User Guide for Auto Update Server 4.9

First Published: August 5, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

User Guide for Auto Update Server 4.9

Preface

This manual describes how to use the Auto Update Server (AUS) application. It is for users who are skilled in network management and configuration, and who are responsible for configuring and maintaining PIX firewalls and Adaptive Security Appliance (ASA) devices.

Conventions

This document uses the following conventions:

Item	Convention
Commands or keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Selecting a menu item in paragraphs	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation

For a list of documentation for the Cisco Security Management Suite, see the documentation roadmap for your product release at http://www.cisco.com/c/en/us/support/security/security-manager/products-documentation-roadmaps-list.html.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

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 **Auto Update Server > 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."

Configuring Security Manager Servers in AUS

Beginning with version 4.8, Security Manager enables you to view the updated version information of a device that has been upgraded using Auto Update Server (AUS).

This feature is disabled by default. To enable AUS to update the version information, do the following:

Step 1 Log into Windows on the Security Manager server and edit the **ausconfig.properties** file in the NMSROOT\MDC\athena\config folder in the installation directory (usually c:\Program Files). Use a text editor such as Notepad to update the file.

Step 2 Locate the allowAUSToUpdateVersion property in the **ausconfig.properties** file and set it to true:

allowAUSToUpdateVersion=true

The following sections describe the procedure to add, edit, and delete CSM servers from within the AUS user interface. The CSM servers would be used for communicating with AUS to display the updated version of the device.

Adding Security Manager Server

Procedure

Step 1 Select **Auto Update Server > Admin > CSM Server Settings**. The CSM Server Settings page appears. This page displays the details of existing Security Manager servers if already added.

Step 2 Click **Add** to add a new Security Manager server. The Add CSM Server Details page appears.

Step 3 Enter the following:

- Server Name—The DNS hostname or IP address of the Security Manager server that you want AUS to communicate with.
- Username—The username for logging into the Security Manager server.
- Password—The password for accessing the Security Manager server. In the Confirm field, enter the password again.
- Port—The port number of AUS. This is typically 443.
- Protocol—Select either HTTPS or HTTP as required.

Step 4 Click **Save.**

Editing Security Manager Server

Procedure

Step 1 Select **Auto Update Server > Admin > CSM Server Settings**. The CSM Server Settings page appears. This page displays the details of existing Security Manager servers configured in AUS.

Step 2 Select a row and Click **Edit**.

Step 3 Modify the details as required and click **Save**.

Note You can edit details of one Security Manager server at a time.

Deleting Security Manager Server

Procedure

Step 1 Select **Auto Update Server > Admin > CSM Server Settings**. The CSM Server Settings page appears. This page displays the details of existing Security Manager servers configured in AUS.

Step 2 Select a row and Click **Delete**. A warning message appears. Review the warning and click **OK**.

Note You can delete one or more Security Manager server configuration at a time.

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 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 1-6

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:

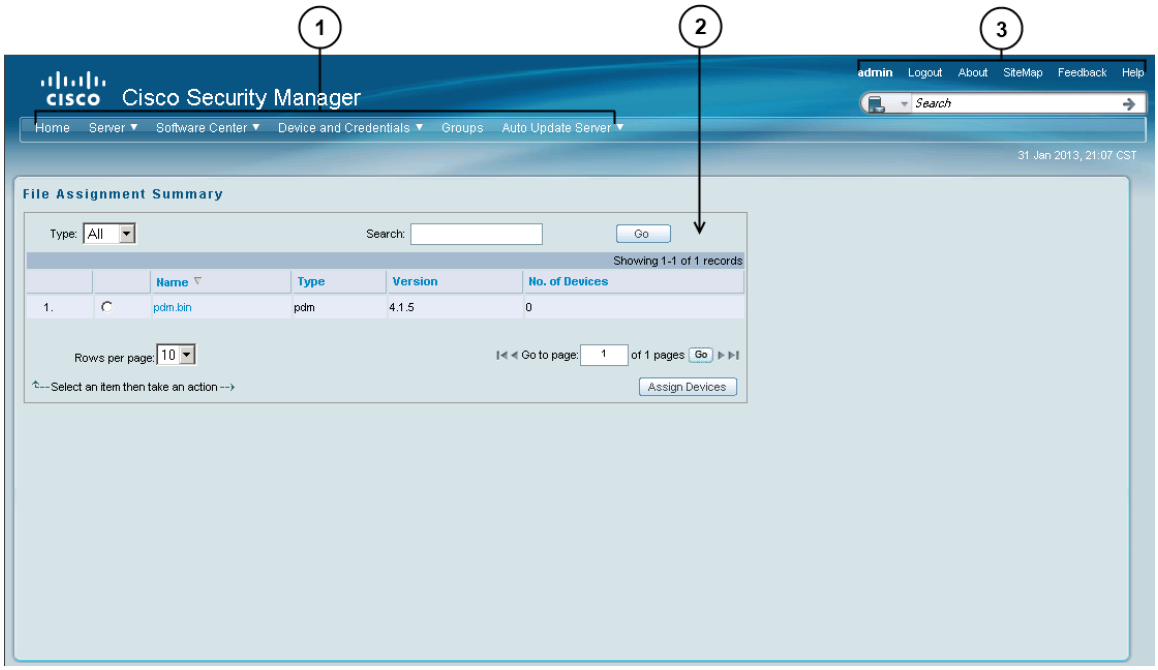
- Enter **net stop crmdmgtd**

- 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



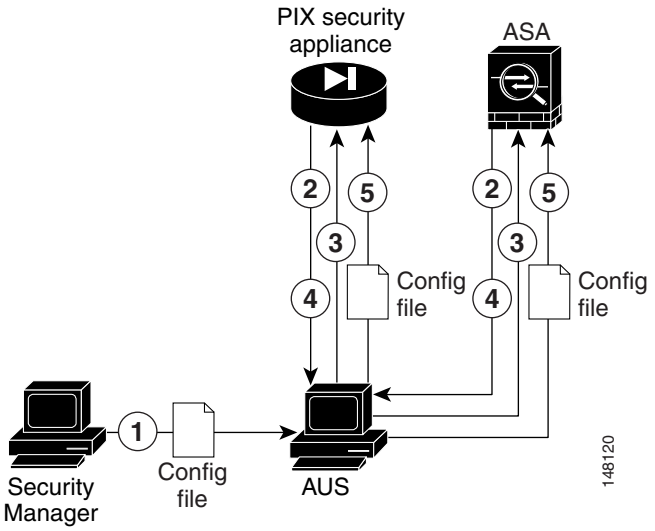
Reference	Location	Description
1	Menu bar	Provides access to the major features of the product. Hover over Auto Update Server, and then click an option to go to that page. • Devices—Displays summary information about the devices managed by AUS. For more information, see Chapter 2, "Managing Devices and 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
2	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.
3	Links	The following links: • Logout—Logs you out of CiscoWorks. • About—Displays the version of the application. • SiteMap—Displays a full listing of all menu commands with links to the various pages available to you. • Feedback—Takes you to Cisco.com where you can navigate to additional information about the product or use the Feedback link at the bottom of the page to provide feedback to Cisco.com. • Help—Opens a new window that displays context-sensitive help for the displayed page.

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.

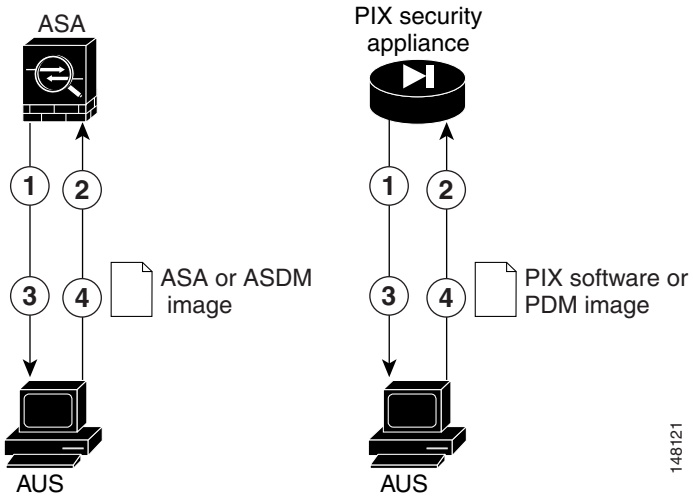
When you update software or device manager images, keep the following in mind:

- 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 1-8).

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."

Managing Devices and Update Schedules

The Device Summary page shows the list of devices that are defined in AUS. From this page, you can configure auto update schedules, initiate an immediate update, and block updates. The following topics help you understand and use the Device Summary page:

Viewing the Device Summary Page

Select **Auto Update Server > Devices** to display the Device Summary page. This page shows all managed devices and contains information about the devices, such as the device ID, device type, whether the device is up-to-date and when it last contacted AUS. From the Device Summary page, you can add or delete a device, initiate an immediate auto update, configure and change update schedules, and launch the PIX Device Manager (PDM) or Adaptive Security Device Manager (ASDM) applications.

Click a column name to sort the table by that column. You can also filter the information displayed in the table or search for a device.

Table 2-1 describes the fields on the Device Summary page.

Table 2-1 Device Summary Page

Element	Description
Check box	Selects the device on which to perform a function.
Device ID	The name that the device uses when identifying itself to AUS, which might differ from the hostname. You determine what is used as the device ID when you bootstrap the device or when you change the AUS policy in Security Manager (see Bootstrapping Security Appliances, page C-1). You can click on a device ID to open a window with a table that shows details and associated files for that particular device. Details include device name, IP address, serial number, sysObjectID, software version, PDM/ASDM version, and the available RAM and flash memory on the device, as well as repeating some information from this table.
Family	Always shows PIX. You can determine if a device is a PIX firewall or ASA device by looking at the model type in the Type field.
Type	The type of device, for example, PIX-535 or ASA-5540.
Up-to-Date	Whether the device is running the newest files: • No (Not Up-to-Date)—The device is not running the latest files deployed to AUS. • Up-to-date—The device is running the latest files deployed from AUS. • NA (Not Applicable)—The device does not fit into one of the other categories. There might not be any files assigned to it. • Not Contacted AUS—The device has never contacted AUS.
Update Type	The method by which a device is scheduled to receive updated files: • Any Time—The device is updated according to the polling schedule defined in the device's configuration. • One Time—The device is updated only once based on a user-defined time and date. • Daily—The device is updated every day based on a user-defined time and day. • Weekly—The device is updated every week based on a user-defined time and date. • Never—The device is never updated (updates are blocked).
Last Contact	The last time the device contacted AUS.
Add button	Click this button to add a device to the table manually. You do not need to add devices that you are managing with Security Manager. For more information, see Adding a Device Directly to AUS, page 2-3.
Update Now button	Click this button to request that a device immediately contact AUS and retrieve new files (an immediate auto update). For more information, see Requesting an Immediate Auto Update, page 2-6.
Launch Device Manager button	Click this button to start the PDM or ASDM application, depending on the device. If you are managing a device with Security Manager, you should not use the application to change the device configuration. For more information, see Launching Device Managers, page 2-7.

Table 2-1 Device Summary Page (continued)

Element	Description
Update Schedule button	Click this button configure an update schedule for a device. For more information, see Configuring Update Schedules, page 2-4.
Update Any Time button	Click this button to cancel an existing update schedule for a device and replace it with the default Any Time schedule, which uses the polling period defined on the device. For more information, see Canceling an Update Schedule, page 2-5.
Block Updates	Click this button to disable auto updates for selected devices. This sets the update schedule to Never. For more information, see Disabling or Blocking Auto Updates, page 2-7.
Delete button	Click this button to delete the device. Deleting the device does not delete it from Security Manager. For more information, see Deleting Devices, page 2-6.

Adding a Device Directly 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 to AUS. This is useful for two purposes:

- If you want to use AUS to manage software and ASDM/PDM image updates for devices not managed by Security Manager.
- If you need to troubleshoot some problem you are encountering.

Any devices that you manually add to AUS are not added to the Security Manager inventory.

Tip You cannot edit any properties after adding a device. If you need to change a property, for example, to update credentials, you must delete the device and add it again.

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page, page 2-1).

Step 2 Click **Add**. The Add Device page appears.

Step 3 Enter the following information to identify the device:

- **Device ID**—The identifier the device uses to identify itself to AUS.

  You configure the type of ID when you configure AUS settings on the device (as explained in Bootstrapping Security Appliances, page C-1), or in the **Platform > Device Admin > Server Access > AUS** policy for the device in Security Manager. Typically, the ID is the hostname of the device.

- **Auto Update Username and Password**—The username and password the device uses to authenticate with AUS. This user account is the one you configure during bootstrapping or from the AUS policy in Security Manager.

Step 4 If you want to be able to perform an immediate auto update (using the Update Now button as explained in Requesting an Immediate Auto Update, page 2-6), you must configure the **Request Auto Update Credentials** field. Select one of the following:

- **None**—No credentials provided. You cannot perform an immediate auto update on the device.
- **TACACS**—If you are using AAA to control access to devices, enter the TACACS+ username and password for the device.
- **Enable Password**—The password to enter enable mode, or privileged EXEC mode, on the device. This credential is also used by the device manager (ASDM or PDM) if you start it from AUS.

Note The TACACS+ and enable passwords are provided to AUS for any device added from Security Manager if you configure those settings in Security Manager. Security Manager uses the HTTP credentials as the TACACS+ credentials.

Step 5 Click **OK** to add the device.

Configuring Update Schedules

When you configure a device to use AUS, you configure a polling period that the device uses to contact AUS. This polling period, configured on the device, is referred to in AUS as an **Any Time** schedule; that is, the device can contact AUS at any time, based on the device's configuration.

The default polling period is 720 minutes. For information on changing the polling schedule defined on the device using the Security Manager client, see Changing the Polling Interval for the Device to Contact AUS, page 2-5.

You can create a schedule in AUS that overrides the schedule defined on the device. If you create a schedule using the following procedure, you can cancel it as described in Canceling an Update Schedule, page 2-5.

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page, page 2-1).

Step 2 Select the devices for which to configure an update schedule.

Step 3 Click **Update Schedule**. The Configure Update window appears.

Step 4 Select the type of schedule you want from the **Allow Updates** list and fill in the required fields. The scheduling options are:

- **One Time**—The device should be updated once. Select the date, enter the start time of the update window in HH:MM format (24-hour), and the duration of the window. The device will request the update within this window.
- **Daily**—The device should be updated every day. Enter the start time and the duration of the update window.
- **Weekly**—The device should be updated every week. Enter the start time and the duration of the update window, and select the day of the week on which the update should occur.

- **Never**—The device should never be updated. This blocks auto updates and is equivalent to clicking the Block Updates button on the Device Summary page. For more information, see Disabling or Blocking Auto Updates, page 2-7.

Step 5 Click **OK**. You are returned to the Device Summary Page and the new schedule is shown in the Update Schedule column.

Changing the Polling Interval for the Device to Contact AUS

If you allow the device to contact AUS according to the schedule defined on the device rather than one defined in AUS (called an Any Time schedule), you can use the Security Manager client to modify the polling schedule.

Procedure

Step 1 Do one of the following in the Security Manager client:

- (Device view) If the device does not use a shared policy, select the device and select the **Platform > Device Admin > Server Access > AUS** policy.
- (Policy view) If the device uses a shared policy, select the policy from the **PIX/ASA/FWSM Platform > Device Admin > Server Access > AUS** policy folder.

Step 2 Select the **Poll Type**, which can be based on frequency or on a specific schedule, and define schedule, polling times, and retry counts.

Your changes do not take effect until you deploy the configuration and the device retrieves the update from AUS. This means that the first deployment after you change this policy will be based on the previous version of the policy.

Canceling an Update Schedule

If you configured an update schedule in AUS for a device, you can cancel it. This changes the update schedule to Any Time, which means the device uses the polling period defined in its configuration to contact the AUS for updates.

You might want to do something different than canceling a schedule:

- If you want to stop the device from receiving updates, see Disabling or Blocking Auto Updates, page 2-7.
- If you want the device to retrieve an update immediately, see Requesting an Immediate Auto Update, page 2-6.

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page).

Step 2 Select the device for which to cancel an update schedule.

Step 3 Click **Update Any Time**. You are asked to confirm that you want to remove the update schedule from AUS.

Deleting Devices

If you no longer want to manage a device in AUS, you can delete it from AUS. If you are still managing the device in Security Manager, it will be added back into AUS if you deploy a configuration to it without changing the device to not use AUS.

You must delete devices separately in AUS and Security Manager. Deleting a device from one application does not delete it from the other application.

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page).

Step 2 Select the devices to delete.

Step 3 Click **Delete**. You are asked to confirm that you want to delete the device.

Requesting an Immediate Auto Update

Sometimes you want to have a device immediately contact AUS to ensure that the device has the newest files running on it instead of waiting for the device to contact AUS according to schedule. For example, you might want to request that a device contact AUS if the security of your network has been compromised, you updated its configuration in Security Manager and deployed it to AUS, but the device is not scheduled to retrieve a configuration for an acceptable amount of time.

To perform an immediate auto update, the you must ensure that the following requirements are met:

- The update schedule cannot be Never. If it is, first select the device and click **Update Any Time** or define an update schedule.
- The HTTPS port on the device must be the default 443. If you change the HTTPS port number on the device to any port number other than the default value of 443, you cannot perform an immediate auto update. Leave the HTTPS port number on the device at the default value if you want the device to contact AUS at times other than the scheduled interval.
- The TACACS+ credentials (when using AAA authorization) or enable password are defined for the device. These credentials are automatically supplied to AUS by Security Manager for the devices it adds so long as you configured them in Security Manager. (Security Manager uses the HTTP credentials as the TACACS+ credentials.) For more information, see Adding a Device Directly to AUS, page 2-3.
- The device must be directly addressable and not behind a NAT boundary.
- The device must have already contacted AUS successfully.

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page).

Step 2 Select the devices to update immediately.

Tip Requesting that a large number of devices immediately contact AUS can result in performance problems. If you want to update a lot of devices, do it in smaller groups.

Step 3 Click **Update Now**. You are asked to confirm your request.

AUS first tries using the TACACS+ credentials (the HTTP username and password) to contact the device. If that is not successful, the enable password is used.

You can use the Event Report to determine whether the update is successful (select **Reports > Events**). For more information, see Viewing the Event Report, page 5-4.

Disabling or Blocking Auto Updates

You can disable, or block, auto updates for a device. Disabling updates does not change the device configuration and you can re-enable updates by either creating an update schedule (see Configuring Update Schedules, page 2-4) or by allowing the device to retrieve updates at any time (by selecting the device on the Device Summary page and clicking **Update Any Time**).

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page).

Step 2 Select the device for which you want to disable auto updates.

Step 3 Click **Block Updates**. You are asked to confirm that you want to block updates, which changes the update schedule to Never.

Launching Device Managers

You can start ASDM or PDM from AUS to view or modify a particular setting on a device if you have installed ASDM or PDM for that device. The device must have already contacted AUS before you can start the device manager for it. If you are using Security Manager to configure the device, you should not use ASDM or PDM to change its configuration.

Note If you change the HTTPS port number on the device to any port number other than the default value of 443, you cannot start the device manager. Leave the default value of 443 if you want to start the device manager from AUS itself.

Procedure

Step 1 Select **Auto Update Server > Devices**. The Device Summary page appears (see Viewing the Device Summary Page, page 2-1).

Step 2 Select the device for which you want to launch the device manager.

Step 3 Click **Launch Device Manager**.

You are prompted to log into the application and the device manager is opened in a separate window. Use the application's online help to learn how to use it.

Managing Files

You can manage six types of files in AUS: PIX software images, ASA software images, PDM images, ASDM images, ASA configuration files, and PIX configuration files.

These topics will help you use AUS to manage the various types of files:

Viewing the File Summary Page

Select **Auto Update Server > Files** to display the File Summary page, which displays information about the files in the AUS database. From this page, you can:

- Add or delete software images, ASDM images, and PDM images
- View or delete configuration files.

Click a column name to sort the table by that column. You can also filter the information displayed in the table or search for a file.

You must boostrap ASA devices 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.

For a description of elements in the File Summary page, see Table 3-1.

Table 3-1 Files Summary Page

Element	Description
Check box	Selects the file on which to perform a function.
Name	The name of the file. Click the name to display a table of information about the file and the devices assigned to it.

Table 3-1 Files Summary Page (continued)

Element	Description
Type	The type of file: • pix-config—An ASA or PIX configuration file. • pix-image—An ASA or PIX software image file. • asdm-image—An ASDM software image. • pdm-image—A PDM software image.
Version	The software version of file. For configuration files, this is the OS version for which the configuration was created.
Create Timestamp	The date and time that the file was added to AUS.
No. of References	The number of devices assigned to the file. For information on assigning devices, see Chapter 4, "Managing File Assignments."
Add button	Click this button to add a file. For more information, see Adding Software Images, page 3-2.
View Config button	Click this button to view the selected configuration file. For more information, see Viewing Configuration Files, page 3-3.
Delete button	Click this button to delete the selected files. For more information, see Deleting Software Files, page 3-3.

Adding Software Images

You can add ASA or PIX software images, Adaptive Security Device Manager (ASDM) software images, or PIX Device Manager (PDM) software images.

Note You cannot add configuration files from AUS. You must use Security Manager to deploy configurations to devices. For more information, see Updating Configuration Files, page 1-8.

Before You Begin

Download the file to your workstation from Cisco.com. You should not change the name of the file, because AUS will not allow you to add files that do not fit the Cisco naming pattern.

Procedure

Step 1 Select **Auto Update Server > Files**. The Files Summary page appears (see Viewing the File Summary Page, page 3-1).

Step 2 Click **Add**. The Add File page appears.

Step 3 Select the type of file you are adding:

- pdm—PIX Device Manager (PDM) software image.
- asdm—Adaptive Security Device Manager (ASDM) software image.
- pix-image—An ASA or PIX software image.

Step 4 Click **Browse** and select the file that you want to add and click **Open**.

Step 5 Click **OK** to add the file. You are prevented from adding the file if it does not fit the normal Cisco name standards.

Deleting Software Files

You can delete any file that you no longer need. When you delete a file that is assigned to devices, all device assignments are also deleted. Before deleting a file, consider assigning devices to other files (see Chapter 4, "Managing File Assignments").

Deleting a file does not remove it from any assigned device that has already downloaded it.

Procedure

Step 1 Select **Auto Update Server > Files**. The Files Summary page appears (see Viewing the File Summary Page, page 3-1).

Step 2 Select the file to delete.

Step 3 Click **Delete**. You are asked to confirm the deletion.

Viewing Configuration Files

You can view the configuration files that Security Manager deploys to AUS.

Procedure

Step 1 Select **Auto Update Server > Files**. The Files Summary page appears (see Viewing the File Summary Page, page 3-1).

Step 2 Select the configuration file you want to view. You can view only one configuration at a time.

Step 3 Click **View Config**. The configuration file is displayed in a separate window.

Managing File Assignments

Use the options on the Assignments page to manage device and file assignments. For example, if a new ASA software image is available, you can download the file, add it to AUS, and then assign it to one or more devices. (For information on adding images, see Adding Software Images, page 3-2.)

You can assign multiple files to a single device. For example, you can assign an ASA software image, ASDM image, and ASA configuration file to a single ASA device. See Figure 4-1.

You can also assign single files to multiple devices. For example, you can assign the same ASA software image or ASDM image to many ASA devices. See Figure 4-2.

Note You cannot assign configuration files to multiple devices.

Figure 4-1 Assigning Multiple Files to One Device

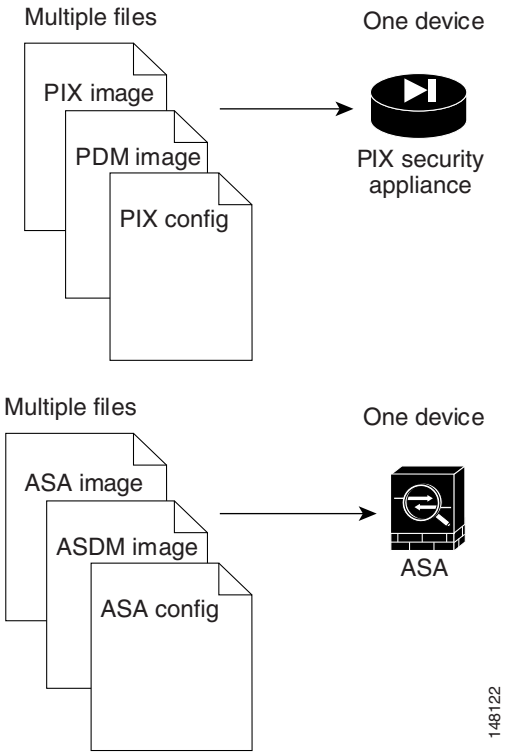
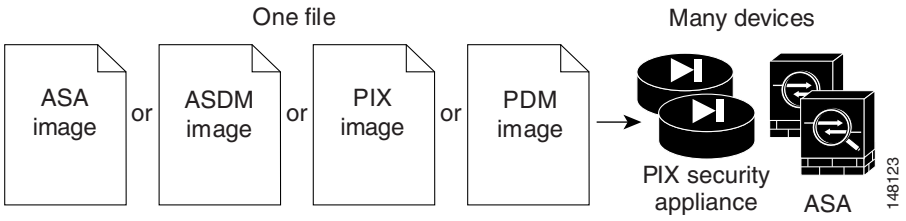


Figure 4-2 Assigning Multiple Devices to One File



These topics help you manage device and image assignments:

Viewing the Device Assignment Summary

Select **Auto Update Server > Assign Files to a Device** to display the Device Assignment Summary table (Table 4-1). The table displays information about the files assigned to each device.

Click a column name to sort the table by that column. You can also filter the information displayed in the table or search for a device.

Table 4-1 Device Assignment Summary

Element	Description
Radio button	Click the button of the device you want to assign files to.
Device ID	The name that the device uses when identifying itself to AUS. You can click on a device ID to open a window with a table that shows details and associated files for that particular device. Details include device name, IP address, serial number, sysObjectID, software version, PDM/ASDM version, and the available RAM and flash memory on the device, as well as repeating some information from this table.
Family	Always shows PIX. You can determine if a device is a PIX firewall or ASA device by looking at the model type in the Type field.
Type	The type of device, for example, PIX-535 or ASA-5540.
PDM Image	The name of the PDM or ASDM image file assigned to the device.
PIX Image	The name of the PIX Firewall or ASA image file assigned to the device.
PIX Config	The name of the PIX Firewall or ASA configuration file assigned to the device.
Assign Files button	Click this button to assign files to the selected device. For more information, see Assigning and Unassigning Files to a Single Device, page 4-3.

Related Topics

- Adding Software Images, page 3-2
- Viewing the File Assignment Summary
- Assigning and Unassigning a File to Multiple Devices

Assigning and Unassigning Files to a Single Device

From the Device Assignment Summary page, you can change which files are assigned to a device. You can unassign files and assign new ones, for example, to update the software image running on a device.

Note When changing an ASA or PIX software image, make sure that the existing configuration file will work with the new image. If an incompatible software image is downloaded, the security appliance will drop all unsupported commands and might experience configuration errors.

Procedure

Step 1 Select **Auto Update Server > Assign Files to a Device**. The Device Assignment Summary page appears (see Viewing the Device Assignment Summary, page 4-2).

Step 2 Select the device to which you want to assign files.

Step 3 Click **Assign Files**. The Select Images to Assign page appears.

Step 4 Select the configuration file, PIX/ASA software image file, or PDM/ASDM image file that you want to assign to the device. You can assign all three types of files. The list includes only those files that you have added to AUS.

Select **none** if you do not want to assign that type of file.

Step 5 Click **OK** to assign the files to the device.

Related Topics

- Adding Software Images, page 3-2
- Viewing the File Assignment Summary
- Assigning and Unassigning a File to Multiple Devices

Viewing the File Assignment Summary

Select **Auto Update Server > Assign a File to Devices** to display the File Assignment Summary table (Table 4-2). The table lists files and the number of devices assigned to each file.

Click a column name to sort the table by that column. You can also filter the information displayed in the table by file type or search for a file.

Table 4-2 File Assignments Summary

Element	Description
Radio button	Click the button of the file you want to assign devices to.
Name	The name of the file. You can click on a file name to open a window with a table that shows details and device assignments for that particular file.
Type	The type of file: • pdm—PIX Device Manager (PDM) software image. • asdm—Adaptive Security Device Manager (ASDM) software image. • pix-image—An ASA or PIX software image. • pix-config—An ASA or PIX configuration file.
Version	The software version of the file. For configuration files, this is the OS version for which the configuration was created.
No. of Devices	The number of devices assigned to a file.
Assign Devices button	Click this button to assign devices to the selected file. For more information, see Assigning and Unassigning a File to Multiple Devices, page 4-4.

Related Topics

- Adding Software Images, page 3-2
- Viewing the Device Assignment Summary
- Assigning and Unassigning Files to a Single Device

Assigning and Unassigning a File to Multiple Devices

From the File Assignment Summary page, you can change which devices are assigned to a file. For example, if you want to deploy a new ASA software image, you can assign it to all of your ASA devices at once.

You cannot assign a configuration file to multiple devices.

Note When changing an ASA or PIX software image for a device, make sure that the existing configuration file running on the device will work with the new image. If an incompatible software image is downloaded, the security appliance will drop all unsupported commands and might experience configuration errors.

Procedure

Step 1 Select **Auto Update Server > Assign a File to Devices**. The File Assignment Summary page appears (see Viewing the File Assignment Summary, page 4-3).

Step 2 Select the file whose assignments you want to change.

Step 3 Click **Assign Devices**. The Select Device Assignments page appears.

Click a column name to sort the table by that column. You can also filter the information displayed in the table or search for a device.

Step 4 Select the devices that you want to assign to the file. To remove an assignment, uncheck the box for the device.

If you want to select all displayed devices, select the check box in the table heading.

Step 5 Click **OK** to update the assignments.

Related Topics

- Adding Software Images, page 3-2
- Assigning and Unassigning Files to a Single Device
- Viewing the Device Assignment Summary

Viewing Reports

Reports provide you with useful information about AUS; for example, you can view reports that show how busy AUS is, show whether any errors have occurred, or display information about devices that have contacted AUS.

These topics help you understand AUS reports:

Viewing the System Information Report

Select **Auto Update Server > Reports > System Info** to display the system information report (Table 5-1).

The report shows general information about AUS, how busy the server is, and statistics related to activity in the past 24 hours.

Table 5-1 System Info Report

Row	Description
General System Information	
Auto Update Server URL	The URL that devices use to connect to AUS. When you add the AUS to Security Manager, use this information to identify the URN.
No. of Devices Managed	The number of devices in the AUS database.
No. of Devices That Never Contacted AUS	The number of devices in the AUS database that have never contacted AUS.
Percentage of Devices Up-to-date	The percentage of devices that successfully contacted AUS and downloaded new images or configuration files.
Percentage of Devices Not Up-to-date	The percentage of devices that have not yet contacted or that failed to contact AUS and download new images or configuration files.
No. of Files	The number of files in the AUS database.

Table 5-1 System Info Report (continued)

Row	Description
No. of Assignments	The number of image to device assignments and device to image assignments.
Statistics For Last 24 Hours	
The values for the following statistics are all based on the previous 24-hour period.	
No. of Successful Auto Updates	The number of times that devices contacted AUS and successfully retrieved an auto update.
No. of Failed Auto Updates	The number of times that devices contacted AUS but failed to retrieve an auto update.
Percentage of Devices that Contacted AUS	The percentage of devices that successfully contacted AUS and downloaded new image or configuration files.
Device That Contacted AUS Most	The device that contacted AUS the most number of times.
Most Downloaded File	The file that devices downloaded most often from AUS.
No. of Unique Files Downloaded	The number of unique files that devices downloaded from AUS.
No. of Successful File Downloads	The number of file downloads that were completed successfully.
No. of Failed File Downloads	The number of times an error occurred while a device was performing an auto update.
No. of Bytes Downloaded	The number of bytes that were downloaded.
No. of New Assignments	The number of new image-to-device and device-to-image assignments.

Related Topics

- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5
- Viewing the No Contact Since Report, page 5-6

Understanding AUS Event Types

When you view any of the event reports, each entry in the report includes an event type. This type describes in general what happened during the event. The description column provides more specific detail.

You can filter the report table by these events. The Event Failures and Event Successes reports provide information only on the failure or success types, whereas you can view all types in the Events report.

See the following topics for information on viewing event reports:

- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5

The following table describes all event types.

Table 5-2 Event Type Descriptions

Event Type	Description
CONNECT_SUCCESS	The device contacted AUS successfully and reported its inventory details.
CONNECT_FAILURE	A problem occurred during an auto update attempt. Possible causes are: • An error while parsing XML. • Invalid credentials. • The device has not been added to AUS. • Connectivity problems. • The database was down while trying to add a record.
DEVICE_CONFIG_ERROR	Errors reported to the server from the device or errors that occurred while the device was loading the configuration file assigned to it. You should use these errors for debugging configuration problems. When an error occurs while the configuration file is being downloaded to the device, the running configuration reverts to the startup configuration.
GENERAL_DEVICE_ERROR	A non-configuration file error reported to AUS from the device. Possible causes are: • Problems connecting to the Auto Update servlet. • Problems with the downloaded image (invalid checksum). To configure the security appliance to use a specific software image or ASDM image if you have more than one installed, or have installed them in external Flash memory, see Configuring the Software Image and ASDM Image to Boot, page C-2.
DOWNLOAD_SUCCESS	The file was successfully sent to the remote device without error. This does not mean that the device is running the image successfully; this message could be followed by either DEVICE_CONFIG_ERROR or GENERAL_DEVICE_ERROR.
DOWNLOAD_FAILURE	An error occurred while an image or configuration file was being downloaded. Possible causes are: • Invalid credentials. • Communication problems. • Database problem.
AUS_IMMEDIATE_SUCCESS	AUS successfully contacted and updated the device when you selected **Update Now** to perform an immediate auto update.
AUS_IMMEDIATE_FAILURE	An error occurred while the device was being updated during an immediate auto update. Possible causes are: • The server does not have direct connectivity to the device (for example, it is behind a NAT boundary). For information on configuring AUS to work with NAT, see Deploying AUS Behind a NAT Boundary, page 1-2. • The enable or TACACS+ username and password that the device uses to authenticate AUS are incorrect. For more information about these credentials, see Adding a Device Directly to AUS, page 2-3. • An internal error occurred.
SYSTEM_ERROR	An internal error occurred.

Viewing the Event Report

Select **Auto Update Server > Reports > Events** to display the event report. This report shows all events, whether successful or unsuccessful.

The report shows information about devices that have contacted AUS. It includes information such as the event type, the result of the event, the date and time of the event, and a detailed description to help you fix any problems that occurred. For a description of possible event types, see Understanding AUS Event Types, page 5-2.

The report also shows information about notifications sent from devices to AUS. For example, if an ASA device downloads a configuration file and discovers errors, it sends an alert to AUS, which the report displays. Entries are added each time a device contacts AUS or a file is downloaded.

Beginning from version 4.8, Security Manager displays the updated version information of a device that has been upgraded using AUS. The event report in AUS shows if the version update for a device in Security Manager has succeeded or failed.

You can manipulate the report in the following ways:

- The report shows events only for a single day. Select the day in the **Date** field (from the past 7 days only) to view events from that day.
- Click a column name to sort the table by column information. When you sort by the Device ID column, the table is sorted first by device ID, then by timestamp.
- You can filter the table and search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the System Information Report, page 5-1
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5
- Viewing the No Contact Since Report, page 5-6

Viewing the Event Failure Summary Report

Select **Auto Update Server > Reports > Event Failures** to display the event failure summary report.

The report lists the devices that encountered an event failure. The information for the device includes the number of times the device encountered each type of failure (no entry in a column indicates no failures of that type). To analyze the report:

- Select the day in the **Date** field (from the past 7 days only) to view events from that day.
- Click the device ID to open a detailed report that shows all of the events for that device on that day.
- Click the number in one of the failure columns to display the detailed report pre-filtered to show failures of that type. Following are the failure types; for a description, see Understanding AUS Event Types, page 5-2.
  - **Auto Update**—The number of CONNECT_FAILURE events (failures of the device to connect to AUS).
  - **Download**—The number of DOWNLOAD_FAILURE events (failures downloading a file to the device).

  - **Request Update**—The number of AUS_IMMEDIATE_FAILURE events (failures performing an immediate auto update).
  - **Configuration**—The number of DEVICE_CONFIG_ERROR events (errors in the downloaded configuration).
  - **General**—The number of GENERAL_DEVICE_ERROR events.
  - **System**—The number of SYSTEM_ERROR events (AUS system errors).
- Click a column name to sort the table by column information. When you sort by the Device ID column, the table is sorted first by device ID, then by timestamp.
- You can filter the table and search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the Event Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5
- Viewing the No Contact Since Report, page 5-6

Viewing the Event Success Summary Report

Select **Auto Update Server > Reports > Event Success** to display the event success summary report.

The report lists the devices that successfully completed an action. The information for the device includes the number of times the device succeeded at each type of event (no entry in a column indicates no successes of that type). To analyze the report:

- Select the day in the **Date** field (from the past 7 days only) to view events from that day.
- Click the device ID to open a detailed report that shows all of the events for that device on that day.
- Click the number in one of the success columns to display the detailed report pre-filtered to show successes of that type. Following are the success types; for a description, see Understanding AUS Event Types, page 5-2.
  - **Auto Update**—The number of CONNECT_SUCCESS events (where the device succeeded in connecting to AUS).
  - **Download**—The number of DOWNLOAD_SUCCESS events (successful file downloads to the device).
  - **Request Update**—The number of AUS_IMMEDIATE_SUCCESS events (performing an immediate auto update successfully).
- Click a column name to sort the table by column information. When you sort by the Device ID column, the table is sorted first by device ID, then by timestamp.
- You can filter the table and search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the No Contact Since Report, page 5-6

Viewing the No Contact Since Report

Select **Auto Update Server > Reports > No Contact Since** to display the no contact since report.

The report lists the devices that have not contacted AUS since the date specified and shows the date and time of the last successful contact. To analyze the report:

- If desired, specify a different date from which you want to view contact information in the **Select Date** field and click **Go**.
- Click the device ID to open a detailed report that shows all of the events for that device. You can view events over the previous 7 days. For more information about the types of events you can view in the detail report, see Understanding AUS Event Types, page 5-2.
- Click a column name to sort the table by column information.
- You can search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the System Information Report, page 5-1
- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5

Troubleshooting AUS

These topics will help you troubleshoot AUS:

Why Is the Device Not Showing Up in the Device Summary?

If the device is not shown in the device summary, it was not added correctly to the Security Manager inventory. The method for adding devices using Security Manager is explained in Updating Configuration Files, page 1-8.

After deploying a configuration as described in that topic, check the Security Manager deployment results to ensure deployment was successful. Also, check AUS event reports to ensure the device successfully contacted AUS and retrieved the configuration.

If deployment was successful and the device successfully downloaded the configuration, it should appear in the AUS device list.

Why Has the Device Not Contacted AUS?

If the device has never contacted AUS, it could be because:

- The device is not configured with the correct AUS URL.
- The device does not have network connectivity.
- The credentials for the device in AUS are incorrect.
- The device is configured correctly but has not yet polled AUS.
- You are not using the correct PIX firewall software version. (You must use a minimum of release 6.3.) All versions of ASA are supported.

For the device to contact AUS, do one or more of the following:

- Wait for the polling period to end.
- If the device has not contacted AUS after the polling period ends, verify that the device can connect to AUS by logging into the device and pinging the AUS server from the device console.
- Verify that the device is configured to operate in its deployed environment. If it is deployed for DHCP, ensure that a DHCP server is present to give the device a network address. If the device is deployed with a static IP address, verify that the IP address is correct.
- Check the event report to see if there are any authentication errors for the device by selecting **Auto Update Server > Reports > Events** in AUS. If there are authentication errors, the Event Type column displays CONNECT_FAILURE and the description column gives a message that the device has an authentication error.
- Check the Auto Update URL to verify that it matches the URL in the system information report (**Auto Update Server > Reports > System Info**). Log into the device, enter enable mode, and enter show auto-update to view the AUS settings configured on the device.

  If the URL does not match the URL shown in the system information report, set the new AUS URL by entering the following.

  ```
  conf t
  auto-update server
  https://username:password@AUSServerAddress:port/autoupdate/AutoUpdateServlet
  ```

- Check the AUS logs to see if there are any errors.

AUS Gives Authentication Errors—What Should I Do?

Authentication errors can occur when the device tries to contact AUS. Authentication errors are visible in the event report (see Viewing the Event Report, page 5-4) or from the device console (if debug is enabled on the console).

To enable debug on the device console, log into the device, enter enable mode, and configure the following commands:

```
conf t
logging on
logging console debug
```

Authentication errors can result from using incorrect credentials:

- When you added the device to AUS, you entered a set of credentials that allowed the device to contact the server. The username/password credentials are incorrect. These credentials come from Security Manager for devices that it adds (the HTTP username and password and the enable password).
- A user changed, through the command line, the set of credentials that the device was using to connect to AUS. Now the credentials no longer match the server credentials.

To resolve the problem, do one or more of the following:

- Wait until the device contacts AUS and reports the new configuration file.
- Access the device to resolve authentication problems. See the appropriate device documentation.
- Log into the device and use the command line to change the username and password. Enter:

```
enable
conf t
auto-update server
https://username:password@AUSServerAddress:port/autoupdate/AutoUpdateServelet
```

Why Is the Device Not Current After I Request an Auto Update?

If you requested that a device immediately contact AUS for an auto update (see Requesting an Immediate Auto Update, page 2-6), but the device is not current, the cause could be one of the following:

- The request has not yet gone through the queue. If you requested that multiple devices immediately contact AUS, it might take a period of time for the request to go through, as AUS processes requests one at a time.
- The device is not accessible.
- The CLI commands generated by Security Manager for the configured policy definitions are incorrect.

To resolve the problem, do one or more of the following:

- Wait a few moments for the request to go through the queue.
- Verify that the device is not behind a firewall or NAT boundary. The Update Now command does not work on such devices; you must wait until the polling period ends for the device to obtain the update.
- Ensure that the device identity configured in the Security Manager inventory matches the device ID configured on the device. Ensure that the correct HTTP username and password, and enable password, are correct.
- View the event report to check whether any command was generated incorrectly for any of the policy settings.

Why Does AUS Give Errors When I Try to Add an Image File?

If you are trying to add a PDM, ASDM, ASA, or PIX software image file to AUS and are receiving error messages, the problem might be one of the following:

- You are not selecting the correct image type to assign to the file.
- The image file that you are adding is not correct, or it is corrupted.
- The file name does not fit the expected file naming pattern.

You can resolve the problem by doing one or more of the following:

- Make sure that you select the correct image type when adding the file.
- Make sure that you do not change the file name when you download the file from Cisco.com.
- Verify that the image file is not corrupted. Check the MD5 checksum of the image file. To view the checksum value, select **Auto Update Server > Files** and click the name of the image file in the Name column. A popup window appears with information about the file, including the checksum value. For more information, see the Viewing the File Summary Page, page 3-1.

  Compare this checksum value with the value you received when the image was downloaded. If they are different, the image file is corrupted.

Why Cannot I Add a Configuration File?

You can add only ASDM, PDM, ASA, and PIX software image files. To add configuration files, you must use Security Manager to configure the device and to deploy the configuration to AUS. For an explanation of the process, see Updating Configuration Files, page 1-8.

I Assigned an Image File To a Device—Why Is It Not Current?

If you assigned an image file to a device but the device does not contain this file, the problem could be because:

- The device must contact AUS to report that it is running an image file. Depending on the polling period of the device, you might need to wait several hours for an update.
- The device is having problems contacting AUS.
- The image file is bad.

To resolve the problem, do one or both of the following:

- Check the AUS timestamp to verify the last time the device contacted AUS. If the polling period has not ended, then the device has not contacted AUS to report the latest information. If you do not want to wait for the polling period to end, you can request that the device contact AUS immediately (see Requesting an Immediate Auto Update, page 2-6).
- Check the event report (select **Auto Update Server > Reports > Events)** to look for errors. If a bad image file is assigned to the device, you will see the DEVICE_CONFIG_ERROR event type in the report, which indicates that an error occurred while downloading the image file. Assign a new image file to the device or remove the assignment to revert to the previously configured image file on the device.

  If the device has not contacted AUS to report that it is running an image file, see Why Has the Device Not Contacted AUS?, page A-2.

Why Cannot I Assign Two Image Files of the Same Type To A Device?

A device can run only one ASA software image, PIX software image, ASDM file, or PDM file at a time, so you can assign only one file of each type to a device.

Why Does the Device Reboot After I Assign A New PIX or ASA Software Image To It?

After you assign a new ASA or PIX software image to a device, a reboot is required. The reboot is automatic.

Why Does the Device Keep Downloading the Same File?

If a device continuously downloads a file, the device is having problems running the image. Check the event report (select **Auto Update Server > Reports > Events**) for errors. If there are errors, assign a new image file.

Why Are Some Buttons Grayed-Out?

If buttons are grayed out on certain AUS screens, you do not have the correct privileges to perform those commands. See Appendix B, "User Roles and Permissions."

Why Cannot I Start AUS After I Reboot My Machine?

It takes AUS a few minutes to restart after you reboot your machine. Do one of the following:

- Wait a few minutes before starting AUS.
- Check the AUS error logs to ensure that all processes are running properly.

How Can I Stop A Device From Trying To Download A Faulty or Incorrect Configuration File?

You can unassign the configuration file. For details, see Assigning and Unassigning Files to a Single Device, page 4-3. After unassigning the configuration file, correct and redeploy it using Security Manager.

How Can I Check the Connection between AUS and a PIX or ASA device?

If you have not installed Security Manager yet, or you simply want to check the connection between AUS and a device, you can add the device to AUS manually. For details, see Adding a Device Directly to AUS, page 2-3.

At the defined interval, the device contacts AUS. Verify that the device contacted AUS by reviewing the event report. See Viewing the Event Report, page 5-4.

After verifying that the connection between AUS and the device is correct, delete the device from AUS.

What Can I Do If Configuration Errors Are Reported?

If the event failure summary report shows configuration errors, view the suspected configuration file to find the problem. See Viewing Configuration Files, page 3-3.

Use the line number in the configuration error to locate the fault in the configuration file.

Understanding Error Messages

You can check the following logs for information about errors:

- *NMSROOT*\MDC\log\operation\autoupdate.log—AUS log that contains all messages from the AUS application.
- *NMSROOT*\MDC\tomcat\logs\stdout.log—Tomcat output log that contains messages from any application running under tomcatServletEngine.
- *NMSROOT*\MDC\tomcat\logs\stderr.log—Tomcat standard error log that contains a java stack trace when the java code breaks.

Table A-1 displays common error messages, their probable causes, and possible solutions.

Table A-1 AUS Error Messages

Message	Probable Cause	Possible Solution
CALLHOME-DB-ADD_FILE_ FAILURE	An error occurred when the file was being added to AUS. A database communications problem occurred.	Try to add the file to AUS again. If that does not work, restart AUS.
CALLHOME-FILE-INVALID_FILE_ NAME	The filename is incorrect. The name of the file is either too long or too short, or does not follow the expected naming pattern.	Enter the correct filename.
CALLHOME-FILE-INVALID_FILE_ CONTENTS	You added a file that is either corrupt or is not the correct file type.	Replace the file or try to add a different file.

Table A-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-FILE_NOT_FOUND	The selected file could not be found. You already deleted this file from the database.	Refresh the screen by clicking the Files tab.
CALLHOME-FILE-BAD_FILE_NAME	There was a problem when AUS tried to access the file. Either the file does not exist or it cannot be read.	Verify that the file exists and that it is not corrupt.
CALLHOME-FILE-INVALID_IMAGE	You cannot add the file to AUS; either the file is corrupted or you are trying to add a file type that is different from the file type specified in AUS.	Download a new version of the image file and add the file to AUS.
CALLHOME-DEVICE-NOT_CALLED_HOME_YET	The device did not contact AUS; AUS does not know the IP address of the device.	Wait until the device contacts the AUS and requests an auto update (see Requesting an Immediate Auto Update, page 2-6).
CALLHOME-SECURITY-NOT_AUTHENITCATED	AUS cannot authenticate your username/password credentials. Either your credentials are incorrect or your session timed out.	Reenter your username and password and log in to AUS.
CALLHOME-COMMON-AUDIT_FAILED	AUS cannot write to either the ACS or the Core audit log. A communication error occurred.	Restart AUS. If the problem persists, contact Cisco technical support.
CALLHOME-DEVICE_NOT_FOUND	AUS cannot find the selected device. The device was already deleted from the database.	Refresh the screen by clicking the Devices tab.
CALLHOME-FILE-CANNOT_DELETE_FILE	You cannot delete the file. The file is in use.	Try to delete the file again. If you cannot delete the file, restart AUS.
CALLHOME-DEVICE-BAD_CALLHOME_IMMEDIATE_RESPONSE	An error occurred during auto update. Enable or AAA credentials are incorrect, or the device does not allow HTTP access.	Ensure that the device allows HTTP access for AUS; ensure that the AUS AAA and enable credentials are correct. See Adding a Device Directly to AUS, page 2-3.
CALLHOME-FILE-MOVE_ERROR	The temporary file used when you added the file cannot be deleted. The filename you specified contains invalid or illegal characters, or the file already exists in the storage area.	Check the storage directory to verify that the file is not already there. Try the task again; if the problem persists, restart AUS and try to add the configuration file again. Check the log file for errors.
CALLHOME-DEVICE-CH_IMMEDIATE_NO_CREDENTIALS	AUS cannot perform an auto update. AUS does not know what credentials to use to communicate with the device because no enable password or AAA credentials were entered for the device.	Modify the device entry with the correct credentials and try the task again. See Adding a Device Directly to AUS, page 2-3.

Table A-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-INVALID_UPLOAD_ FILE	The file is invalid.	Enter a valid filename.
CALLHOME-DB-NO_CONNECTION	AUS cannot connect to the database. The database server is stopped.	Restart AUS and try the task again.
CALLHOME-DB-BAD_PASSWORD_ STATE	An error occurred while the database password was being changed. The AUS db.prop file does not contain the correct username and password for the database, or you entered the password incorrectly.	Verify that the AUS db.prop file contains the correct username and password for the database and enter your username and password again.
CALLHOME-DB-COMMIT_ERROR	AUS is unable to write data to the database.	Restart AUS and try the task again.
CALLHOME-DB-POOL_ERROR	AUS is unable to connect to the database.	Restart AUS and try the task again.
CALLHOME-DB-DISK_FULL	You ran out of disk space.	Remove unneeded information from your hard drive or add a new hard drive.
CALLHOME-DB-ADD_DEVICE_ FAILURE	There is a problem adding the device to the system. A database communications problem occurred.	Try to add the device again. If you still cannot add the device to AUS, restart AUS.
CALLHOME-DB-ADD_FILE_ FAILURE	There is a problem adding the file to the system. A database communications problem occurred.	Try to add the file again. If you still cannot add the file to AUS, restart AUS.
CALLHOME-DB-DUPLICATE_ VALUE	You are trying to add a file that already exists in AUS.	Use the existing entry, or delete the existing entry and retry the task.
CALLHOME-DB-DEVICE_NOT_ FOUND	AUS cannot find the requested device. A device that was added to AUS tried to contact AUS.	Verify that you entered the correct device ID and try the task again.
CALLHOME-DEVICE-INVALID_ AUTHORIZATION	The device passed invalid authorization information. Check the device username and password.	Update the device username and password.
CALLHOME-FILE-CHECKSUM_ MISMATCH	The checksum of the file has changed since the file was added to the database. Either another user changed the file or your system is compromised.	Make sure your machine is secure. Then delete the image file and add a new copy of the file to AUS.
CALLHOME-INVALID_UPLOAD_ FILE	The filename is invalid.	Enter a valid filename to upload.
CALLHOME-UI_CANNOT_MODIFY_ CONFIG_MAPPING	The assignments for the configuration file cannot be modified.	Use Security Manager to modify the configuration file.

Table A-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-UI_INVALID_ IPADDRESS	The IP address is invalid. You entered an invalid IP address.	Enter a valid IP address.
CALLHOME-UI_MULTICAST_ ADDRESS	The multicast address is not within the RFC multicast range (224.0.0.0-239.255.255.255). An invalid multicast address was entered.	Enter a valid multicast IP address.
CALLHOME-UI_NO_DEVICE_EXIST	The device no longer exists. You might have already deleted the device.	Refresh the screen by clicking the Devices tab.
CALLHOME-BOUNDS-INVALID_ EMPTY_START_UPDATE_WINDOW_ TIME	The start time for auto update schedule was left blank. You did not enter the time for auto update to start.	Enter the start time using the HH:MM format.
CALLHOME-BOUNDS-INVALID_ EMPTY_END_UPDATE_WINDOW_ TIME	The duration for the auto update schedule is left blank. You did not enter the duration time for the auto window.	Enter the duration time using the HH:MM format.
CALLHOME-BOUNDS-INVALID_ EMPTY_UPDATE_WINDOW_DAY_ INFO	The day of the week on which you want a weekly auto update to occur was left blank. You did not select the days of the week for auto updates to occur.	Select the day of the week on which weekly update must occur.
CALLHOME-COMMON-MISSING_ UPDATE_WINDOW	The update schedule type is missing. A null or invalid device ID object was passed.	Ensure that the device ID is passed properly.
CALLHOME-BOUNDS-INVALID_ UPDATE_WINDOW_TYPE	The configured update schedule type is invalid. You configured an invalid update schedule type.	Ensure that the update schedule type is configured properly.
CALLHOME-UPDATE_WINDOW_ NOT_CONFIGURED	The auto update schedule cannot be deleted. You did not configure an update schedule.	Schedule a configuration update first before you try to delete it.
CALLHOME-UPDATE_WINDOW_ UNSUCCESSFUL	The update schedule configuration was unsuccessful. You already configured an update schedule type for the device.	Delete the existing update schedule.

User Roles and Permissions

Your username and password must be authenticated for you to use AUS. Your username and password pair are compared with either the CiscoWorks Server or Cisco Secure Access Control Server (ACS) database, depending on which you configured to use with AUS.

After authentication, your authorization is based on the privileges that were assigned to you. A privilege is a task or operation defined within the application. The set of privileges assigned to you defines your role and dictates how much and what type of system access you have.

These topics provide details about the user roles and permissions associated with the two types of authentication methods:

AUS Privileges

AUS privileges are the major actions that you can perform. These privileges are assigned to the CiscoWorks Server and ACS roles described in the following sections:

- CiscoWorks Server Roles and AUS Privileges, page B-2
- Cisco Secure ACS Roles and AUS Privileges, page B-3

The following table lists the AUS privileges.

Table B-1 AUS Privileges

Privilege	Description
API_View_Device GUI_View_Device	Allows you to view device information.
API_View_Images GUI_View_Images	Allows you to display information about software images.
API_View_Assignment GUI_View_Assignment	Allows you to gather and display information about device-to-file and file-to device assignments.
API_View_Reports GUI_View_Reports	Allows you to display system summary information and event reports.

Table B-1 AUS Privileges

Privilege	Description
API_View_Admin GUI_View_Admin	Allows you to display AUS administrative information.
API_Modify_Device GUI_Modify_Device	Allows you to force a device to contact AUS.
API_Modify_Images GUI_Modify_Image	Allows you to add images to and delete images from AUS.
API_Modify_Assignment GUI_Modify_Assignment	Allows you to assign a file to devices and devices to a file.
API_Modify_Admin GUI_Modify_Admin	Allows you to change AUS administrative configuration settings.

CiscoWorks Server Roles and AUS Privileges

When you perform an action to devices using the CiscoWorks Server authentication method, the action is authorized according to the selected device.

The CiscoWorks Server has five roles that correspond to likely functions within your organization.

The following table lists roles for use with AUS.

Table B-2 CiscoWorks Roles

Role	Description
System Administrator	Can perform all CiscoWorks Server and AUS tasks, for example, add users, set user passwords, add or delete images, and delete assignments.
Network Administrator	Can perform CiscoWorks Server administrative tasks and has the same privileges as the system adminstrator.
Network Operator	Has read-only access to all information in AUS.
Approver	Can modify devices. Has read-only access for images, assignments, reports, and administration tasks.
Help Desk	Has read-only access to all information in AUS.

Table B-3 lists AUS roles and their supported privileges. See Table B-1 for descriptions of the privileges.

Table B-3 CiscoWorks Roles and AUS Privileges

	CiscoWorks Role				
AUS Privilege	System Admin	Network Admin	Network Operator	Approver	Help Desk
API_View_Device GUI_View_Device	X	X	X	X	X
API_View_Images GUI_View_Images	X	X	X	X	X

Table B-3 CiscoWorks Roles and AUS Privileges (continued)

AUS Privilege	CiscoWorks Role				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
API_View_Assignment GUI_View_Assignment	X	X	X	X	X
API_View_Reports GUI_View_Reports	X	X	X	X	X
API_View_Admin GUI_View_Admin	X	X	X	X	X
API_Modify_Device GUI_Modify_Device	X	X	–	X	–
API_Modify_Images GUI_Modify_Image	X	X	–	–	–
API_Modify_Assignment GUI_Modify_Assignment	X	X	–	–	–
API_Modify_Admin GUI_Modify_Admin	X	X	–	–	–

Cisco Secure ACS Roles and AUS Privileges

Cisco Secure ACS supports roles that are application-specific. A higher-level role includes all privileges associated with lower-level roles. Unlike other applications that use ACS for authentication, AUS checks authorization with itself, not on a per-device basis.

You can use the AUS roles already defined in ACS, or you can create your own, customized roles.

For more information about using ACS and for an understanding of ACS security advantages, see the *User Guide for Cisco Secure ACS for Windows Server.*

The following table lists the default roles for use with AUS.

Table B-4 ACS Roles

Role	Description
System Administrator	Full privileges (superuser).
Network Administrator	Full privileges (superuser).
Network Operator	Read privileges for the GUI.
AUS Remote Interface	Privileges to access only the external interface and not the GUI.
Help Desk	Read-only privileges for nonsensitive data.
API Reader	Read privileges for the external interface.
API Writer	Read and write privileges for the external interface.
GUI Reader	Read privileges for viewing information on the GUI.
GUI Writer	Read and write privileges for viewing and modifying information on the GUI.

Note For communication between Security Manager and AUS to be successful, the username and password entered for AUS in Security Manager must be associated with the API_Writer role, a role that has the same privileges, or the AUS remote interface.

Table B-5 lists the default AUS roles and their supported privileges. See Table B-1 for descriptions of the privileges.

Table B-5 ACS Roles and AUS Privileges

AUS Privilege	ACS Role							
	System Admin	Network Admin	Network Operator	Help Desk	API Reader	GUI Reader	API Writer	GUI Writer
API_View_Device	X	X	X	–	X	–	X	–
GUI_View_Device	X	X	X	X		X	–	X
API_View_Images	X	X	X	–	X	–	X	–
GUI_View_Images	X	X	X	X		X	–	X
API_View_Assignment	X	X	X	–	X	–	X	–
GUI_View_Assignment	X	X	X	X		X	–	X
API_View_Reports	X	X	X	–	X	–	X	–
GUI_View_Reports	X	X	X	X		X	–	X
API_View_Admin	X	X	X	X	X	–	X	–
GUI_View_Admin	X	X	X	–	–	X	–	X
API_Modify_Device	X	X	–	–	–	–	X	–
GUI_Modify_Device	X	X	–	–	–	–	–	X
API_Modify_Images	X	X	–	–	–	–	X	–
GUI_Modify_Images	X	X	–	–	–	–	–	X
API_Modify Assignment	X	X	–	–	–	–	X	–
GUI_Modify_Assignment	X	X	–	–	–	–	–	X
API_Modify_Admin	X	X	–	–	–	–	X	–
GUI_Modify_Admin	X	X	–	–	–	–	–	X

Bootstrapping Devices to Operate with AUS

To enable communication between AUS and devices, you must configure transport settings on the devices, before you add them to AUS or the Security Manager inventory. You configure devices according to the functionality you need.

Bootstrapping Security Appliances

Before you can manage a PIX firewall or an ASA device using AUS, you must set up the device with a minimum configuration that provides basic connectivity. See the *User Guide for Cisco Security Manager* for details about setting up basic connectivity.

In addition to basic connectivity, you need to configure some settings specific to AUS. The following procedures describe how to configure and verify these settings using the command line interface on the device. You can also use the PIX Firewall Device Manager (PDM) Setup wizard to configure a PIX version 6.3 device, or the Adaptive Security Device Manager (ASDM) Startup Wizard to configure PIX 7.0+ or ASA devices. See the ASA, ASDM, and PDM documentation for more information.

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.

To bootstrap a PIX or ASA device to operate with AUS, follow these steps from the console terminal connected to the device console port:

	Command	Purpose
Step 1	**enable** *password*	Enters privileged EXEC mode.
Step 2	**config terminal**	Enters configuration mode.
Step 3	**http server enable**	Enables the HTTP server on the device so that it can be monitored or have its configuration modified from a browser or HTTP connection.

	Command	Purpose
Step 4	**http** *ip_address* [*netmask*] [*if_name*]	Specifies the host or network authorized to initiate an HTTP connection to the device. Enter this command for each host you want to allow HTTP access. • *ip_address*—IP address of the host or network authorized to initiate an HTTP connection to the device. At minimum, you should use this command to specify the addresses of the AUS and Security Manager servers. • *netmask*—Network mask for the IP address. • *if_name*—The device interface name (default is **inside**) through which AUS or Security Manager initiates the HTTP connection. **Note** You must configure this setting to perform immediate auto updates. This setting also determines from which hosts you can access the device through ASDM/PDM or other HTTP connections.
Step 5	**auto-update server https://***username***:***password@AUSserver_IP_address***:***port***/autoupdate/AutoUpdateServlet**	Connects the device to AUS. • *username*—Login name used to enter the AUS server. • *password*—Password for the user. • *AUSserver_IP_address*—IP address of the AUS server. • *port*—Port number of the AUS server, typically 443.
Step 6	**auto-update poll-period** *poll_period [retry_count] [retry_period]*	Configures the polling period for AUS. • *poll_period*—The polling period interval between two updates. Default is 720 minutes (12 hours). • *retry_count*—The number of times to retry if the server connection attempt fails. Default is 0. • *retry_period*—The number of minutes between retries. Default is 5.
Step 7	**auto-update device-id [hardware-serial | hostname | ip_address** [*if_name*] **| mac-address** [*if_name*] **| string** *text* **]**	Configures the device to use the specified device ID to identify itself. • *if_name*—The device interface name (the default is **inside**). • *text*—Text that identifies the device. In the following example, the hostname is used as the device ID: `auto-update device-id hostname`
Step 8	**write memory**	Saves the configuration.
Step 9	**show auto-update**	Shows the AUS URL, poll period, timeout, and device ID. Verify the settings.
Step 10	**exit**	Exits configuration mode.

Configuring the Software Image and ASDM Image to Boot

By default, the security appliance boots the first software image it finds in internal Flash memory. It also boots the first ASDM image it finds in internal Flash memory, or of none exists there, then in external Flash memory. If you have more than one image, you should specify the image you want to boot. In the case of the ASDM image, if you do not specify the image to boot, even if you have only one image installed, then the security appliance inserts the **asdm image** command into the running configuration. To avoid problems with auto update (if configured), and to avoid the image search at each startup, you should specify the ASDM image you want to boot in the startup configuration.

You must use the **boot system** and **asdm image** commands on your security appliance to point the Flash memory to the version of images that are downloaded using AUS to the device. Otherwise, the existing image on the security appliance is overwritten with the latest version being downloaded from AUS and the update of the ASDM image might fail.

Also, the configuration file that is assigned to a security appliance must point to the same boot software image and ASDM image that are configured on the device. Otherwise, the existing image on the security appliance is overwritten with the latest version being downloaded from AUS.

If you see the following messages on the security appliance, make sure that the ASDM image on the security appliance is compatible with the current version. You can verify this condition by viewing the output of the **show run** command on the device.

```
Auto-update client: Sent DeviceDetails to /autoupdate/AutoUpdateServlet of server
10.1.1.200
Auto-update client: Processing UpdateInfo from server 10.1.1.200
Auto-update client: Failed to contact: https://10.1.1.200/autoupdate/AutoUpdateServlet,
reason: ErrorList error code: CALLHOME-PARSER-ERROR, description: The XML parser
encountered an error: The content of element type "DeviceDetails" must match
"(DeviceID,HostName,PlatformFamily,PlatformType,SerialNumber,SysObjectId,IPAddress+,Versio
nInfo*,Memory*)
```

The following explains how to configure these settings using the device command line. You can also configure these settings in Security Manager using the **Platform > Device Admin > Boot Image/Configuration** policy.

- To configure the software image to boot, enter the following command:

  `hostname(config)# boot system url`

  where *url* is one of the following:

  – {**flash:/** | **disk0:/** | **disk1:/**}[*path*/]*filename*

    The **flash:/** keyword represents the internal Flash memory on the PIX 500 series security appliance. You can enter **flash:/** or **disk0:/** for the internal Flash memory on the ASA 5500 series adaptive security appliance. The **disk1:/** keyword represents the external Flash memory on the ASA.

  – **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*

    This option is only supported for the ASA 5500 series adaptive security appliance.

  You can enter up to four **boot system** command entries to specify different images to boot from in order; the security appliance boots the first image it finds. Only one **boot system tftp:** command can be configured, and it must be the first one configured.

- To configure the ASDM image to boot, enter the following command:

  `hostname(config)# asdm image {flash:/ | disk0:/ | disk1:/}[path/]filename`

INDEX

A

B

C

D

E

F

G

H

I

M

N

P

R

S

T

U