Merchandising Server 2.1

Contents

Merchandising Server 2.1

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 Merchandising Server:

About Citrix Merchandising Server	Contains new features, known issues, and issues fixed in this release.
System Requirements for Merchandising Server 2.1	Contains system requirements, supported browsers, capacities, and plug-ins supported by Merchandising Server.
Install	Contains installation tasks.
Get Started	Contains an overview of Merchandising Server and the components with which it interacts.
Managing Merchandising Server 2.1	Contains information on configuring and maintaining Merchandising Server, as well as using auditing features.
Delivering Applications and Desktops from Merchandising Server	Contains information about deploying Citrix products with Merchandising Server, creating deliveries, and managing plug-ins.
Troubleshooting Merchandising Server 2.1	Contains information on troubleshooting.

About Citrix Merchandising Server

What's New

- Merchandising Server 2.1 facilitates an improved user experience by supporting plug-in authentication through Delivery Services. For information, search the eDocs Technologies node for "Delivery Services".

Known Issues

This section contains:

- Installation Issues
- General issues

Installation Issues

- To upgrade Receiver for Windows or Receiver for Mac, schedule a delivery.
- To upgrade plug-ins or to add new plug-ins to Merchandising Server, download plug-in and metadata files to Merchandising Server and create and schedule a delivery. You can also use **Plug-ins > Get New** page to obtain plug-ins that run in standalone mode. Although the 1.0 version plug-ins are compatible with Merchandising Server 2.1, it is recommended that you upgrade to benefit from new functionality.
- To upgrade to Merchandising Server 2.1, download the Merchandising Server 2.1 RPM file from Citrix.com and see Upgrading Merchandising Server. After you upgrade 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, see Installing SSL Certificates.
    - Recommended: Use the XenCenter console to set the Appliance Terminal password.

General Issues

- Domain names partially hidden on grid on Delivery Report page. If the browser window is too small, the domain names are not fully displayed in the Administrator Console. Workaround: Resize browser window [#2054].

- Creating a delivery rule based on LDAP Groups may fail. Because membership in LDAP groups is implicit, AD does not list all members; consequently, Merchandising Server does not get any user hits. Workaround: Use a different, explicitly populated group when creating the delivery rule; or if appropriate for all users, define the delivery with the **Default delivery** checkbox selected [#2898].

- Using Enter key instead of clicking Save generates error when attempting to create a rule based upon operating system. Creating a delivery rule with operating system as the criteria will generate an error page without Administrator Console UI controls. Workaround: Click browser's back button. Recreate rule (**Deliveries > Rules**, click **Create**). After making rule entries, click **Save** [#3314].

- When configuring a Delivery Services server for authentication, you may receive an inadequate error message: "Invalid delivery services URL". There are three possible causes for this error: (1) the Delivery Services URL cannot be reached, (2) the Delivery Services URL is not a valid Delivery Services URL, or (3) the Delivery Services URL does not have a valid certificate. In the last case, a valid Delivery Services certificate needs to be configured and a root certificate needs to be imported [#3623].

Fixed Issues

- Client logfile suggests there are connection errors when retrieval attempt is made when user is changing connection type (WiFi, inside firewall vs. VPN connection) [#3325].

- Receiver displays Microsoft .NET Framework "unhandled exception" error when Merchandising Server delivery completion text includes a URL without "http://" [#3359].

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.

System Requirements for Merchandising Server 2.1

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

Server Requirements

- Active Directory 2003 Service Pack 2 and above. Your corporate directory must be accessible through Active Directory.

One of the following server tools:

- Citrix XenServer™ 5.x with 8 GB of available disk space and 1 GB available RAM. You can download the XenServer free of charge from http://www.citrix.com.
- VMware (VMware vSphere 4.0, VMware Server 2.x, or ESX 3.5 and later).

Supported Browsers

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

- Internet Explorer 7
- Internet Explorer 8
- Firefox version 3.x

Merchandising Server supports the following browsers for Citrix Receiver Updater download pages:

- Internet Explorer 7
- Internet Explorer 8
- Firefox version 3.x
- Safari

Capacity

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 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.

Note: While you can configure Merchandising Server with less than 4 GB of RAM when importing it into XenCenter, we discourage using less than 4 GB except in small deployments or testing environments.

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 (XenServer); 4.2 GB/4 CPU (VMware)	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, as well as the operating systems supported by those plug-ins:

Plug-in	Compatible Operating Systems	Minimum Receiver Updater Version
Windows		
Microsoft Application Virtualization Desktop Client 4.5	Windows 7 (32- and 64-bit), Vista, XP and Professional (32-bit)	1.2
Acceleration plug-in 5.5.4.26	Windows XP Professional, Vista, Windows 7	2.0
Acceleration plug-in 5.5.2.24	Windows XP Professional, Vista (32-bit)	1.2

Citrix Receiver (Updater) for Windows 2.0.38007	Windows XP Professional SP3 (32- and 64-bit), Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows Server 2003 SP2 (32- and 64-bit), and Windows Server 2008 (32- and 64-bit)	2.0
Citrix Receiver for Windows 3.0	Windows 7 (32- and 64-bit - including Embedded Edition), Windows XP Professional (32- and 64-bit) , Windows XP Embedded, Windows Vista (32- and 64-bit), Windows Server 2003 and 2008 (32- and 64-bit - not supported with XenDesktop connections)	
Citrix Self-service plug-in 2.0.0.27090	Windows XP Professional (32-and 64-bit), Windows 7 (32- and 64-bit)	2.0
Dazzle plug-in 1.1.2.18299	Windows XP Professional (32- and 64-bit), Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit)	1.2
EasyCall 2.2.1.872	Windows XP Professional, Windows Server 2003, Windows Server 2008 (32- and 64-bit), Vista (32- and 64-bit),	1.1
EasyCall 3.0.1.985	Windows XP Professional, Windows Server 2003, Windows Server 2008 (32- and 64-bit), Windows Vista (32- and 64-bit), WIndows 7 (32- and 64-bit)	1.1
Offline plug-in 6.0.0.1304	Windows XP Professional, Vista, Windows Server 2003 and 2008 (32- and 64-bit), Windows 7	1.2
Online plug-in 12.1.0.30	Windows XP Professional (32- and 64-bit), Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows Server 2003 and 2008 (32- and 64-bit)	1.1
Profile Management plug-in 2.0.1.48 *****	Windows XP Professional, Vista, Windows Server 2003 and 2008 (32- and 64-bit)	1.1

Secure access plug-in 5.0.1	Windows XP Professional, Windows Vista (32- and 64-bit), Windows 7(32- and 64-bit)	2.0
Secure access plug-in 4.6.3.0800	Windows XP Professional, Windows Vista (32- and 64-bit), Windows 7(32- and 64-bit)	1.1
Secure access plug-in 4.6.2.0600	Windows XP Professional, Windows Vista (32- and 64-bit), Windows 7(32- and 64-bit)	1.1
Secure access plug-in 9.2.49.8	Windows XP Professional, Windows Vista, Windows 7	2.0
Secure access plug-in 9.2.49.8	Windows Vista (64-bit), Windows 7 (64-bit)	2.0
Secure access plug-in 9.2.45.7	Windows XP Professional, Windows Vista, Windows 7	1.1
Secure access plug-in 9.2.45.7	Windows Vista (64-bit), Windows 7 (64-bit)	1.1
Secure access plug-in 9.1.104.5	Windows XP Professional, Windows Vista, Windows 7	1.1
Secure access plug-in 9.1.104.5	Windows Vista (64-bit), Windows 7 (64-bit)	1.1
Secure access plug-in 9.1.103.9	Windows XP Professional, Windows Vista, Windows 7	1.1
Secure access plug-in 9.1.103.9	Windows Vista (64-bit), Windows 7 (64-bit)	1.1
Secure access plug-in 9.0.68.6	Windows XP Professional, Windows Vista	1.1
Service monitoring plug-in 5.3.4101	Windows XP Professional, Windows Vista, Windows 7	1.1
Service monitoring plug-in 5.3.4101	Windows XP Professional (64-bit), Windows Vista (64-bit), Windows 7 (64-bit)	1.1
Mac		
Citrix Receiver for Mac 2.0.169145	Mac OSX 10.5-10.6 (32- and 64-bit)	2.0
Communication plug-in for Mac 3.0.1.1077	Mac OSX 10.5-10.6 (32- and 64-bit)	1.1
Online plug-in 11.2.0.169077	Mac OSX 10.5, 10.6 (32- and 64-bit)	1.2
Secure access plug-in 2.0	Mac OSX 10.5, 10.6 (32- and 64-bit)	2.0
Secure access plug-in 1.2.0.58	Mac OSX 10.5, 10.6 (32- and 64-bit)	1.2

*****The Profile Management plug-in must be downloaded from http://mycitrix.com.

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.

Installing Merchandising Server 2.1

The five tasks listed below provide installation and quick configuration of Merchandising Server.

I. 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. You can import it into Citrix XenCenter or VMware (VMware vSphere 4.0, VMware Server 2.x, or ESX 3.5 and later).

Getting the Merchandising Server Software

1. Download the Merchandising Server virtual appliance from the Citrix support site. It is one of the downloads available under the Citrix Receiver product group.
   - For XenCenter: the image is in the form: citrix-merchandising-server-[*releaseNumber*].bz2
   - For vSphere: the image is in the form: citrix-merchandising-server-VMware[*releaseNumber*].ova
2. If needed, unpack the zip file using bz2, winzip, or another archive utility.

Importing the Virtual Appliance into XenCenter

Verify that you have a minimum of 20 GB of available hard disk space before proceeding.

1. Start Citrix XenCenter.
2. Select **File > Import VM**. The Import VM pop-up window displays.
   a. Click **Browse**, navigate to the .xva file, and click **Open**.
   b. Select **Exported VM** as the Import Type and then click **Next**.
   c. In the **Home** server screen of the wizard, select the XenServer instance where this VM should be imported and then click **Next**.
   d. In the **Storage** screen, select the XenServer where the storage repository resides and then click **Import**.

The import begins and the Network screen opens.

e. In the **Network** screen, select the appropriate network designation. If you only have one network, select **Network 0** and click **Next**.

f. In the **Finish** screen, clear the check box for **Start VM after Import** and then click **Finish**.

3. After the import process completes, right-click the VM and choose **Properties**.

a. Click the **CPU and Memory** tab, choose the amount of memory for the VM, and choose the number of VCPUs. Citrix recommends allocating at least 4 GB of memory and configuring 2 VCPUs.

b. Click **OK**.

4. Select the VM, and click the **Network** tab.

- Click the **Properties** button, select **Auto-generate**, and click **OK**.

5. Right-click the VM and choose **Start**.

6. Click the **Console** tab.

a. As needed, configure network settings.

b. Enter **9** to save the configuration.

c. When prompted, enter a new password for the virtual appliance.

The virtual appliance restarts.

Importing the Virtual Appliance into ESX using vSphere 4.0

Note: Unzipping and manually importing the .ova file is not supported.

1. Start vSphere Client (or other VMware solution equivalent, such as VMware vSphere 4.0, VMware Server 2.x, or ESX 3.5 and later).

2. Select or enter an IP address or host name.

3. Enter user name, password, and click **Login**.

4. Select **File > Deploy OVF Template**. The Deploy OVF Template pop-up appears.

a. Click **Browse** and navigate to the .ova file or enter a URL, and click **Next**.

b. Verify the OVF template details, and click **Next**.

c. Click **Accept** to accept the end user license agreement, and click **Next**.

d. Enter the name of the Merchandising Server virtual appliance you are creating in the inventory folder, and click **Next**.

e. Select a datastore, and click **Next**.

f. Review your deployment settings, and click **Finish**.

5. Select the Merchandising Server virtual machine name in the inventory.

6. In the Getting Started tab, click **Edit virtual machine settings**. A properties pop-up window appears. Citrix recommends allocating at least 4 GB of memory and configuring 2 VCPUs.

   a. In the Hardware tab, select **Memory**.

   b. Change the Memory Size to **4** GB.

   c. Select **CPUs**.

   d. Change the number of virtual processors to **2**.

   e. Click **OK**.

7. In the Getting Started tab, click **Power on the virtual machine**.

8. Click the **Console** tab.

   a. As needed, configure network settings.

   b. Enter **9** to save the configuration.

   c. When prompted, enter a new password for the virtual appliance.

   The virtual appliance restarts.

II. Configuring Your Administrator Users

1. Open a browser window and enter the Administrator Console URL. The URL must be in the form https://[*server_address*]/appliance, where *server_address* is your Merchandising Server host name or IP address.

2. Enter `root` for username, `C1trix321` for the Administrator Console 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.

III. Configuring the Administrator Console

1. Log on 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, 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 drop-down 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.

IV. 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 dialog box.

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. Type the rule **Name** and **Description**.
4. Select the rule type from the **Field** menu. Possible values are **Machine Name**, **User Domain Membership**, **Computer Domain Membership**, **Operating System**, **LDAP User**, and **LDAP Group, Machine Name**, **IP Address Range**.
   - If you select **LDAP User** or **LDAP Groups**, the screen displays the **Search** functionality.
   - If you select **User Domain Membership**, **Machine Domain Membership**, **Operating System**, or **IP Address Range**, select **Is** or **Is Not** for the **Operator** field and type the appropriate **Value** entry.
   - If you select **Machine Name**, select either **Begins With**, **Contains**, or **Is Exactly**, and type the appropriate **Value** entry.
5. Click **Save** to save your rule.

V. Creating Deliveries

To create a delivery

1. In the Administrator Console, select **Deliveries** > **Create / Edit**.
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 check boxes 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 check box 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.

Merchandising Server is now ready for your users to download Citrix Receiver. Once they have downloaded Receiver, it will automatically fetch your scheduled delivery and install plug-ins.

Getting Started with Merchandising Server 2.1

Easily “Merchandise” Virtual Apps and Desktops

With centralized management, Merchandising Server allows you to “merchandise” virtual applications and desktops across the entire organization. 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

Merchandising Server provides easy management, setup, and distribution of plug-ins to your Citrix Receiver end 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 desktop with a broad range of IT services, from applications to virtual desktops, anywhere in the world in 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

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

Once installed, the Receiver fetches the delivery information from Merchandising Server 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 Merchandising Server and Receiver to simplify desktop and application delivery. The Receiver infrastructure provides:

Seamless installation

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

Managed connections to delivery services

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

Simplified administration

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

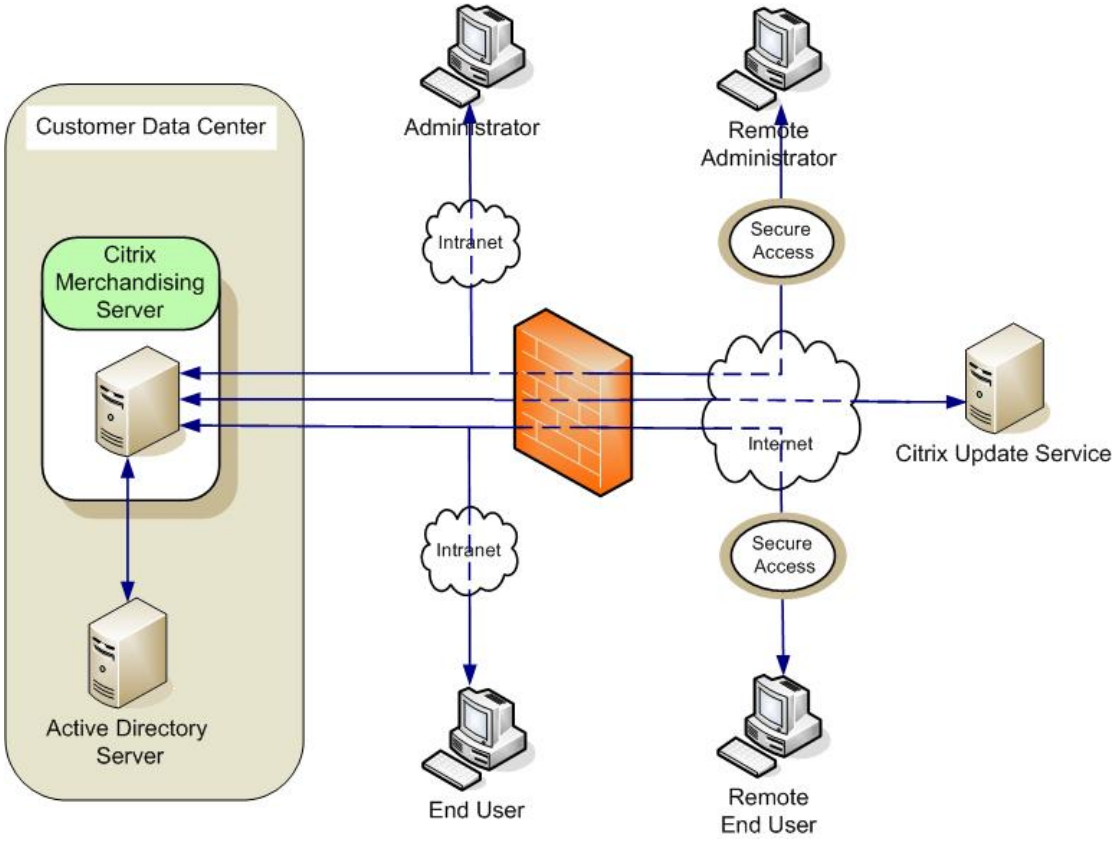
Simplified installation and upgrade

Import the Merchandising Server virtual appliance through Citrix XenServer (or supported VMware equivalent). Upgrades to Merchandising Server are imported directly through the Administrator Console.

Components

The Citrix Receiver end-to-end infrastructure consists of five components: Citrix Merchandising Server, the Administrator Console, Citrix Receiver, the Citrix Update Service, and the Software Development Kit.

Citrix Merchandising Server



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

Configure Merchandising Server to connect to:

- Microsoft Active Directory server

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

  Merchandising Server uses the imported user and group information to:

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

- Receiver

  The Receiver client software, installed on user devices, connects to Merchandising Server through HTTPS.

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

- Citrix Update Service

  Citrix posts new and updated plug-ins to the Citrix Update Service. For more information, see Getting Plug-ins for Merchandising Server.

Administrator Console

Use the Administrator Console to configure and update 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 Plug-in 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.

Use the console to configure the following features:

- Grant user permissions. See Granting Administrator and Auditor Permissions.
- Configure and sync Active Directory. See Connecting to Active Directory.
- Install SSL Certificates. See Installing SSL Certificates.
- Update Service polling frequency. See Defining Update Service Polling Frequency.
- Token expiration frequency. See Defining User Token Expiration Frequency.
- Default domain name. See Configuring the Default Domain Name.

- HTTPs redirection. See Disabling HTTPS Redirection.
- Support contact information. See Configuring Support Contact Information.
- Proxy server. See Configuring the Proxy Server
- Upgrade Merchandising Server. See Upgrading Merchandising Server.

Listed below are links to the task-based video instructions available within the Administrator Console.

Merchandising Server How To Videos
How To: Configure Active Directory Synchronization
How To: Create a Delivery Rule
How To: Download Plug-ins
How To: Modify Metadata Files for Plug-ins
How To: Schedule a Plug-in Delivery
How To: Set Up SSL Certificates
How To: Uninstall a Client Delivery
How To: View and Download Delivery Reports
How To: View and Download Logs

Citrix Receiver

Receiver for Windows can be pushed using your standard ESD process; otherwise, end-users can download and install Receiver for Windows or Receiver for Mac. From inside your firewall, Receiver can be downloaded from Merchandising Server's download page. From outside your firewall, you can post a bundled installer containing Receiver on a Web-hosted site.

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

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 that provide the functionality required to integrate applications with 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

User Authentication

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

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

Configure token expiry in the administrator console.

Secure Data Transfer

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

Managing Merchandising Server 2.1

Merchandising Server is administered through the Administrator Console.

- Configuring Merchandising Server
- Maintaining Merchandising Server
- Auditing the Administrative Actions

Configuring Merchandising Server

Use the administrator console to configure Merchandising Server:

1. Log on to the Administrator Console with root permissions.
2. Synchronize 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 a proxy server.

You are now ready to create deliveries.

Configuring your Administrator Account

To set up your administrator account:

1. Log on to the Administrator Console with root. See Logging on as Root.
2. Configure your corporate Active Directory. See Connecting to Active Directory.
3. Grant Administrator permission to your Active Directory user account. See 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 in the form https://[*serverAddress*]/appliance

   where *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 logon credentials are:

   - User name: root
   - Password: C1trix321

   Note: User logon credentials are case-sensitive.

   The Administrator Console opens at the Set Up page.

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

Resetting the Root Password

Citrix recommends 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, must include both alphabetic and numeric characters, and must contain at least one upper case character.
3. Click **Change Password**.

Connecting to Active Directory

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, 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, to complete the configuration tasks you must force a synchronization by using the **Save Changes and Sync** button. You can configure a backup Active Directory should the primary one be unavailable.

If you change the AD server configuration, 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. Click the tab of the desired Active Directory (**Primary** or **Backup**).
3. 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 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, Citrix recommends that you use an administrative connection, rather than an anonymous connection, from 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")

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

5. To have the directory synchronized with Merchandising Server immediately, click **Save Changes and Sync** . When the synchronization is complete, a message appears in the status bar of the console.

Granting Administrator and Auditor Permissions

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

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

Permission	Access	Grantee
Administrator	All Administrator 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 check box 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 administrators access to the Administrator Console now, or you can 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 off 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 off. The remaining configuration tasks are completed when you log back on with your administrator user account.

Logging on as an 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 in the form https://[*serverAddress*]/appliance

   where *serverAddress* is the Merchandising Server IP address or the host name.

2. Enter 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 *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.

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 the Default Domain Name.
- HTTP Redirection. Enable or disable automatic redirection to HTTPS; see Disabling HTTPS Redirection.
- Citrix Update Service Polling Frequency. The frequency for polling the Update Service for plug-in updates; see Defining Update Service Polling Frequency.
- Beacon Websites for Advanced Roaming; see Configuring Beacon Web Sites for Enhanced Roaming.
- Token Expiration Frequency. The expiration interval for the unique token used to authenticate users; see Defining User 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 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 end users, enter the http or https address here. The value should be in the form 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 your GoToAssist server in the form http(s)://www.gotoassist.acme.com.

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

3. Click **Save Changes**.

Configuring the Default Domain Name

You can improve the user experience by including your Active Directory domain name in the **Default Domain** field on the **Configurations > Options** page. If you configure this option, when your Receiver users log on, 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**.

Disabling HTTPS Redirection

By default, any attempt to access 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. Because each Merchandising Server uses a different SSL private key, it is 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 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**.

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

Defining Update Service Polling Frequency

The Polling Frequency settings in **Configurations > Options** allow you to specify how often 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** drop-down menu to define how often Merchandising Server checks for plug-in updates. The possible options are one **Week**, **2 Weeks**, and **4 Weeks**. By default, Merchandising Server checks the Citrix Update Service for updates daily at 12:01 a.m. With the non-default setting, Merchandising Server uses the time the non-default setting was saved as the new time to poll the Update Service.

3. Click **Save Changes**.

Defining User Token Expiration Frequency

The first time Receiver for Windows requests a delivery from Merchandising Server, the user enters their user credentials for access. As soon as the user is authenticated, a unique user token is generated and installed on the user's computer. Subsequent requests from Receiver to 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-authenticate before Receiver can access Merchandising Server for delivery updates. When the credentials have been authenticated again by Merchandising Server, a new token is generated and is effective 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** drop-down menu to define the interval for token expiration. The default value for token expiration is 6 months.
3. Click **Save Changes**.

Configuring Beacon Web Sites for Enhanced Roaming

If you configure beacon Web sites on the **Configurations > Options** page, Citrix Receiver can better determine the nature of the connection and avoid interrupting users with messages.

Two internal and two external beacon addresses are recommended. IP addresses can be used for **Internal Beacon Address** entries, but fully qualified domain names are recommended for beacon addresses.

To define beacon Web sites

1. Log on to the Administrator Console as administrator and select **Configurations > Options**.
2. Enter an IP address or Web site URL in the **Internal Beacon Address** field and select **Domain Controller** or **HTTP** from the pull-down list. This address should be accessible by computers when connected inside the corporate firewall.
3. Enter a Web site URL in the **External Beacon Address** field and select **HTTP** from the pull-down list. These entries should be sites that are generally accessible anywhere over the Internet (for example, through Google or Yahoo).
4. To add additional beacon addresses, click **Click here to add another address**.
5. Click **Save Changes**.

Configuring Tokens for Anonymous Deliveries

Installing Citrix Receiver with a system token enables Receiver to fully configure plug-ins without users needing to authenticate when connecting to Merchandising Server.

Use the Citrix Receiver Packager to create a bundled installer containing Citrix Receiver and the system token. Host the bundled installer on a download page. For information, search the eDocs Receiver and Plug-ins node for "external download". Users who download Receiver from the Merchandising Server download page will not be configured with a system token.

Alternatively, you can also use the **Token Value** when installing Receiver for Windows with ESD tools. For information, search the eDocs Receivers and Plug-ins node for "Pushing Citrix Receiver".

Important: The system token is a special character string created by Merchandising Server. Changing the system token after it has been issued and installed with Receiver will prevent Receiver from logging on to Merchandising Server. Receiver will need to be reinstalled with the new token value to restore anonymous deliveries.

To create and use a token for anonymous deliveries

1. Log on to the Administrator Console as administrator and select **Configurations > Authentication**.
2. Click **Create Token**.
3. Use this token value when creating a bundled installer with Citrix Receiver and Citrix Access Gateway. You can also use the **Token Value** when installing Receiver for Windows with ESD tools.

Sharing a Token Value between Merchandising Servers

If you are configuring a second Merchandising Server, you can use the same system token for deliveries from that Merchandising Server by copying the token.

To copy a token for anonymous deliveries from one Merchandising Server to another

1. Log on to the Administrator Console as administrator and select **Configurations > Authentication**.
2. Copy the **Token Value** field value.

3. Log on to the alternate Merchandising Server Administrator Console and select **Configurations > Authentication**.

4. Click **Generate Token**.

5. Click the **Enter Token Value** check box, paste the token value into the field, and click **Create Token**.

Configuring Authentication through Delivery Services

Configuring authentication through Delivery Services reduces the need of Receiver for Windows users to authenticate when using the Self-service plug-in, the Online plug-in, the Offline plug-in, or the Secure Access plug-in.

To configure authentication through Delivery Services

1. Log on to the Administrator Console as administrator and select **Configurations > Authentication**.
2. Enter the URL of the **Delivery Services Server**.
3. Click **Save**.
4. Depending upon how your Delivery Services Server is configured, you may need to import a root certificate. (See Importing Root Certificates.)

Installing SSL Certificates

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

Only 1024-bit SSL certificates are supported by Merchandising Server. 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 (CA). 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 from a Certificate Authority and Creating a Signing Request for Microsoft Certificate Services for instructions on obtaining a certificate using Microsoft Certificate Services. See Importing Root Certificates for information about importing certificates from a Delivery Services server.

Generating a Self-signed SSL Certificate

A self-signed certificate is already installed on 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** drop-down menu.

3. In **Common Name**, enter the Merchandising Server host name or IP address . The value you enter in **Common Name** must be the same value you use to access 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.

Creating a Certificate Signing Request

To obtain an SSL certificate from a certificate authority (CA), 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. 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** drop-down menu to create the certificate signing request.

3. In **Common Name**, enter the Merchandising Server host name or IP address 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.

Importing Certificates from a Certificate Authority

To replace the temporary certificate, you must import a server certificate into 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** drop-down menu.

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

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

Merchandising Server restarts.

Importing Root Certificates

If you are using Delivery Services for authentication, you may need to import a root certificate.

1. Log on to the Administrator Console as administrator and select **Configurations** > **SSL Certificate Management**.
2. Select **Import root certificate** from the **Select an action** drop-down menu.
3. Click **Browse** to locate the root certificate file.
4. Enter a name in the **Alias** field to ease certificate identification.
5. Click **Submit** to upload the certificate.
6. Click **Confirm**. Merchandising Server restarts.

Creating a Signing Request for Microsoft Certificate Services

The following describes a generic process for requesting and downloading a 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.

Installing Local or Customized Certificates on Client Devices

Communications between Receiver and 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 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 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** check box. 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** check box. (Note: If user authentication is required, users need https access only.) The User Name and Password fields are displayed.
5. Enter the user name and password for proxy server authentication.
6. Click **Save Changes**.

Maintaining Merchandising Server

Use the XenCenter console in XenServer (or supported VWware equivalent) to perform tasks on Merchandising Server such as:.

- Shuting down and restarting
- Backing up

Other Merchandisng Server maintenance tasks include:

- Changing Server Network Settings
- Ensuring Merchandising Server High Availability
- Upgrading Merchandising Server

Changing Server Network Settings

XenCenter (and the supported VMware equivalent) contain the functionality for changing your Merchandising Server IP address, the host name, netmask, gateway, and domain name system settings. They also contain the diagnostic capabilities to ping a server, traceroute, and set the root password. If you are not familiar with using XenCenter, refer to Installing Merchandising Server 2.1.

Note: 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 restarts after saving the changes.
5. Enter 8 to troubleshoot the server with this utility. If you have not saved your changes, the changes are 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 update XenTools: selecting this option will cause the system to restart. This option is not available on supported VMware equivalent server tools.
    d. Enter 4 to open a terminal session.
    e. 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 Merchandising Server.

Ensuring Merchandising Server High Availability

Merchandising Server may be deployed as a single server. If Merchandising 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 Merchandising Server is restored.

If you require higher availability, the simplest and easiest method is to use the capabilities provided by XenServer or the supported VMware equivalent. 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 Merchandising 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 Merchandising Server

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

To upgrade your Merchandising Server

1. Download the Merchandising Server upgrade file from 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 **OK** in the confirmation popup to continue with the upgrade. While the upgrade file is copied to the server, the Administrator Console Upgrade Server page displays a spinning icon and the page is grayed out.

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

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

Auditing Administrative Actions

A 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 administrator 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 to two features within the Administrator Console: viewing the audit trail and granting auditor permissions. Only a user logged on 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 in the form http://[*serverAddress*]/appliance where *serverAddress* is the Merchandising Server IP address or the host name.

2. Enter your user name and password, then click **Log on**.

   - User name: Your Active Directory user account name. Enter the user name in the form *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 trailand grant users 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 on to the Administrator Console with auditor permissions.
2. Select **Reporting and Logging > View Audit Trail**.
3. Enter the dates that define the period 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**.

Delivering Applications and Desktops from Merchandising Server

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

- Online Applications (For information, search the eDocs Receiver and Plug-ins node for "Using the Merchandising Server and Citrix Receiver to Deploy the Plug-ins".)
- Streaming applications
- Microsoft Application Virtualization (App-V) plug-in
- Access Gateway
- Branch Repeater Acceleration
- Self-service plug-in (For information, search the eDocs Receiver and Plug-ins node for "Deploying and Removing the Citrix Self-service Plug-in for Windows".)
- Edgesight monitoring
- Profile management
- Deploying Receiver on XenDesktop images
- Deploying Receiver on XenApp published desktops
- Using other VPNs with Citrix Receiver

For information on how to install Receiver (Updater) on Windows or Mac desktops, see the eDocs Receiver and Plug-ins node. The Receiver (Updater) topics include "System and Compatibility Requirements" for the plug-ins supported in Merchandising Server and Receiver. See the Citrix Ready Product Catalog for third party products to use with Citrix Receiver.

Deploying Streaming Applications with Receiver

For information about application streaming, search the eDocs XenApp node for the following topics:

"Application Streaming"	Contains an overview of application streaming.
"Components for Application Streaming"	Contains information on the components of application streaming.
"Installing the Offline Plug-in"	Contains information on installing the offline plug-in.

Deploying the Microsoft Application Virtualization (APP-V) Plug-in with Receiver

To deliver the App-V client with Citrix Merchandising Server and Citrix Receiver Updater

1. In the Merchandising Server Administrator Console, navigate to the **Plug-in** > **Upload** page.

2. To upload the App-V_Reg plug-in components:

    a. For the **Metadata File**, click **Browse** to navigate to the unzipped location of **AppVReg_MetaData.xml**.

    b. For the **Plug-in File**, click **Browse** to navigate to the unzipped location of **AppVReg.msi**.

    c. Click **Upload**.
3. To upload the App-V client components:

    a. For the **Metadata File**, click **Browse** to where you downloaded **App-V_MetaData.xml**.

    b. For the **Plug-in File**, click **Browse** to navigate to the location of the Microsoft Application Virtualization Desktop Client installer, **setup.exe**.

    c. Click **Upload**.
4. Configure a delivery to communicate with your App-V server.

An overview of the entire Plug-in upload and delivery process when using Merchandising Server 1.0 can be viewed at http://www.citrix.com/tv/#videos/773.

If users have the Self-service Plug-in, they can add published App-V sequences as they normally add applications.

The Microsoft App-V Integration Kit must be downloaded from citrix.com/downloads. For additional information, search the eDocs XenApp node for "Publishing App-V sequences in XenApp".

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: www.citrix.com

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 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.

You can also use 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.

Deploying Branch Repeater Acceleration

The 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 it 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 plug-in because 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 of 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:

- Leverage 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 none of these solutions meets 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.

Installing Receiver on Private and Shared XenDesktop Images

Where you publish XenDesktop images and want to use other Citrix plug-ins, Receiver can improve the overall user experience and help keep desktops up-to-date as it does on physical desktops.

Citrix Receiver for Windows can be deployed on private or shared desktop images. For private desktops, the desktop configuration and updates persist between sessions. In this scenario it is a remote desktop and Receiver performs the same services as on a normal local desktop. In a shared (or pooled) desktop image, the desktop image is reloaded each time the user logs on, essentially discarding any changes made by Receiver and returning the desktop back to its original state.

For additional information about private and shared desktops, see the topics about desktop groups in the eDocs XenDesktop node.

Private XenDesktop Images

With a private desktop image, updates to Receiver are triggered in the same manner as they are with other client devices.

To install and set up Receiver on a private XenDesktop image

1. Log on to the master shared image with administrator permissions.
2. Download Citrix Receiver for Windows from the Receiver Download page hosted on the Merchandising Server, following the process described in your Citrix Merchandising Server Administrator's Guide. The URL is: https://[*merchandisingServer*], where [*merchandisingServer*] is the hostname or IP address of your Merchandising Server.
3. Wait for Receiver to install the updates. When the private user accesses XenDesktop, Receiver will start up and provide the applications as configured. Updates are performed automatically or as requested by the user.

Shared XenDesktop Images

On shared desktops (where the whole desktop image is fresh each time), you can use Receiver as an image preparation tool. Initially, Receiver is installed on the base image and it sets up the plug-ins. After you disable the update mode, the base image post plug-in install is used. When new plug-ins are deployed, enable the update mode in the base image so Receiver can install the updates, then disable the update mode and create a new image.

To manually install and set up Citrix Receiver for Windows on a shared XenDesktop image

1. Create the Windows base image.
2. Install the online plug-in by running CitrixOnlinePluginFull.exe.
3. Install the offline plug-in by running CitrixOfflinePlugin.exe.
4. Pre-cache and pre-extract all offline applications using the radedeploy utility (see http://support.citrix.com/article/ctx115137).
5. Install Receiver using the following: `msiexec.exe /I Receiver.msi ALLUSERS=1`
6. Install Dazzle using the following: `msiexec.exe /I Dazzle.msi STORE1="`*`Storename`*`;https://`*`XMLServerURL`*`/Citrix/PNAgent/config.xml;ON;`*`Store Description`*`" ALLOWADDSTORE=A ALLOWSAVEPWD=A ALLUSERS=1`

To use Merchandising Server to install and set up Citrix Receiver for Windows on a shared XenDesktop image

The procedure below disables automatic updates.

Caution: Editing the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Log on to the master shared image with administrator permissions.
2. Download Citrix Receiver for Windows from the Receiver Download page hosted on Merchandising Server. The URL is: https://[*merchandisingServer*], where [*merchandising Server*] is the hostname or IP address of your Merchandising Server.
3. Wait for Receiver to install updates.
4. When updates are completed, add the `-nopluginupdates` option to the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CitrixReceiver` registry:
   a. Go to **Start** > **Run**, enter `regedit`, and click **OK**.
   b. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and click **CitrixReceiver** in the name column. The **Edit String** popup displays a **Value data** entry that is similar to `"C:\Program Files\Citrix\Receiver\Receiver.exe" -autoupdate -BCType:http`.
   c. Add `-nopluginupdates` at the end of the entry in the **Value data** field.

d. Click **OK** to apply the changes.

e. Exit the registry.

The next time a user logs onto the shared desktop all applications and plug-ins will be available and the user will not be annoyed by repeated updates.

Deploying Receiver on XenApp Published Desktops

When publishing XenApp desktops, you can install Citrix Receiver and plug-ins to improve the overall user experience. Because updates to XenApp published desktops may not be available to users, you can manually trigger updates.

To install Citrix Receiver on a XenApp Published Desktop

1. Publish the server desktop. For information, search the eDocs XenApp node for "Publishing Resources".
2. Log on to the XenApp published desktop with administrator permissions.
3. Download Citrix Receiver for Windows from the Receiver Download page hosted on the Merchandising Server. For information, search the eDocs Receiver and Plug-ins node for "To Install Receiver for Windows".

Receiver is installed but is not yet configured to retrieve updates from the Merchandising Server.

1. To trigger an update, right-click the Citrix Receiver icon in the notification area and select **Exit**.
2. Open a command prompt window and start Citrix Receiver in the updating mode by typing the following command:

   ```
   C:\Program Files\Citrix\Receiver\Receiver.exe -autoupdate
   -allowadminTSupdates
   ```

3. Once the updates have been installed, exit Receiver by right-clicking the Receiver icon in the notification area and selecting **Exit**.

The updates are now available for your XenApp published desktop users.

Using other VPNs with Citrix Receiver

Citrix Receiver is fully integrated with Access Gateway Enterprise Edition and automatically detects 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.

Getting Plug-ins for Merchandising Server

There are two methods of getting plug-ins into Merchandising Server. You can download plug-ins directly into Merchandising Server, or you can upload plug-ins you have downloaded to a file location from Citrix.com.

Downloading Plug-ins into Merchandising Server

This method gets plug-ins from the Citrix Update Service.

1. In the Administrator Console, select **Plug-ins > Get-New**. The Administrator Console displays the plug-ins compatible with the current version of Merchandising Server.

2. Select the plug-in from the listing and click **Download to Server** or click **Download All 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**.

Uploading Plug-ins into Merchandising Server

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

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 are 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 **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 drop-down 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 the user name check box from the search results. c. Click **Add**.
User Domain membership	a. Select the Operator from the drop-down 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 the group name checkbox from the search results. c. Click **Add**.

Operating System	a. Select the Operator from the drop-down list. The possible options are **Is** and **Is Not**. b. Select the operating system value from the drop-down menu.
IP Address Range	a. Select the Operator from the drop-down 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 drop-down 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 drop-down 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.

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 belongs 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 belong 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 use 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 Getting Plug-ins for Merchandising Server.

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

- General. Define a delivery name, a description, and server polling frequency for delivery updates. See Defining Installation Parameters.
- Plug-ins. Select the 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 do not 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 the plug-in's 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 or you can create a new delivery.

To create a new delivery

1. Select **Deliveries > Create / Edit** 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.
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 check box designates the delivery as the default and as such, no rules can be defined. Users receive the default delivery if they are not scheduled to receive any other delivery. Only one delivery can be designated as the default delivery.
Silent Install	If this is enabled, Receiver does not give the end user the opportunity to cancel or pause any part of the installation.
User Help URL	The URL for the user help system for 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 Receiver's interval for polling Merchandising Server for delivery updates.
Secure connectivity	One of two options is available: always provide a secure connection or ask the user permission before providing a secure connection. This feature either allows the user to define connectivity through the Receiver Preferences or grays out the preference and makes it configurable only by the administrator.
Completion text	Enter the message you want displayed to the end user when the Receiver installation completes. The following table contains recommended text for the various access methods. If you enter a URL in this field, the URL must include "http://" or "https://".

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].
Self-service plug-in	Select **Open** on the Receiver menu.

* 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 plug-in, 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 drop-down list at the top-right of the page. The possible options are **Install** and **Uninstall**.
4. Select the check box for each plug-in 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 you have added to your delivery. For most plug-ins, the **Configuration** tab contains fields to define each plug-in's server information.

To define the configuration parameters for your plug-ins

1. Click the **Configuration** tab from within a delivery creation or editing process.
    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 the offline plug-in, enter the XenApp server IP address, FQDN, or Web server address.
    d. If you are delivering the 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 logon 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 appears.
    d. Select one or more of the rule check boxes 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 appears. 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 is displayed in the **Advanced** page and the **Add Rule to Delivery** page again appears. Add the appropriate rule(s).
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

Note: If you click **Cancel** on this page, none of your changes is saved. If you are in the process of editing an existing delivery, canceling results 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.

1. Click the **Schedule** tab from within a delivery creation or editing process.

2. In **Schedule Delivery Start Time**, select **Deliver Now** or **Deliver 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.

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

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 the 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 redeliver the latest delivery or uninstall the Receiver and the plug-ins installed with this delivery. For more information on redelivery and uninstall, see Creating Deliveries.

To view a 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 check box 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** drop-down list. The list of all users that have received a delivery is displayed.

    b. Select the check box 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 Receiver and its Plug-ins.

Updating Plug-ins in a Delivery

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

Note: If users are inside a firewall, Merchandising Server updates the secure access plug-in. Remote users are updated the first time they encounter 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 Getting Plug-ins for Merchandising Server.
2. To add the plug-in update to an existing delivery:
    a. Select the delivery check box in the delivery listing at **Deliveries > Create / Edit**.
    b. Click on the **Plug-ins** tab.
    c. Select the check box of the plug-in you want to remove.
    d. Click **Remove**. 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.

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 reinstalls 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 **Associated Name** in the **Search By** drop-down list. The list of user names is displayed. You can also search by **Machine Name**. **Domain** name, or **IP Address.**
3. Select the check box 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 reinstalled on this user's device.

Removing Plug-in Files from Merchandising Server

You remove plug-ins from 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 along with a listing of the active deliveries that contain this plug-in.

To remove plug-in files from Merchandising Server:

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

Removing 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 because they are uninstalled during this process.

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

Modifying Plug-in Metadata

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 do not require modification. However, if you wish to edit the metadata files, the metadata schema and a sample metadata file are provided on theCitrix Community Receiver Metadata Web page.

Troubleshooting Merchandising Server 2.1

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

- Triggering Retrieval of Client Log.
- Enabling System Debug Logging.
- Enabling End User Debug Logging.
- Viewing Debug Logs.
- Viewing Client Logs.
- Changing Merchandising Server in Citrix Receiver.

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 Downloading the Debug Log 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 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 check box 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 behalf of the specified end user are continually posted to the `appliance.log` file on the server until you disable end user debugging.

Triggering the Retrieval 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 a client device:

1. In the Administrator Console, select **Reporting and Logging > Enable / Disable Logging**.
2. Select the check box 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 check box for user name.
3. Click **Trigger Client Log Retrieval**.
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 Merchandising Server.

Viewing Client Log Files

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

To view the log files retrieved from a client device

1. In the Administrator Console, click **Reporting and Logging > View Log Files**.
2. Select the check box 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.

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 check boxes for files you want to download from the **Download Server Logs** popup.
4. Click **Download Logs**.
5. Click **Save File**, provide the location for the file, and click **Save**. The compressed zip file is saved to the location you entered. Decompress the file for viewing.

Changing Merchandising Server in Citrix Receiver

Changing Merchandising Server in Receiver for Windows

In the event a user downloaded Receiver from the incorrect download page, you can change the Merchandising Server associated with Citrix Receiver.

1. Click **Start > Control Panel** and open **Citrix Receiver.**
2. Change the *ServerAddress* portion of the path (`https://[ServerAddress]/appliance/services/applianceService/`).
3. Save your changes and close the window.

Changing Merchandising Server in Receiver for Mac

1. Open *`Macintosh HD`*`/Library/Application Support/Citrix/Receiver.cfg`
2. Change the *ServerAddress* portion of the path (`https://[ServerAddress]/appliance/services/applianceService/`).
3. Save your changes and close the window.