Schema

The metadata file for an installer is an xml file that defines the properties for each of the applications present in the installer file.

Note: We recommended that if you edit a metadata file, you should validate it against the schema shown here using one of many available XML Schema verification tools. The schema is available for download from the Citrix support web site.

The metadata file has the following schema:

```
<xs:schema
   xmlns="http://www.citrix.com/AppReceiver"
   elementFormDefault="qualified"
   targetNamespace="http://www.citrix.com/AppReceiver"
   id="metadata"
   xmlns:xs="http://www.w3.org/2001/XMLSchema">

 <xs:element name="metadata">
     <xs:complexType>
     <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="100" name="plugin" type="pluginListType" />
      </xs:sequence>
        <!-- This attribute is listed as optional for backward compatibility, but
            plugins adopting 1.1 schema elements "MUST" set this to "1.1" to
            ensure correct options -->
      <xs:attribute default="1.0" name="versions" type="xs:token" user="optional" />
     </xs:complexType>
 </xs:element>

 <xs:complexType name="pluginListType">
    <xs:all>
      <!-- Supported platforms -->
      <xs:element name="platforms" type="platformTypeList" minOccurs="1" />

      <!-- Released Version of Plugin (Installer) -->
      <xs:element name="version" type="versionType" />

      <!--URL to EULA text (if available)-->
      <xs:element name="EULAlocation" type="xs:anyURI" minOccurs="0" />

      <!-- Install string & Attributes -->
      <xs:element name="autoInstall" type="arUpdatingInstallType" />

      <!-- Uninstall string & Attributes -->
      <xs:element name="autoUninstall" type="arInstallType" minOccurs="0" />

      <!-- Upgrade string & Attributes -->
      <!-- If the upgrade string is omitted the install string will be used for upgrades. -->
      <xs:element name="autoUpgrade" type="arUpdatingInstallType" minOccurs="0" />
```

```
<!--  Admin requirements-->
<xs:element name="adminOptions" type="installationAdminPrivsType" default="none" />

<!--  This plugin normally deployed if not present, it will be updated
     by itself in communication with its server component -->
<xs:element name="installOnce" type="xs:boolean" default="false"  minOccurs="0" />

<!--  Should it be important to maintain the filename of the installer,
     provide this element -->
<xs:element name="installerFilename" type="xs:string" />

<!-- Admin console GUI generating information -->
<xs:element name="installerOptGUI" type="commonInstallerOptGUIListType" minOccurs="0" />

<!-- Informed Consent / Plugin Description -->
<xs:element name="pluginDescriptions" type="pluginDescriptionListType" />

<!-- List of Languages the plugin supports  -->
<xs:element name="pluginLanguages" type="languageTypeList" minOccurs="1" />

<!-- Rules use to detect currently installed version of plugin - see Receiever Client SDK doc for more de
<xs:element name="detectCurrentVersionRulesList" type="detectCurrentVersionType" minOccurs="0" />

<!-- Other plugins on which this plugin depends at run time -->
<xs:element name="functionalDependencies" type="dependencyList" minOccurs="0" />

<!-- Other plugins on which this plugin depends at install time -->
<xs:element name="installationDependencies" type="dependencyList" minOccurs="0" />

<!-- Is this plugin a fully fledged, product level 'plugin' or a component
    associated with -->
<!-- a plugin that we  might want to represent at a different (lesser)
    level -->
<xs:element name="fullPlugin" type="xs:boolean" default="true" minOccurs="0" />

<!-- 1.1 Elements -->
<xs:element name="configuration" type="configType" minOccurs="0"  />

<!-- URL to README file (if available)  -->
<xs:element name="READMElocation" type="xs:anyURI" minOccurs="0" />

<!-- Sequence of Localised product names -->
<xs:element name="localisedProductNames" minOccurs="0">
 <xs:complexType>
  <xs:sequence>
   <xs:element minOccurs="1" maxOccurs="50" name="productName" type="localisedStringType" />
  </xs:sequence>
 </xs:complexType>
</xs:element>

<!-- Installer True Exit Code location. If set Receiver will look
    at a reg DWORD value of this path for the true exit code of the
    installer. Copes with MetaInstaller wrappers that throw away exit
    codes. HKLM paths only supported.
-->
<xs:element name="installerTrueExitCodePath" type="xs:string" minOccurs="0" />
```

```
<!-- Installer Failure Details Message location. If set, Receiver will
    look at a reg string value of this path for any extra detail on
    the cause of an installer exiting with the opaque 'Fatal
    Installer Error' code. HKLM paths only supported.
-->
<xs:element name="installerDetailExitMessagePath" type="xs:string" minOccurs="0"  />

<!-- pluginSupportsAdvancedMenuOptions: this plugin will mark some menu
    entries as being suitable for optional 'advanced' display. Option
    to enable such entries will only be shown in admin console if this
    is set.
-->
<xs:element name="pluginSupportsAdvancedMenuOptions" type="xs:boolean" default="false" minOccurs=

<!-- DeInstallPredecessor ranges: to meet the conditions like the Desktop Receiver upgrade failure case
    Specify version ranges over which upgrade will not work & deinstallation prior to applying the new v
    is required. If a detected version does not fall into one of the specified ranges then it is assumed th
    upgrade will work.
-->
<xs:element name="deinstallPredecessor" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="range" minOccurs="1" maxOccurs="100" />
        <xs:complexType>
          <xs:attribute name="min" type="xs:string" use="optional" />
          <xs:attribute name="max" type="xs:string" use="optional" />
        </xs:complexType>
      </xs:element
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- Running all the time: is it normal that a plug-in is active & able
    to report status (as say online / offline normally are) or is it
    OK that it may not be active all the time (eg ICA Engine) -->
<xs:element name="runningAllTheTime" type="xs:boolean" minOccurs="0" />

<!-- Incompatible Plugin: To cope with the case where multiple plugins
    perform the same role (eg PNA nd Anthem). Would stop them being
    deployed together in same Delivery, or at least generate a warning.
-->
<xs:element name="incompatiblePlugin" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="plugin" type="guid" minOccurs="1" maxOccurs="50" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

</xs:all>

<xs:attribute name="product" use="required" type="guid" />
<xs:attribute name="productName" use="required" type="xs:string" />

<!-- If this is true then this is part of the Citrix Receiver itself (both main client or UE component)-->
```

```
    <xs:attribute name="appReceiverComponent" type="xs:boolean" default="false" use="optional" />
  </xs:complexType>

<!-- Every plugin has a unique GUID. This is release invariant -->
<xs:simpleType name="guid">
  <xs:restriction base="xs:string" >

    <!-- This is the way it often appears in Windows.-->
    <xs:pattern value="[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}" />

    <!-- And this is a plain 32 character hex string.-->
    <xs:pattern value="[0-9a-fA-F]{32}" />
  </xs:restriction>
</xs:simpleType>

<!-- Version is normally a dotted string Major.Minor.BUild.Custom as applicable
<xs:simpleType name="versionType">
  <xs:restriction base="xs:token"/>
</xs:simpleType>

<!-- The relationship between the installer (action) and admin privilege  -->
<xs:simpleType name="installationAdminPrivsType">
  <xs:restriction base="xs:normalizedString">

    <!-- Installation requires admin privs and should fail if they are not
         available.-->
    <xs:enumeration value="demand" />
    <!-- Installation should be done with admin privs if available.
         If not available then proceed as non-admin user. -->
    <xs:enumeration value="prefer" />
    <!-- Install with non-privileged account.  Does not prevent
         installation if current user happens to be an admin. -->
    <xs:enumeration value="none" />
  </xs:restriction>
</xs:simpleType>

<!-- Possible Platforms for which this installer is valid (& platformType below) -->
<xs:simpleType name="platformTypeList" >
    <xs:list>
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="XP"/>
          <xs:enumeration value="XP64"/>
          <xs:enumeration value="Vista"/>
          <xs:enumeration value="Vista64"/>
          <xs:enumeration value="WS08"/>
          <xs:enumeration value="WS08_64"/>
          <xs:enumeration value="2K3"/
          <xs:enumeration value="2K364"/>
          <xs:enumeration value="Win7"/>
          <xs:enumeration value="Win764"/>
          <xs:enumeration value="WS08R2"/>
          <xs:enumeration value="WS08R2_64"/>
          <xs:enumeration value="Tiger"/>
          <xs:enumeration value="Leopard"/>
          <xs:enumeration value="SnowLeopard"/>
```

```
      </xs:restriction>
    </xs:simpleType>
  </xs:list>
</xs:simpleType>

<!-- Possible Languages for which this installer is valid (& platformType below)  -->
<xs:simpleType name="languageTypeList" >
   <xs:list itemType="xs:language" />
</xs:simpleType>

<!--  Details needed to perform an uninstall (& forms the basis of installs) -->
<xs:complexType name="arInstallType" >
 <xs:sequence minOccurs="1" maxOccurs="1">
    <xs:sequence>
   <!--  Basic structure of Command eg INSTALLERFILENAME $SILENTSWITCH $PARAMETERS -->
   <xs:element minOccurs="1" maxOccurs="50" name="command" type="localisedStringType" />
    </xs:sequence>
    <xs:sequence>
   <!--  Name=$param(Param GUI Name) pairs-->
   <xs:element minOccurs="0" maxOccurs="50" name="commandParameters" type="localisedStringType" />
    </xs:sequence>
    <xs:sequence>
   <!--  Switch needed to make the install run silently eg /qn-->
   <xs:element name="silentSwitch" type="xs:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
 </xs:sequence>
 <xs:attribute name="reboot" type="xs:boolean" use="optional"/>
</xs:complexType>

<!-- Type that supports Installs & Upgrades -->
<xs:complexType name="arUpdatingInstallType" >
 <xs:complexContent >
   <xs:extension base="arInstallType" >
    <xs:sequence>

      <!-- Does the Receiver need to start the plugin after install (we prefer the installer not to do so itself)
      <xs:element name="startAfterInstall" type="xs:boolean" minOccurs="0" />

      <!-- Information on how the plugin (auto) starts on login -->
      <xs:sequence minOccurs="0" maxOccurs="50">
        <xs:element name="autoStart" type="autoStartType" />
      </xs:sequence>

      <!--  Switch needed to make the install run with basic ui eg /qb -->
      <xs:element name="lessSilentSwitch" type="xs:string" minOccurs="0" />
    </xs:sequence>
    <!-- In some cases an update (or an 'installation' that effects an update)
        require any earlier versions to be removed beforehand.  I.e. they can't
        handle it themselves. -->
    <xs:attribute name="deinstallPredecessors" type="xs:boolean" default="false" use="optional"/>
    <!-- Set this if the installer can detect & handle a running instance --->
    <xs:attribute name="canUpgradeWhilePluginRunning" type="xs:boolean" default="false"/>
   </xs:extension>
 </xs:complexContent>
</xs:complexType>
<!-- If a plugin autostarts on login then it does so (on Windows!) via either a
```

```
    registry Run key or via a Startup menu entry  -->
<!-- Let the Receiver have that information so it can steal the info & use it to
    start the plugin at it's own convenience   -->
<!-- Receiver will look in both per user & machine wide locations so this entry
    should be relative to these roots  -->
<xs:complexType name="autoStartType" >
 <xs:sequence>
  <xs:choice minOccurs="1" maxOccurs="50" >
   <xs:element name="startupMenu" type="xs:string" />
   <xs:element name="startupRunKey" type="xs:string" />
  </xs:choice>
 </xs:sequence>
</xs:complexType>

<!-- The Receiver admin console will want to prompt the admin for common install
    time params & fill them in on the installer  -->
<!-- command lines. This can be achieved by adding something of the form
    PARAM=$(VarName) to the command line;  -->
<!-- then below pass that variable name & it's description. -->
<!-- e.g. Description="The Server URL for PNA" varname="PNAURL" -->
<xs:complexType name="commonInstallerOptGUIListType" >
 <xs:sequence>
  <xs:element name="config" type="commonInstallerOptGUIConfigEntry" minOccurs="1" maxOccurs="100" />
 </xs:sequence>
</xs:complexType>
<xs:complexType name="commonInstallerOptGUIConfigEntry" >
 <xs:sequence>
  <xs:element name="InstallerOpt" type="commonInstallerOptGUIType" minOccurs="1" maxOccurs="100" />
 </xs:sequence>
 <xs:attribute name="varname" type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="commonInstallerOptGUIType" >
 <xs:sequence>
  <xs:element name="description" type="xs:string"/>
 </xs:sequence>
 <xs:attribute name="language" type="xs:language" />
</xs:complexType>

<!-- Include a description of the plugins function & any information pertinent to
    its activity (eg installs kernel  -->
<!-- components, such that a user can used that information for informed consent
    to an install  -->
<xs:complexType name="pluginDescriptionListType" >
 <xs:sequence>
  <xs:element name="descriptions" type="pluginDescriptionType" minOccurs="1" maxOccurs="100" />
 </xs:sequence>
</xs:complexType>

<!-- Note that the description is required in all relevant languages  -->
<xs:complexType name="pluginDescriptionType" >
 <xs:sequence>
  <xs:element name="description" type="xs:string"/>
  <xs:element name="shortdescription" type="xs:string"/>
 </xs:sequence>
 <xs:attribute name="language" type="xs:language" use="required"/>
</xs:complexType>
```

```
<!-- GUID sequence for package & install dependencies -->
<xs:complexType name="dependencyList" >
  <xs:sequence>
    <xs:element name="dependency" type="dependencyType"  minOccurs="1" maxOccurs="100" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="dependencyType">
  <xs:attribute name="id" type="guid" use="required" />
</xs:complexType>

<!-- Rules use to detect currently installed version of plugin - see Receiver Client SDK doc for more details
<xs:complexType name="detectCurrentVersionType" >
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="100" name="detectRule">
     <xs:complexType>
       <xs:simpleContent>
         <xs:extension base="xs:string">
           <xs:attribute name="ignoreAfterVer" type="xs:string" use="optional" />
         </xs:extension>
       </xs:simpleContent>
     </xs:complexType>
   </xs:element>
  </xs:sequence>
</xs:complexType>

<!-- 1.1 config types. -->

<!-- Core type for L10N -->
<xs:complexType name="localisedStringType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute default="en" name="lang" type="xs:language" use="optional" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<!-- List of config elements -->
<xs:complexType name="configType">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="100" name="value" type="configElementType" />
    <xs:element name="introText" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element minOccurs="1" maxOccurs="50" name="intro" type="localisedStringType" />
        </xs:sequence>
       </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

<!-- Construct as choice so the entries can be in any order -->
<xs:complexType name="configElementType">
  <xs:choice minOccurs="1" maxOccurs="1">
    <xs:element name="string" type="valueStringType" />
    <xs:element name="bool" type="valueBoolType" />
```

```
    <xs:element name="list" type="valueListType" />
    <xs:element name="upload" type="valueFileUploadType" />
  </xs:choice>
  <xs:attribute name="name" type="xs:string" use="required" />
</xs:complexType>

<!-- Ensure enforcement types are correctly formed -->
<xs:simpleType name="enforceTypesSet">
  <xs:list>
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="http" />
        <xs:enumeration value="https" />
      </xs:restriction>
    </xs:simpleType>
  </xs:list>
</xs:simpleType>

<!-- Specifier for a single string entry
    Attr: required - data must be entered
    Attr: enforceType - http or https (URL types)
    Attr: passwordField - don't echo output
    Attr: defaultValue - start with this string, use it
    if no modification or field cleared. -->
<xs:complexType name="valueStringType">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="50" name="prompt" type="localisedStringType" />
  </xs:sequence>
  <xs:attribute name="required" type="xs:boolean" use="optional" default="false" />
  <xs:attribute name="enforceType" type="enforceTypesSet" use="optional" />
  <xs:attribute name="passwordField" type="xs:boolean" use="optional" />
  <xs:attribute name="defaultValue" type="xs:string" use="optional" />
  <xs:attribute name="example" type="xs:string" use="optional" />
</xs:complexType>

<!-- Specifier for a boolean config entry
     Attr initialValue: is the value 'true' by default or not -->
<xs:complexType name="valueBoolType">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="50" name="prompt" type="localisedStringType" />
  </xs:sequence>
  <xs:attribute name="initialValue" type="xs:boolean" use="optional" />
</xs:complexType>

<!-- Specifier for a list of config entries.
    Attr: required - data must be entered
    Attr: enforceType - http or https (URL types) -->
<xs:complexType name="valueListType">
  <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="50" name="prompt" type="localisedStringType" />
  </xs:sequence>
  <xs:attribute name="required" type="xs:boolean" use="optional" default="false" />
  <xs:attribute name="enforceType" type="enforceTypesSet" use="optional" />
  <xs:attribute name="example" type="xs:string" use="optional" />
</xs:complexType>
```

```
  <!-- Specifier for an 'advanced settings' file upload entry
     Attr: required - data must be entered -->
  <xs:complexType name="valueFileUploadType">
    <xs:sequence>
      <xs:element minOccurs="1" maxOccurs="50" name="prompt" type="localisedStringType" />
    </xs:sequence>
    <xs:attribute name="required" type="xs:boolean" use="optional" default="false" />
  </xs:complexType>

</xs:schema>
```

Attribute and Element Descriptions

New Elements in Release 1.1

The following elements are introduced in release 1.1.

- `version` - The main plug-in element has a new string attribute version. This is declared as optional for backward compatibility, however to ensure correct operation if you depend upon 1.1 features, you should declare this and set it to "1.1".

- `configuration` - A major Receiver 1.1 feature is the support of configuration updates that can be specified in the Administrator Console and passed down to the plug-in via an SDK entry callback. The config to be supported can be simple and specifiable as explicit entries to be shown in the admin console, or 'advanced' implying that a file will be uploadable to the admin console. The configuration section describes the UI entries that are required. It describes one or more elements, to be shown in the order specified in the metadata file and consisting of either strings, bools, lists or uploads. For each of these config values, they have a name to distinguish entries once passed to the client and an admin facing prompt description which can be repeated in localised forms as appropriate (distinguished by lang attributes).

- `string` entries - Simple string entry. Takes the following attributes.

  - `required` - If true then data must be entered in this field. Default:false.

  - `enforceType` - Currently the valid enforcement types are http or https which will enforce the appropriate URL forms.

  - `passwordField` - Don't echo output.

  - `defaultValue` - A string used to pre-populate the config GUI. If the admin leaves it untouched (or even if they clear the field for some reason), this value will be used. If the admin changes the value to a new one, the new value will be used.

  - `example` - The example text will be shown alongside the entry box.
- `bool` entries - Simple bool entry. Takes the following attribute.

  - `initialValue` - Default state of the bool.
- `list` entries - A repeated set of strings. Has the required, enforceType and example attributes as defined above.

- `upload` entries - A file upload box for advanced settings. Takes the required attribute. As well as the values, you can also include a introText element that contains text that describes the configuration section helping the admin understand how to fill out the fields.

An example configuration section follows:

```
<configuration>
  <value name="SampleBool">
    <bool initialValue="false">
```

```
      <prompt lang="en">True or false</prompt>
      <prompt lang="fr">Vrai ou faux</prompt>
    </bool>
  </value>
  <value name="SampleString">
    <string enforce="true" enforceType="http" example="http://showcasesample.citrite.net" >
      <prompt lang="ja">Please enter http URL</prompt>
    </string>
  </value>

  <value name="secondBool">
    <bool initialValue="true">
      <prompt lang="de">Damen oder Herren?</prompt>
      <prompt lang="zh-chs">Do you know this language?</prompt>
    </bool>
  </value>

  <value name="AdvancedSettingsFileUpload">
    <upload required="true">
      <prompt lang="en">Enter File Location</prompt>
      <prompt lang="it">Entri nella posizione della lima</prompt>
    </upload>
  </value>

  <value name="SampleList">
    <list  enforce="true" blankIsValid="true" enforceType="https">
      <prompt lang="en">Enter a set of https URLs</prompt>
      <prompt lang="fr">Entrez ensemble URL de https</prompt>
    </list>
  </value>

  <introText>
    <intro>Some config values for you to configure with
          useful configurations of your local configuration values</intro>
    <intro lang="fr">ce figuier est une fraude</intro>
   </introText>
</configuration>
```

Note that at the client end, this would result in data being passed to the client callback in the following form:

```
<configuration>
  <bool name="SampleBool">true</bool>
  <string name="SampleString">the string entry</string>
  <bool name="secondBool">true</bool>
  <upload name="AdvancedSettingsFileUpload">base 64 encoded file contents</upload>
  <list name="SampleList">
    <entry>list entry 1</entry>
    <entry>list entry 2</entry>
    <entry>list entry 3</entry>
  <list>
</configuration>
```

- `READMElocation` - Is a URL to a plug-in release README file (if available). The intention is that, if set, this will be made available as a link in the admin console.

- `installerTrueExitCodePath` - Installer Alternative Exit Code location. If set Receiver will lookat a reg DWORD value of this path for the true exit code of the installer. Copes with MetaInstaller wrappers that throw away exit codes. HKLM paths only supported. In V1.0 we looked at a hardwired location for this information (to support streaming installer). Flagging it in Metadata adds more control to this operation.

- `deinstallPredecessorRange` - DeInstallPredecessor ranges: to meet the conditions like the Desktop Receiver upgrade failure case. If the version of the currently installed plug-in is in this range then upgrade is invalid and the plug-in will be reinstalled (uninstall / install).

- `installerDetailExitMessagePath` - Installer Alternative Exit Message location. If set, Receiver will look at a reg string value of this path for any extra detail on the cause of an installer exiting with the opaque 'Fatal Installer Error' code. HKLM paths only supported. Examples here might be the Online App plugin bailing on detecting a prior Desktop Receiver installer or Streaming not installing on a FAT filesystem.

Example Metadata. Note that if min is ommitted then the range is defined as ver 0 to the max value. If max is omitted then the range is defined as all versions greater than that min value.

```
<deinstallPredecessor>
  <range min="10.9" max="11.0"></range>
  <range max="6.3"></range>
</deinstallPredecessor>
```

- `runningAllTheTime` - Running all the time: is it normal that a plug-in is active & able to report status (as say online / offline normally are) or is it OK that it may not be active all the time (eg Dazzle).

- `incompatiblePlugin` - Incompatible Plugin: To cope with the case where multiple plugins perform the same role (eg PNA and Anthem). Would stop them being deployed together in same Delivery, or at least generate a warning. This is a list of guid entries.

Localisation Additions

- `localisedProductNames` - In the (rare!) event of the plug-in product names being localised add a list of the localised names here.

- localisedInstall - In the event that a localised install implies a different command line, command line parameter set or start menu shortcut name, you can now add these overrides under their default (en) entries.

Example:

```
<autoInstall reboot="false">
  <command>msiexec /I $INSTALLERFILENAME $SILENTSWITCH $PARAMETERS</command>
  <command lang="fr">msiexec /I $INSTALLERFILENAME /leplumedematant</command>
```

```
  <commandParameters>ENABLE_SSON=Yes ALLOW_REBOOT=No SERVER_LOCATION=$ServerLoc REBOOT=Re
  <commandParameters lang="de">MeineHoseIstAbgereist=TRUE ALLOW_REBOOT=NO</commandParameters
  <silentSwitch>/qn</silentSwitch>
  <startAfterInstall>false</startAfterInstall>
  <autoStart>
     <startupMenu>Citrix XenApp.lnk</startupMenu>
     <startupMenu lang="fr">Citrix XenFrappe.lnk</startupMenu>
  </autoStart>
  <lessSilentSwitch>/qb</lessSilentSwitch>
 </autoInstall>
```

Elements in Release 1.0

The follow describes the metadata schema for release 1.0.

- `productName` attribute — Name (friendly name).
- version element — Version (major / minor / build / custom). Between 1 and 4 numeric entries, separated by dots.
- `Type` attribute — this is the GUID that identifies the particular plug-in. The metadata author should generate a GUID and then stick with it for future releases.
- `platforms` element — List of platforms that the plug-in supports (XP, XP64, Vista, Vista64, MacOS).
- `pluginLanguages` element — List of languages that the plug-in supports (standard locale encodings).
- `pluginDescriptions` element — User Informed Consent Information (potentially in several languages).
    - description of what the plug-in is used for and any relevant disclosure information (eg. Installs kernel components).
    - An abbreviated shortdescription used for summary display
- command lines for Install, Upgrade & Uninstall — The basic command line sets out the structure of installer command, parameters and switches to turn off (or down) the UI. To help Citrix Receiver select the relevant portions required for different install contexts the structure should include the following tokens:
    - `$INSTALLERFILENAME` — will be replaced by the installer name once downloaded to the client.
    - `$SILENTSWITCH` — placeholder to be replaced by a switch to suppress installer UI. All variants of the command line can take a silentswitch element (eg /qn for msiexec). Upgrade can also take a lessSilentswitch element which is used in case an upgrade needs to prompt the user to close down running apps (and/or the plug-in itself). If the fully silent form returns a failure, Citrix Receiver will then run the ëless silentí form of the upgrade.
    - `$PARAMETERS` — used to specify local environment specific parameters to the install.

      Where a parameter needs filling for the environment with a piece of configuration information (eg Server URL for PNAgent), Citrix Receiver can generate GUI within

the admin tool to prompt for that information. The installerOptGUI element of the metadata should support this by specifying:

- The Information Prompt (eg Server URL) and a "variable" key which corresponds to part of the unattended install line. As an example, the unattended install line may contain SERVERURL=$ServerLoc.
- There is then the related description section (supporting multiple languages) for that variable

As an example:

<installerOptGUI varname="ServerLoc">
<InstallerOpt language="en">
<description>Address of the WI server hosting XenApp PNA site </description>

Example of command line

msiexec /I $INSTALLERFILENAME $SILENTSWITCH $PARAMETERS

- `canUpgradeWhilePluginRunning` - Should the Upgrade not be suitable for running whilst a plug-in is active then set the `canUpgradeWhilePluginRunning` attribute on the upgrade section. If this is set, Citrix Receiver will defer the upgrade until the next login or boot.
- `deinstallPredecessors` - If this installer is not backwardly compatible with previous version for upgrades, set the `deinstallPredecessors` attribute. This will cause any previous instance of the plug-in to be uninstalled before the upgrade is applied rather than an upgrade run on the install.
- `reboot` - If the installer is likely to require a reboot after install then set the `reboot` attribute and suppress the reboot using whatever command flag is required (Citrix Receiver will coordinate all required reboots from installers).
- `InstallerFilename` - The `InstallerFilename` element should be set to the original filename envisioned when preparing the command line.
- `adminOptions` - The `adminOptions` element is set to one of `demand`, `prefer` or `none` depending on the level of Admin privilege required to install correctly.
  - `Demand` implies the installer always requires admin privilege.
  - `Prefer` that it has value without admin privilege, but perhaps with reduced functionality.
  - `None` that it is independent.
- `autoStartup` - The `autoStartup` element key (Registry or Start Menu relative). The `autoStartup` element is made available so that Citrix Receiver can (if required) take the details of the start mechanism and take control over the timing of this startup instead of allowing the normal explorer startup. This aids coordination with updates and any secure connection establishment. This element will contain either the name of the startup menu shortcut (.lnk) file or the valuename of the relevant registry 'Run' entry.
- URL of EULA (if available).

- Plug-in Dependencies: Provide the type GUID of any other plug-ins on which this plug-in has dependencies, either at install time (`installationDependencies`) or runtime (`functionalDependencies`).

- `detectCurrentVersionRulesList` — The `detectCurrentVersionRulesList` element provides information to help detect previous installations of plug-ins. As the installer GUIDs and names may not be consistent between releases, custom rules are required. These can take the following form (as required).

    - `REG` - path to registry value. If the value is a DWORD then the format is assumed to be Mmbb - 8 bits Major, 8 bits Minor, 16 bits Build. If the value is a string then it will be assumed to be numeric dot separated up to 4 parts (major, minor, build, custom). Supported prefixes for the Reg path are:HKLM, HKCU, HKCR

    - `EXE` - path to exe file where version can be extracted. The path can include environment variables: ProgramFiles, ProgramFiles(x86), WinDir, SystemRoot.

    - `UPGRADECODE` - packed GUID from installer *

    - `DISPLAYNAME` - display name of the package *

As many of these as are necessary can be specified.

- It helps Citrix Receiver operation if one of these rules are used as Uninstall Strings and actual Display names of the installed plug-ins can be detected at the same time.

  Examples:

  ICA client package

  UPGRADECODE:9B123F490B54521479D0EDD389BCACC1

  Streaming

  UPGRADECODE:CF106F6CA08399341B9EB788F1071D2D

  AG Standard

  REG:hklm\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Net6 Vpn\DisplayVersion
  DISPLAYNAME:Citrix Secure Access Client
  EXE:%programfiles%\Net6

  WANScaler

  UPGRADECODE:2E36AAD0884DAD11993000016C1E5903

- Version Upgrade / Reinstall list — for all previous detected versions of the plug-in (in min / mix pairs) is the current version able to upgrade or should the prior version be uninstalled first. If the latter, then what is the uninstall string to be used.

If an installer contains multiple plug-ins then there should be a section within the metadata file for each plug-in. Ideally the plug-ins will install separately.

Sample Metadata File

The following is a sample of a metadata file for the Receiver for Windows installer.

```
<?xml version="1.0"?>
<metadata
  xmlns="http://www.citrix.com/AppReceiver"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.citrix.com/AppReceiver MetaData.xsd">
<plugin product="11111111-1111-1111-1111-111111111111"
  productName="Citrix Receiver" appReceiverComponent="true" >
  <platforms>XP Vista</platforms>
  <version>1.0.0.6380</version>
  <installerFilename>AppReceiver.msi</installerFilename>
  <fullPlugin>true</fullPlugin>
  <!-- Install string & Attributes -->
  <autoInstall reboot="false">
    <command>msiexec /i $INSTALLERFILENAME $PARAMETERS $SILENTSWITCH</command>
    <commandParameters>BCTYPE=http BROADCASTER=$UpdateServer/appliance/services/applianceService
    <silentSwitch>/qn</silentSwitch>
    <lessSilentSwitch>/qb</lessSilentSwitch>
  </autoInstall>
  <!-- Uninstall string & Attributes -->
  <autoUninstall reboot="false">
    <command>MsiExec.exe /X{1C8DA3EE-A45F-464C-AD8F-EEF7BE4101FD} $SILENTSWITCH</command>
    <silentSwitch>/qn</silentSwitch>
  </autoUninstall>
  <adminOptions>demand</adminOptions>
  <!-- Informed Consent / Plugin Description  -->
  <pluginDescriptions>
    <descriptions language="en" >
      <description>Citrix Receiver version 1.0.0.6380 manages plugin installation and runtime orchestration fo
      </description>
      <shortdescription>Citrix Receiver version 1.0.0.6380- Manages your Citrix plugins automatically</shortde
    </descriptions>
  </pluginDescriptions>
  <!-- Admin console GUI generating information -->
  <installerOptGUI>
    <config varname="ServerLoc">
      <InstallerOpt language="en">
        <description>Address of the Broadcast Server</description>
      </InstallerOpt>
      <InstallerOpt language="fr">
        <description>Adresse du serveur de Broadcast Serveur </description>
          </InstallerOpt>
    </config>
  </installerOptGUI>
  <!-- List of Languages the plugin supports  -->
  <pluginLanguages>en</pluginLanguages>
  <!-- Rules use to detect currently installed version of plugin - see CR Client SDK doc for more details  -->
```

```
  <detectCurrentVersionRulesList>
    <detectRule>UPGRADECODE:508B3DEB038C58A4AA232045B1DADAB1</detectRule>
  </detectCurrentVersionRulesList>
  <installOnce>false</installOnce>
 </plugin>
</metadata>
```