



## CHAPTER 2

# Getting Started With AUS

---

The following topics help you get started with using AUS:

- [Navigating in AUS, page 2-1](#)
- [Understanding the User Interface, page 2-10](#)
- [Setting Up Browser-Server Security, page 2-8](#)
- [Adding Devices to AUS, page 2-13](#)
- [Updating Configuration Files, page 2-14](#)
- [Updating PIX Security Appliance, ASA, ASDM, and PDM Images, page 2-17](#)

## Navigating in AUS

To navigate in AUS, you must log in to the Cisco Security Management Suite desktop or CiscoWorks server desktop. Then you can select the AUS application from the desktop to gain access to AUS functions.

## Logging In to CiscoWorks and Cisco Security Management Suite Home Pages

You can log in to the CiscoWorks and Cisco Security Management Suite home pages in normal mode (HTTP) or Secure Sockets Layer (SSL)-enabled mode (HTTPS).

## Logging In to the CiscoWorks and Cisco Security Management Suite Home Pages in Normal Mode

To log in to the CiscoWorks or Cisco Security Management Suite home page in normal mode, enter the URL for your CiscoWorks server or Cisco Security Management Suite server in your browser:

```
http://server_name:port_number
```

where *server name* is the name of the server and *port number* is the TCP port used by the CiscoWorks server.

The default TCP port for the server is 1741. On Windows, the server always uses the default port numbers.

For more information, see [Logging in to the Cisco Security Management Suite Server, page 2-3](#). See also the *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

**Note**

---

We recommend that you log in to the CiscoWorks or Cisco Security Management Suite home page in normal mode only when you are using the standalone AUS application. If you are integrating AUS with Security Manager, you must enable the browser-security mode on the machine that runs AUS for proper communication to take place between Security Manager and AUS. In a Security Manager-integrated AUS network, log in to the home page in SSL-enabled mode.

---

## Logging In to the CiscoWorks and Cisco Security Management Suite Home Pages in SSL-Enabled Mode

To log in to the CiscoWorks or Cisco Security Management Suite Server home page in SSL-enabled mode:

- 
- Step 1** Enter the URL for your CiscoWorks server or Cisco Security Management Suite Server in your browser.

```
http://server_name:port_number
```

where *server name* is the name of the server and *port number* is the TCP port used by the server.

The default TCP port for the server is 443. On Windows, the server always uses the default port numbers. For more information, see the *Installation and Setup Guide for CiscoWorks Common Services on Windows*.

If you use Microsoft Internet Explorer to log in to the CiscoWorks or Cisco Security Management Suite Server home page, the browser displays a Security Alert window, stating that you are about to view web pages over a secure connection.

- a. Click **OK**. The Security Alert window displays the security certificate alert.
- b. Click **Yes**.

If you use Netscape to log in to the CiscoWorks or Cisco Security Management Suite home page, the browser displays the New Site Certificate wizard.

In the New Site Certificate wizard, you can accept the certificate for the current session or accept it until the certificate expires. To avoid going through the New Site Certificate wizard every time you log in to the home page, accept the certificate until it expires.

If Common Services is running in a plug-in environment, it displays plug-in alerts, for example, server certificate details, hostname mismatch details).

**Step 2** Click **Yes** in a plug-in alert to go to the Login panel.

If the server is in SSL mode, and you enter **http://server\_name:1741**, you are redirected to **https://server\_name:443**.

---

## Logging in to the Cisco Security Management Suite Server

Use the Cisco Security Management or CiscoWorks desktop to log in to AUS.



### Note

If a Cisco Security Management Suite application, such as Security Manager, IPS Manager, or AUS, is installed on your computer and you log in to the security management application from your web browser, the Cisco Security Management Suite home page appears. If none of the Cisco Security Management Suite applications are installed and only network management applications such as RME are installed on your computer, then the CiscoWorks login page appears. You can also launch AUS from the CiscoWorks home page.

---

---

**Step 1** In your web browser, enter **http://SecManServer:1741**, where *SecManServer* is the name of the computer where Cisco Security Management Suite is installed.




---

**Note** If you are using SSL, you are redirected to **https://SecManServer:443**.

---

The Cisco Security Management Suite login screen is displayed. Make sure that that JavaScript and cookies are enabled and that you are running a supported version of your browser. For information on configuring the browser to run Common Services, see the *Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Windows*.

**Step 2** Log into the Cisco Security Management Suite server with the username **admin** and password that you defined during product installation (Figure 2-1).

If you installed CiscoWorks server and are logging in for the first time, use the reserved *admin* user name and password. The CiscoWorks server administrator can set the passwords for admin users during installation. Contact your administrator if you do not know the password. The admin account has full read-write privileges for all tasks and options in AUS or Security Manager GUI.

**Step 3** Click **Login**. You are now logged in to CiscoWorks server.

The Cisco Security Management Suite home page appears.

From this page, you can launch AUS, manage Security Manager, and access other applications installed on the server.

**Step 4** Do one of the following:

- To exit the application, click **Logout** in the upper right corner of the screen.
- Click **About** for information about Cisco Security Management Suite.
- Click **CiscoWorks** to go to the CiscoWorks home page.




---

**Note** To log in to the Cisco Security Management Suite home page from the CiscoWorks desktop, click **Launch CSMS Desktop** in the Cisco Security Management Suite drawer.

---



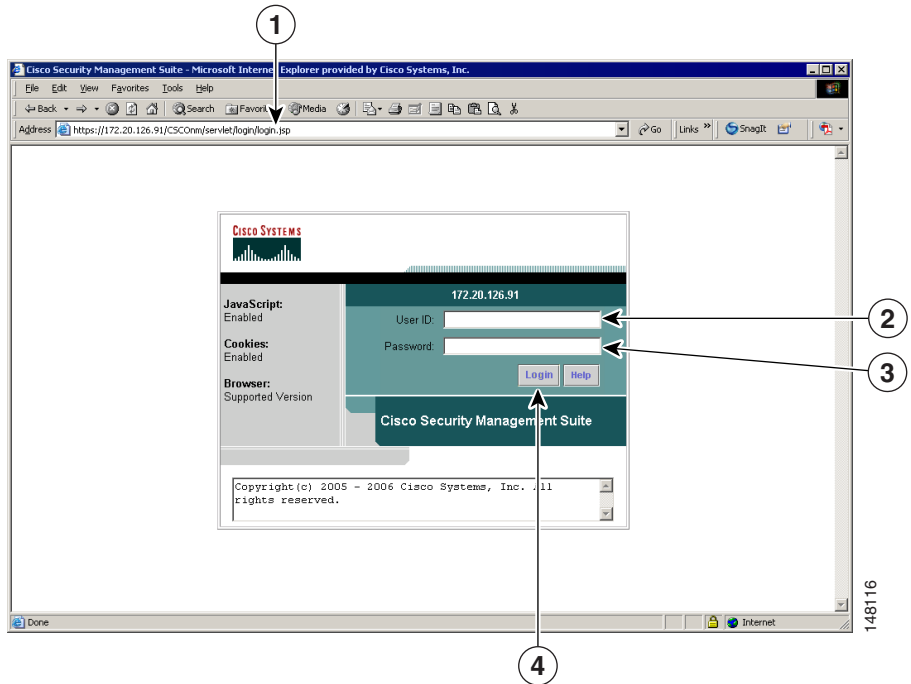
---

This procedure describes how to change the admin password in the CiscoWorks home page.

- 
- Step 1** In the CiscoWorks home page, select **Common Services > Server > Security > Local User Setup**. The Local User Setup page appears.
  - Step 2** Click **Modify My Profile** to modify the admin user profile.
  - Step 3** Enter the password in the Password field. Reenter the password in the Verify field.
  - Step 4** Click **OK** to submit the changes.
- 

For additional information about the CiscoWorks server desktop, see the *User Guide for CiscoWorks Common Services*.

Login sessions time out after 2 hours of inactivity. If the session is not used for 2 hours, you are prompted to log in again. If you try to do any task after timeout, a message tells you that your session has timed out and the Login page appears. After you log in, the page you were working on before the timeout is displayed.

**Figure 2-1 Cisco Security Management Suite Server Login Page**

|          |   |          |                |
|----------|---|----------|----------------|
| <b>1</b> | Address of Cisco Security Management Suite server | <b>3</b> | Login password |
| <b>2</b> | Login name  | <b>4</b> | Login button   |

## Starting and Exiting AUS

The Cisco Security Management Suite home page contains panels for each security management application such as Security Manager, AUS, IPS Manager, and MCP (Figure 2-2).

The CiscoWorks server desktop contains drawers for the installed network and security management applications such as Common Services and AUS (Figure 2-3). The link for launching AUS is in the Auto Update Server drawer.

This procedure tells you how to launch AUS from the Cisco Security Management Suite desktop:

- 
- Step 1** Log in to the Cisco Security Management Server desktop.
  - Step 2** Click the **Auto Update Server** panel. AUS starts.
  - Step 3** To exit AUS, click the close button in the upper right corner of the Auto Update Server window.
- 

**Figure 2-2** Cisco Security Management Suite Desktop

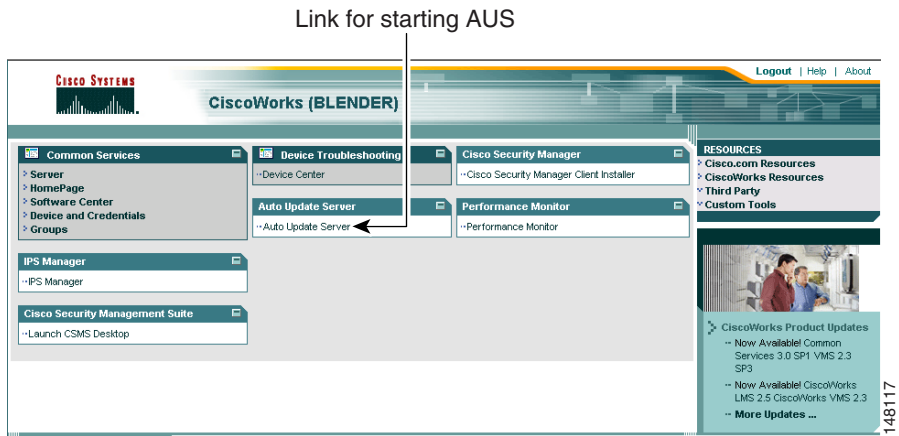


This procedure tells you how to launch AUS from the CiscoWorks desktop:

- 
- Step 1** Log in to the CiscoWorks server desktop.
  - Step 2** (Optional) If the Auto Update Server drawer is not open, click the link in the top right corner of the drawer.
  - Step 3** Select **Auto Update Server** from the Auto Update Server drawer. AUS starts.

- Step 4** To exit AUS, click the close button in the upper right corner of the Auto Update Server window.

**Figure 2-3** CiscoWorks Server Desktop



## 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.

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.

The CiscoWorks server uses certificates for authenticating secure access between the client browser and the management server. The following topics tell you how to enable browser security:

- [Enabling Browser-Server Security from the CiscoWorks Server, page 2-9](#)
- [Enabling Browser-Server Security from the Command Line Interface \(CLI\), page 2-10](#)

## Enabling Browser-Server Security from the CiscoWorks Server

This procedure tells you how to enable browser-server security from the CiscoWorks server.

---

**Step 1** In the CiscoWorks home page, select **Common Services > Server > Security > Browser-Server Security Mode Setup**.

The Browser-Server Security Mode Setup dialog box appears.

**Step 2** Select the **Enable** check box.

**Step 3** Click **Apply**.

**Step 4** Log out from your CiscoWorks session, and close all browser sessions.

**Step 5** Restart the Daemon Manager from the CiscoWorks server CLI:

On Windows:

- a. Enter `net stop crmdmgtd`
- b. Enter `net start crmdmgtd`

**Step 6** Restart the browser, and the CiscoWorks session.

If you do not change the URL from **https** to **http** and the port number from **1741** to **443** when you restart the CiscoWorks session, the CiscoWorks server redirects you automatically. These port numbers are for CiscoWorks server running on Windows.

If another application uses the default port (1741), you can select a different port during installation. For details, see the *Installation and Setup Guide for CiscoWorks Common Services*.

---

## Enabling Browser-Server Security from the Command Line Interface (CLI)

This procedure tells you how to enable browser-server security from the CLI:

- 
- Step 1** Select **Start > Run** from the Windows taskbar. The Run dialog box appears.
  - Step 2** In the Open field, enter **cmd**, then click **OK**. A command prompt window appears.
  - Step 3** Navigate to the directory **NMSROOT\MDC\Apache**.
  - Step 4** Enter **NMSROOT\bin\perl ConfigSSL.pl -enable**
  - Step 5** Press **Enter**.
- 

## Understanding the User Interface

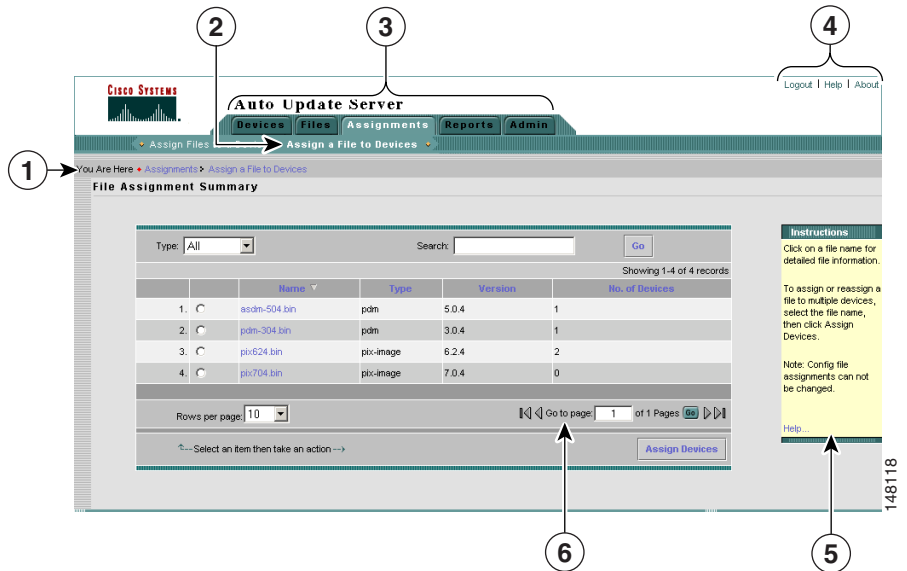
Use the information in these sections to help you understand and navigate the AUS user interface:

- [AUS GUI Elements, page 2-10](#)
- [AUS Table Elements, page 2-12](#)

## AUS GUI Elements

See [Figure 2-4](#) for descriptions of the AUS GUI elements.

Figure 2-4 AUS GUI

Figure 2-4  
Reference

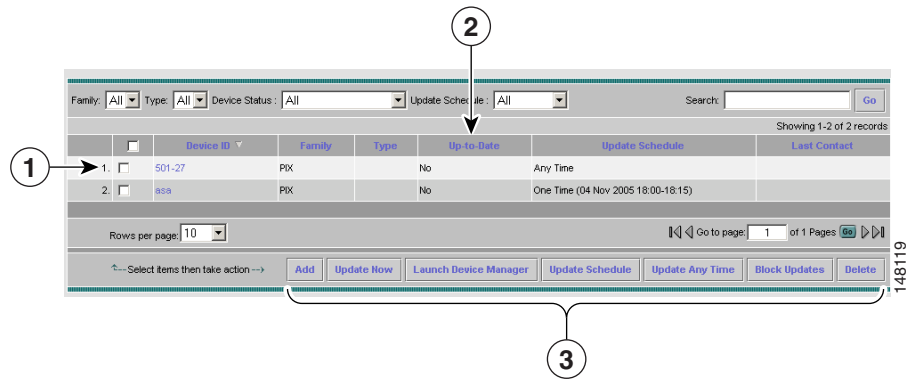
| Reference | Location   | Description   |
|-----------|------------|---|
| 1         | Path bar   | Provides a context for the displayed page. Shows tab, option, and the current page. |
| 2         | Option bar | Displays the options available for the selected tab.                                |

| Figure 2-4<br>Reference | Location         | Description   |
|-------------------------|------------------|---|
| 3                       | Tabs             | <p>Provides access to product functionality. Click a tab to access its options.</p> <ul style="list-style-type: none"> <li>• Devices—Displays summary information about firewall devices.</li> <li>• Images—Displays information about PIX security appliance and ASA software images, PDM and ASDM images, and configuration files and enables you to add and delete PIX security appliance or ASA software images and device manager images.</li> <li>• Assignments—Displays assignment information and enables you to change device-to-image assignments and image-to-device assignments.</li> <li>• Reports—Displays reports.</li> <li>• Admin—Enables you to perform administrative tasks, such as changing your database password.</li> </ul> |
| 4                       | Tools            | <p>Contains the Logout, Help, and About buttons.</p> <ul style="list-style-type: none"> <li>• Logout—Logs you out of CiscoWorks.</li> <li>• Help—Opens a new window that displays context-sensitive help for the displayed page. The window also contains buttons that you use to go to the overall help contents, index, and search tool.</li> <li>• About—Displays the version of the application.</li> </ul>   |
| 5                       | Instructions box | Provides a brief overview of how to use the page.   |
| 6                       | Page             | Displays the area in which you perform application tasks.   |

## AUS Table Elements

Figure 2-5 shows the elements in a typical AUS table.

Figure 2-5 Typical AUS Table



| Reference | Location       | Description  |
|-----------|----------------|--|
| 1         | Row            | Contains information fields for one item in the table.             |
| 2         | Column         | Contains one information field for each item in the table.         |
| 3         | Action buttons | Contains buttons that initiate actions or commands for this table. |

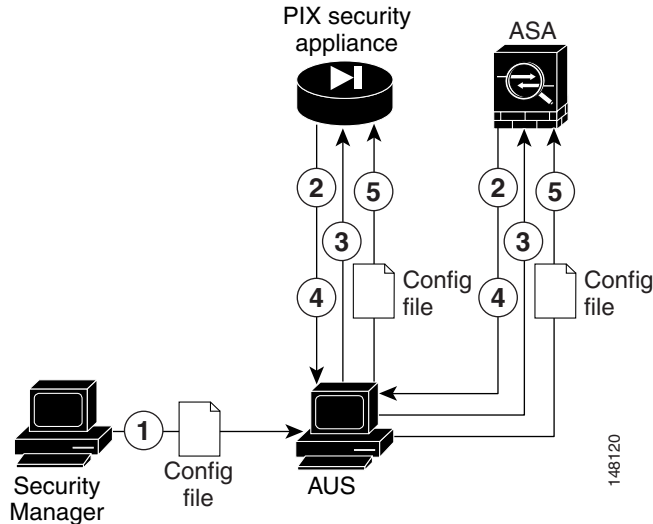
## Adding Devices to AUS

You add devices to AUS primarily through the Security Manager application. To add devices from the Security Manager GUI, see [Adding Devices of Auto Update Type to the Security Manager Inventory, page A-4](#). However, you can also add devices manually from the AUS GUI. For more information, see [Adding a Device Directly to AUS, page 3-5](#).

# Updating Configuration Files

You can update configuration files using Security Manager and deploy the files to AUS.

**Figure 2-6** Updating Configuration Files Using Security Manager and AUS



| <b>Figure 2-6 Reference</b> | <b>Description</b>  |
|-----------------------------|---|
| <b>1</b>                    | Security Manager deploys the PIX security appliance or ASA configuration file to AUS.                     |
| <b>2</b>                    | After the preset polling interval, the PIX security appliance or ASA device contacts the AUS for updates. |

|   |  |
|---|--|
| 3 | The AUS sends a list of image file or configuration file URLs with the checksum or both that the PIX security appliance or ASA device should be running.                         |
| 4 | The PIX security appliance or ASA 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 PIX security appliance or ASA device.  |

This procedure describes how to generate configuration files using Security Manager and deploy them to AUS.

- 
- Step 1** Bootstrap the PIX security appliance or ASA device to operate with AUS. See [Appendix D, “Bootstrapping Devices to Operate with AUS”](#).
- Step 2** From Security Manager, do the following:
- a. Add the PIX security appliance or ASA device to the Security Manager inventory by selecting the **Add New Device** option from the New Device - Choose Method wizard page. For more information, see [Adding Devices of Auto Update Type to the Security Manager Inventory, page A-4](#).  
  
PIX security appliances or ASA devices come from the factory with certain settings already configured. We highly recommend that after you manually add a PIX security appliance or ASA device to Security Manager, you discover (import) the factory-default policies for that device. Importing these policies prevents you from unintentionally removing them the first time you deploy to that device.
  - b. From the New Device - Device Information wizard page, enter the AUS identity information in the appropriate fields to enable the device to be managed by AUS.  
  
You can enter server details such as the hostname, domain name, IP address, username for the server, password used to access the server, the port number for the AUS managed device to use to communicate with the server, and the uniform resource name for AUS.
  - c. Define the security policies you require:
    - Use Device view (select **View > Device View** or click the **Device View** button on the toolbar) to define policies on specific devices.

- Use Policy view (select **View > Policy View** or click the **Policy View** button on the toolbar) to create and manage reusable policies that any number of devices can share. Any change to a shared policy is applied to all devices to which that policy is assigned.




---

**Note** Before you deploy configuration files to AUS, make sure that you use Security Manager to define AUS policy settings if you are unable to discover the AUS policies and settings on your device into Security Manager. To define AUS server access settings from Security Manager, select **Platform > Device Admin > Server Access > AUS** from the Device Policy selector.

---

- d. From the Deploy Saved Changes dialog box, deploy the settings and policies you defined in Security Manager to your devices.

A deployment job defines how configuration changes are sent to devices. Security Manager translates policy configurations for each device into CLI commands, which you can preview and then deploy to devices. After you deploy jobs, you can track their success or failure from the Deployment Manager page.




---

**Note** See the *User Guide for Cisco Security Manager 3.1* for details.

---

Security Manager sends the configuration file to AUS. After the preset polling interval, the PIX security appliance or ASA device contacts AUS and downloads the new configuration file. These actions take place without user intervention. See [Figure 2-6](#).

- Step 3** Confirm that the configurations were updated. Display the Event Report to see information about devices that contacted AUS. See [Viewing the Event Report, page 6-3](#).




---

**Note** 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 B, “Troubleshooting AUS.”](#)

---

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

You can update PIX security appliance software, ASA software, ASDM, and PDM images using AUS without using Security Manager.

**Caution**

---

Make sure the new PIX security appliance or ASA software image will work with the configuration file running on the device. If an incompatible PIX security appliance or ASA image is downloaded, the PIX security appliance or ASA device will drop all unsupported commands and might experience configuration errors.

Make sure that the new PDM or ASDM image will work with the existing security appliance image running on the device. If an incompatible PDM or ASDM image is downloaded, PDM or ASDM might not start.

---

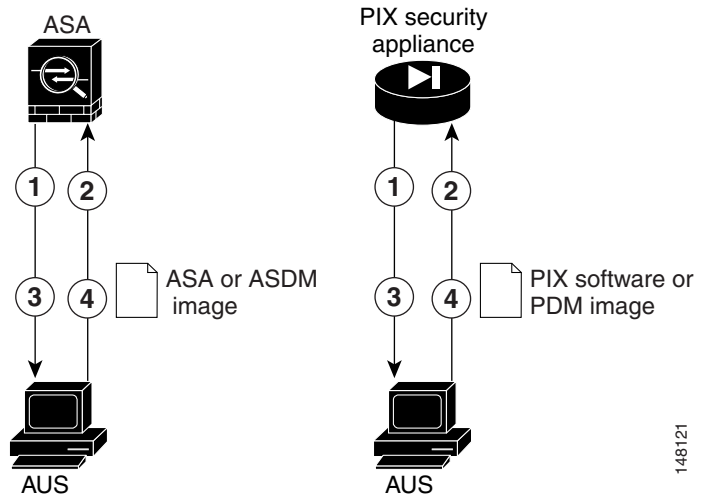
**Note**

---

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 D-4.

---

**Figure 2-7** Updating PIX Security Appliance, ASA, ASDM, and PDM Images Using AUS



148121

| <b>Figure 2-7 Reference</b> | <b>Description</b>   |
|-----------------------------|--|
| <b>1</b>                    | At the preset polling interval, the PIX security appliance or ASA device contacts the AUS for updates.   |
| <b>2</b>                    | The AUS sends a list of image files or configuration files or both that the PIX security appliance or ASA device should be running.  |
| <b>3</b>                    | The AUS sends a list of image file or configuration file URLs with the checksum or both that the PIX security appliance or ASA device should be running.                         |
| <b>4</b>                    | The PIX security appliance or ASA 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. |

This procedure describes how to update PIX security appliance, ASA, PDM, and ASDM images.

---

**Step 1** Bootstrap the PIX security appliance or ASA device to operate with AUS. See [Appendix D, “Bootstrapping Devices to Operate with AUS”](#).

**Step 2** Add the image to AUS. For details, see [Adding Software Images, page 4-2](#).

**Step 3** 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 5-4](#).

To assign the file to multiple devices, see [Assigning and Unassigning a File to Multiple Devices, page 5-7](#).

After the preset polling interval, the security appliance contacts the AUS and downloads the new security appliance, ASDM, or PDM image. These actions take place without user intervention. See [Figure 2-7](#).

After you update a PIX security appliance or ASA software image, the PIX security appliance or the ASA 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 D-1](#).

**Step 4** Confirm that the configurations were updated. Display the Event Report to see information about devices that contacted AUS. See [Viewing the Event Report, page 6-3](#).



---

**Note** 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 B, “Troubleshooting AUS.”](#)

---

