CHAPTER 1

Getting Started With AUS

Auto Update Server (AUS) is a web-based interface for upgrading device configuration files and software images on PIX firewalls and Adaptive Security Appliances (ASA) that use the auto update feature.

Security appliances that use the auto update feature connect to AUS periodically to upgrade device configuration files and to pass device and status information.

Note For more information on how to install AUS and other related server applications, see the *Installation Guide for Cisco Security Manager*.

The following topics help you get started with using AUS:

Overview of Auto Update Server

The Auto Update Server (AUS), a component of the Cisco Security Management Suite, is a tool for upgrading PIX firewall software images, ASA software images, PIX Device Manager (PDM) images, Adaptive Security Device Manager (ASDM) images, and PIX firewall and ASA configuration files.

Although you can update software and ASDM/PDM images for any ASA or PIX device, to update configuration files you must use the Security Manager application to create and deploy the configurations.

You can use AUS with any ASA or PIX device and operating system version supported by Security Manager (for a list of devices, see *Supported Devices and Software Versions for Cisco Security Manager* on Cisco.com). However, the device must be running in single-context mode; you cannot use AUS with devices that host security contexts. You can manage up to 1000 devices with a single AUS server.

You can use AUS for updating devices with static IP addresses or for devices that obtain IP addresses dynamically through DHCP. You must use AUS to update configurations for devices that use DHCP. A network management server cannot directly initiate communication to devices that acquire their

interface addresses using DHCP because their IP addresses are not known ahead of time. Furthermore, these devices might not be running, or they might be behind firewalls and NAT boundaries when the management system needs to make changes.

Whether a device uses static or dynamic IP addresses, if you configure them to use the auto update feature, they connect to AUS at periodic intervals. The device gives AUS its current state and device information. AUS responds to the device by providing a list of versions for the software images and configuration files that the device should be running. The device compares the file versions with the versions it is running. If the versions are different, the device downloads the new versions from the URLs provided by AUS. After the device is up-to-date with the new file versions, it sends AUS its state and device information again.

You can also use AUS to update a device configuration or software image on demand instead of waiting for the device to contact the server. This ability is useful if you are updating the device to respond to an immediate threat.

The following topics provide more information about AUS:

- Deploying AUS Behind a NAT Boundary, page 1-2
- Adding Devices to AUS, page 1-3
- Backing Up and Recovering the AUS Database, page 1-3
- Understanding User Roles and Permissions, page 1-3

Deploying AUS Behind a NAT Boundary

If you want to deploy AUS behind a NAT boundary in either the Enterprise network or in the Enterprise DMZ, then the PIX firewalls and ASA devices being managed by AUS must all be on the same side of the NAT boundary. For example, you can deploy AUS in the DMZ behind a NAT boundary and manage devices that were deployed only on the Internet; however, you cannot deploy AUS in the DMZ behind a NAT boundary with some devices using private addresses on the inside of the boundary and some outside on the Internet.

If AUS is behind a NAT boundary, the address that the device uses to contact AUS is most likely different from the actual IP address of the AUS server. Therefore, you must specify the IP address that devices on the public side of the NAT boundary must use to access AUS. For example, a typical setup could look like the following:

AUS has a public address 209.165.201.1 that corresponds to an internal AUS address of 192.168.0.1

Because all the devices connect to the public address, you must configure the IP address in the NAT Settings page to 209.165.201.1. If no NAT boundary is involved, you can leave the default, which is the IP address of the local machine.

Note All devices must be on one side of the NAT boundary. For configurations with devices on both sides of the NAT boundary, two AUS servers are required.

Step 1 Select **Admin > NAT Settings**. The NAT Settings page appears.

Step 2 Select **NAT Address** and enter the IP address that translates to the server's IP address.

(If you are not using NAT, or you later stop using NAT, select **Actual Host Address**.)

Step 3 Click **OK** to apply your changes.

Adding Devices to AUS

When you use Security Manager to deploy configurations to a device through AUS, the device is automatically added to the AUS inventory after the device successfully contacts AUS and retrieves the configuration. This is the normal method for adding devices.

However, you can manually add devices if you want to use AUS for software and ASDM/PDM image updates for devices not managed by Security Manager, or for troubleshooting purposes. For more information, see Adding a Device Directly to AUS.

When adding a device to AUS, Security Manager includes the enable password and the HTTP username and password (defined as the TACACS+ username and password in AUS). These credentials are used if you perform an Update Now action (an immediate auto update) to direct a device to immediately update its configuration. For more information, see Requesting an Immediate Auto Update, page 2-6.

Backing Up and Recovering the AUS Database

To back up and restore the AUS database, you use the standard Security Manager/CiscoWorks backup and restore utilities. You can use a database backup when installing AUS on a new server to restore the database.

For information on using these tools, see the *User Guide for Cisco Security Manager*.

Understanding User Roles and Permissions

AUS supports two methods for authentication: CiscoWorks Server or Cisco Secure Access Control Server (ACS). When you install AUS and Security Manager, you can configure which of these methods to use. For more information, see Appendix B, "User Roles and Permissions."

Logging In to and Exiting Auto Update Server

You log into the Auto Update Server using the Cisco Security Management Suite home page. You can also use the home page to install the Security Manager client or to access Common Services, Performance Manager, RME, and other software installed into Common Services.

Procedure

Step 1 In your web browser, open one of these URLs, where *AUSServer* is the name of the computer where AUS is installed. Click **Yes** on any Security Alert windows.

- If you are not using SSL, open http://*AUSServer*:1741
- If you are using SSL, open https://*AUSServer*:443

The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser. For information on configuring the browser to run Security Manager, see *Installation Guide for Cisco Security Manager*.

Note We recommend that you use SSL for proper security. You also need to enable the browser-security mode on the machine that runs AUS for proper communication to take place between Security Manager and AUS. For more information, see Setting Up Browser-Server Security, page 1-4

Step 2 Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username **admin** and the password defined during product installation.

Step 3 When you log in, you are shown the Cisco Security Management Suite home page. The home page lists the suite applications installed on the server. You can access at least the following features on the server running AUS. Other features might be available depending on how you installed the product.

- Auto Update Server—Click this item to open the Auto Update Server interface.
- Server Administration—Click this item to open the CiscoWorks Common Services Server page. CiscoWorks Common Services is the foundation software that manages the server. Use it to configure and manage back-end server features such as server maintenance and troubleshooting, local user definition, and so on.
- CiscoWorks link (in the upper right of the page)—Click this link to open the CiscoWorks Common Services home page. You can also access AUS from this page.

Step 4 To exit the application, click **Logout** in the upper right corner of the screen. If you log out of any window for the server (for example, the AUS window or the Security Manager home page), you are logged out of all windows.

Login sessions time out after 2 hours of inactivity.

Setting Up Browser-Server Security

Devices managed by AUS that you add to the Security Manager device inventory require that browser-server security mode be enabled so that Security Manager can properly deploy configuration files to AUS.

Common Services uses SSL to provide secure access between the client browser and AUS, and also between AUS and devices. Common Services provides secure access between:

- The client browser and management server (AUS).
- AUS and Security Manager.
- AUS and devices.

SSL is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys. SSL encrypts the transmission channel between the client and server. The CiscoWorks server uses certificates for authenticating secure access between the client browser and the management server.

You must enable SSL for secure access between the client browser and the management server and between AUS and Security Manager. However, you can disable SSL if you run a standalone AUS application; that is, AUS not integrated with Security Manager.

Procedure

Step 1 From the Cisco Security Management Suite home page, click **Server Administration** to open Common Services.

Step 2 In Common Services, click **Browser-Server Security Mode Setup.** (The full path to the page is **Server > Security > Single-Server Management > Browser-Server Security Mode Setup**.)

Step 3 If the "Current Setting" is shown as Enabled, the service is already enabled and you are finished.

If the service is not enabled:

a. Select **Enable**.

b. Click **Apply**.

a. Log out from your CiscoWorks session and close all browser sessions.

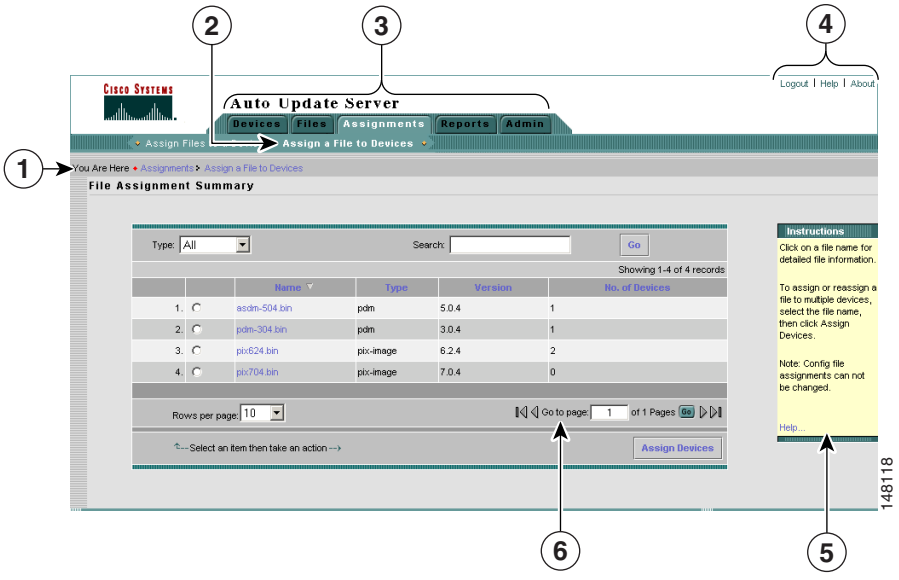
b. Restart the Daemon Manager from the CiscoWorks server CLI:

- Enter **net stop crmdmgtd**
- Enter **net start crmdmgtd**

Understanding the User Interface

The Auto Update Server application runs in a browser. Use the links and buttons in the interface instead of your browser buttons to operate the application. Figure 1-1 shows the interface and is followed by a detailed explanation.

Figure 1-1 AUS GUI



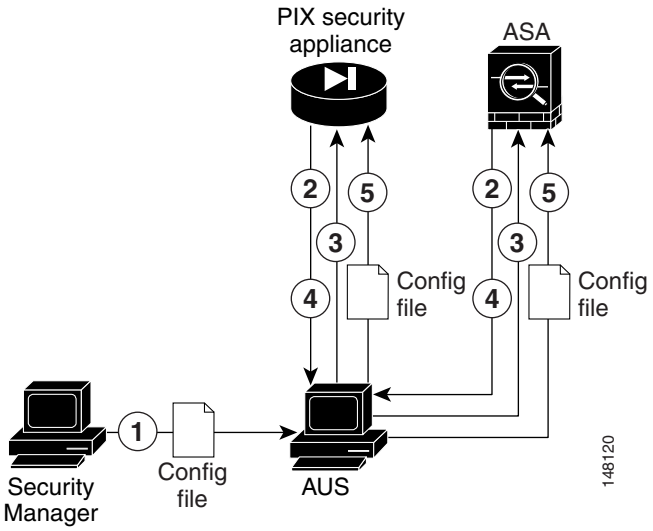
Reference	Location	Description
1	Path bar	Provides a context for the displayed page. Shows tab, option, and the current page. You can click a link to go to that page in the hierarchy.
2	Option bar	Displays the options available for the selected tab. Click an option to view the page.
3	Tabs	Provides access to the major features of the product. Click a tab to access its options. • Devices—Displays summary information about the devices managed by AUS. For more information, see Chapter 2, "Managing Devices and Update Schedules." • Files—Displays information about software images, PDM and ASDM images, and configuration files and enables you to add and delete software images and device manager images. For more information, see Chapter 3, "Managing Files." • Assignments—Displays assignment information and enables you to change device-to-image assignments and image-to-device assignments. For more information, see Chapter 4, "Managing File Assignments." • Reports—Displays reports. For more information, see Chapter 5, "Viewing Reports." • Admin—Enables you to configure NAT settings. For more information, see Deploying AUS Behind a NAT Boundary, page 1-2
4	Links	The following links: • Logout—Logs you out of CiscoWorks. • Help—Opens a new window that displays context-sensitive help for the displayed page. • About—Displays the version of the application.
5	Instructions box	Provides a brief overview of how to use the page. Click the Help link for more information.
6	Page	Displays the area in which you perform application tasks. Many pages, such as the one shown, contain tables. To operate on an item in a table, select the checkbox in the left-most column, then click the button beneath the table that corresponds to the action you want to take. You can sort tables by clicking the heading of the column by which you want to sort. You can search for items in the table by entering a search string and clicking **Go**. You can also filter the items in the table (to show only those that interest you) by making selections in the fields above the table. This operation filters the table only, and does not remove any data from the database.

Updating Configuration Files

Security Manager uses AUS as a conduit for updating configurations on managed PIX firewall and ASA devices. You must use Security Manager to create and deploy these configurations; you cannot use AUS for configuration deployment by itself.

Figure 1-2 shows how this is accomplish, and the following procedure explains how to use Security Manager and AUS together to deploy configurations.

Figure 1-2 Updating Configuration Files Using Security Manager and AUS



Reference	Description
1	Security Manager deploys the PIX firewall or ASA configuration file to AUS.
2	According to the configured schedule, the device contacts the AUS for updates.
3	The AUS sends a list of image file or configuration file URLs (or both) with the checksum of the files that the device should be running.
4	The device looks at the checksum it receives from AUS to verify whether it is running the correct file. If not, it requests the file from the AUS.
5	The file is downloaded to the device.

Procedure

Step 1 Configure the devices to use the AUS server. See Appendix C, "Bootstrapping Devices to Operate with AUS".

Step 2 In Security Manager, add the device using any of the available methods in the New Device wizard:

- If you select **Add New Device** or **Add Device from File**, you can select the AUS server that manages the device in the wizard. This is the same server you configured during bootstrapping. If the AUS server is not already defined in the inventory, you can define it during device addition.
- If you select **Add Device from Network** or **Add from Configuration Files**, you cannot select the AUS server in the wizard. Instead, after adding the device, select **Tools > Device Properties** and select the AUS server on the General tab. If the AUS server is not already defined in the inventory, you can define it through the device properties.

Besides specifying the AUS server that manages the device, ensure that you specify the following information either in the wizard or in the device properties:

- The device identity—When you bootstrap the device, you configure what you will use as the identity string, which is typically the device host name. Enter the identity either in the wizard or in the device properties.
- Credentials—You must enter an enable password. If you are using AAA to control access to a device, you must also enter the HTTP username and password required by the device.

See the Security Manager online help for detailed information about adding devices and AUS servers to the inventory and for any other Security Manager tasks mentioned in this procedure.

Step 3 Configure the AUS policy for the device in Security Manager. Do one of the following:

- Configure the policy for a single device. In Device view, select the device, and then select **Platform > Device Admin > Server Access > AUS** from the Device Policy selector.
- Configure a shared policy that you can assign to many devices that share the same AUS. In Policy view, select **PIX/ASA/FWSM Platform > Device Admin > Server Access > AUS** from the Policy Types selector. Right-click **AUS** and select **New AUS Policy** to create a policy, or select an existing policy from the Policies selector to change the policy. Select the Assignments tab to assign the policy to specific devices.

Configure other policies as desired to implement the configuration you want to deploy to the device.

Tip You cannot successfully deploy a configuration to AUS that requires Security Manager to download other files to the device. For example, some remote access VPN policies allow you to configure plug-ins, Anyconnect clients, and Cisco Secure Desktop configurations. These files are not sent to AUS. Do not use AUS if you want to configure these types of policy.

Step 4 In Security Manager, deploy your configurations using the **Deploy to Device** deployment method. Security Manager sends the configuration to the AUS, where the network device retrieves it.

The first time you deploy to a device, Security Manager adds it to the AUS inventory. You must successfully deploy to the device through the AUS before you can do any operations on the device using the AUS interface, such as doing an immediate auto update (an Update Now action). For a deployment to be successful, the device must contact AUS and retrieve the configuration.

Step 5 Confirm that the configurations were updated. Display the Event Report to see information about devices that contacted AUS. See Viewing the Event Report, page 5-4.

It might take some time for devices to be updated. If you do not see updated information, wait a few minutes and check the report again. If you still do not see updated information, see Appendix A, “Troubleshooting AUS.”

Related Topics

- Updating PIX Security Appliance, ASA, ASDM, and PDM Images
- Adding Devices to AUS, page 1-3
- Adding a Device Directly to AUS

Updating PIX Security Appliance, ASA, ASDM, and PDM Images

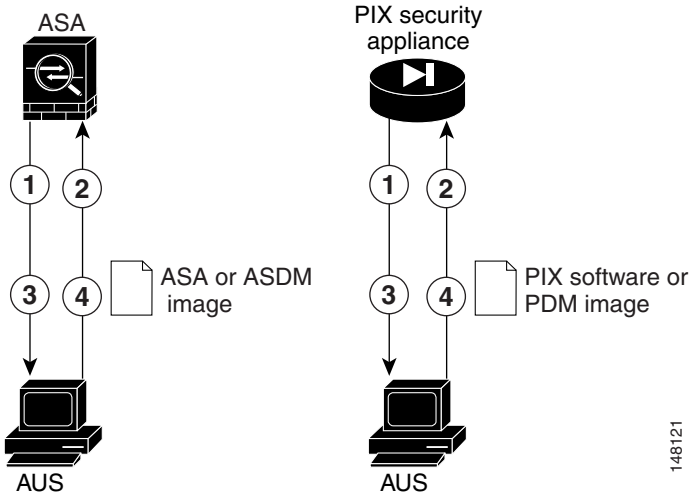
You can update PIX firewall software, ASA software, ASDM, and PDM images using AUS. These image updates do not involve Security Manager, so you can do them for devices whose configurations you are not managing with Security Manager.

When you update software or device manager images, keep the following in mind:

- Make sure the new PIX or ASA software image will work with the configuration file running on the device. If an incompatible software image is downloaded, the device will drop all unsupported commands and might experience configuration errors.
- Ensure that the new PDM or ASDM image will work with the existing software image running on the device. If an incompatible PDM or ASDM image is downloaded, PDM or ASDM might not start.

Note ASA devices must be bootstrapped with the **asdm image** and **boot system** commands to manage ASDM and ASA software images using AUS. For more information, see Configuring the Software Image and ASDM Image to Boot, page C-2.

Figure 1-3 Updating PIX Security Appliance, ASA, ASDM, and PDM Images Using AUS



Reference	Description
1	According to the configured schedule, the device contacts the AUS for updates.
2	The AUS sends a list of image file or configuration file URLs (or both) with the checksum of the files that the device should be running.
3	The device looks at the checksum it receives from AUS to verify whether it is running the correct file. If not, it requests the file from the AUS.
4	The file is downloaded to the device.

Procedure

Step 1 Configure the devices to use the AUS server. See Appendix C, "Bootstrapping Devices to Operate with AUS".

Step 2 Ensure that the device is added to AUS, either automatically during configuration deployment by Security Manager, or manually using the procedure described in Adding a Device Directly to AUS, page 2-3.

Step 3 Add the image to AUS. For details, see Adding Software Images, page 3-2.

Step 4 Assign the file to one or more devices.

- To assign the file to a single device, see Assigning and Unassigning Files to a Single Device, page 4-3.
- To assign the file to multiple devices, see Assigning and Unassigning a File to Multiple Devices, page 4-4.

According to the schedule you configure, the security appliance contacts the AUS and downloads the new software, ASDM, or PDM image. These actions take place without user intervention.

After you update a software image, the device is rebooted automatically. The reboot will cause a loss of connectivity, and all existing sessions through the firewall will break.

For this reason, you might choose to update security appliance images at a nonpeak traffic period. To ensure that all firewalls are updated during the nonpeak traffic period, you can set a limited polling period. For example, you might set a polling period of 3 hours and schedule the update to occur at 12:00 a.m. All firewalls would be updated between 12:00 a.m. and 3:00 a.m. For details about setting polling intervals, see Bootstrapping Security Appliances, page C-1. If the device is managed by Security Manager, you should configure these settings in the AUS policy (see Updating Configuration Files, page 1-6).

Step 5 Confirm that the images were updated. Display the Event Report to see information about devices that contacted AUS. See Viewing the Event Report, page 5-4.

It might take some time for devices to be updated. If you do not see updated information, wait a few minutes and check the report again. If you still do not see updated information, see Appendix A, "Troubleshooting AUS."