



CHAPTER 3

Viewing Device Summary Information

You click the Devices tab to display the Device Summary page. This page shows all managed devices and contains information about the devices, such as the device ID, platform family, platform 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, request the Auto Update Immediate feature, configure and change update schedules, and launch the PIX Device Manager (PDM) or Adaptive Security Device Manager (ASDM) application.

These topics help you understand and use the Device Summary page:

- [Viewing the Device Summary Page, page 3-1](#)
- [Adding a Device Directly to AUS, page 3-6](#)
- [Configuring the Update Type, page 3-8](#)
- [Canceling the Update Type, page 3-10](#)
- [Deleting Devices, page 3-11](#)
- [Requesting an Auto Update, page 3-12](#)
- [Disabling Auto Updates, page 3-13](#)
- [Launching Device Manager, page 3-14](#)

Viewing the Device Summary Page

To view information in the Device Summary table, click a column name to sort the table by column information. For a description of elements in the Device Summary table, see [Table 3-1](#)

Table 3-1 **Device Summary Page**

Element	Description
Family	Shows the series to which a device belongs, for example, PIX or IDS. You can select the family from the list to filter the table according to family.
Type	Shows the type of device in a family, for example, PIX. You can select the type from the list to filter the table according to type. The options available in the Type list correspond to the family specified in the Family list. Note The family type will be displayed as PIX for both PIX security appliance and ASA devices. You can differentiate between the two by seeing the device model type.
Device Status	Shows the status of the device. You can select the device status from the list to filter the table according to device status. Options are: <ul style="list-style-type: none"> • All—Lists all devices in the AUS database. • Not Up-to-Date—Lists only devices that are not running the latest files deployed to AUS. • Up-to-date—Lists only devices that are running the latest files received from AUS. • Not Applicable (NA)—Lists all devices with a status other than Not Up-to-Date, Up-to-date, and Not Contacted AUS. • Not Contacted AUS—Lists only devices that have never contacted AUS.
Search button	Enables you to enter the ID of the device for which you want to search.
Go button	Begins a search for the information entered in the Search field.
Check box	Selects the device on which to perform a function.

Table 3-1 *Device Summary Page (continued)*

Element	Description
Device ID	Shows the name that the device uses when identifying itself to AUS, which might differ from the hostname. You can click on an entry in the Device ID column to open a window with a table that shows details and associated files for that particular device ID. See Device ID Popup Window, page 3-4 .
Family	Shows the family to which the device belongs, for example, PIX. Note The family type will be displayed as PIX for both PIX security appliance and ASA devices. You can differentiate between the two by seeing the device model type.
Type	Shows the type of device in a family, for example, PIX-535 or ASA-5540.
Up-to-Date	Shows if the device is running the newest files.
Update Type	Shows the method by which a device is scheduled to receive updated files. <ul style="list-style-type: none"> Any Time—Device is updated according to set polling information. Default is 720 minutes. One Time—Device is updated only once based on a user-defined time and date. Daily—Device is updated every day based on a user-defined time and day. Weekly—Device is updated every week based on a user-defined time and date. Never—Device is never updated.

Table 3-1 Device Summary Page (continued)

Element	Description
Allow Update on	Lists the days of the week. The update occurs on the selected day immediately following the user-defined start date. Note This setting is used only when you want to configure a weekly update for a device.
Last Contact	Shows the last time the device contacted AUS.
Rows per page	Specifies the number of rows per page you want displayed.
Add button	Enables you to add a device to the table.
Update Now button	Requests that a device immediately contact AUS (Auto Update Immediate feature).
Launch Device Manager button	Launches PDM or ASDM, depending on the device, and enables you to view or modify settings on a device.
Update Schedule button	Enables you to configure an update schedule for a device.
Update Any Time button	Cancels an existing update schedule for a device and replaces it with the default Any Time, which updates the device based on the device polling settings.
Block Updates	Disables auto updates for selected devices.
Delete button	Deletes a device from the table.

Device ID Popup Window

Use the Device ID popup window to view specific device information. To access the Device ID popup window, simply click a device ID in the Device Summary page.

Table 3-2 **Device ID Popup Window**

Element	Description
Device ID	Displays the unique identification number that the device uses when identifying itself to AUS, which might be different from the hostname.
Device Name	Displays the DNS hostname of the device. When you enter the hostname, the same name is automatically entered in the Display Name field. If you edit the display name and enter a unique name for the device, the modified name is displayed in this field.
Family	Displays the family to which the device belongs, for example, PIX or ASA.
Type	Displays the type of device in a family, for example, PIX-535 or ASA-5540.
IP Address	Displays the management IP address of the device.
Serial Number	Displays the serial number of the device.
Auto Update Timestamp	Displays the time that the device last contacted AUS for new information.
SysObjectId	Displays the system object IDs for the device type you selected.
Current PDM Version	Displays which PDM or ASDM image is assigned to the device, if any.
Current PIX Image Version	Displays which PIX image is assigned to the device, if any.
Memory (bytes)	Displays the available RAM and flash memory on the device.

Adding a Device Directly to AUS

You can add devices directly to AUS for troubleshooting purposes.



Note

To add a device to AUS from the Security Manager GUI, see [Adding Devices of Auto Update Type to the Security Manager Inventory](#), page A-4.

If you add devices to AUS directly, the devices are not added to the Security Manager inventory and are therefore not listed in the Security Manager GUI.

This procedure describes how to add a device directly to AUS.

-
- Step 1** Select **Devices**. The Device Summary page appears.
 - Step 2** Click **Add**. The Add Device page appears.
 - Step 3** Enter information in the fields ([Table 3-3](#)).
 - Step 4** Click **OK** to add the device. Click **Cancel** to exit the page without making any changes.
-

Table 3-3 **Add Device Page**

Element	Description
Device ID	Unique number that identifies the device with AUS.
Auto Update Username	Name that the device uses to authenticate with AUS.
Auto Update Password	Password that the device uses to authenticate with AUS.

Table 3-3 Add Device Page (continued)

Element	Description
Request Auto Update Credentials	<p>Click the radio button corresponding to the credentials the device uses to authenticate AUS:</p> <ul style="list-style-type: none"> • None—No credentials are used. • TACACS—(Optional) Enter the TACACS username and TACACS password in the appropriate fields. Required for Auto Update Immediate and AAA authentication to function. • Enable Password—(Optional) Enter the password that activates enable mode on a security appliance, if enable mode is configured on that device, in the appropriate field. Required for Auto Update Immediate feature to function.

The enable password that you enter while adding a device to AUS is the credential that the device uses to authenticate AUS when the device needs to contact AUS immediately for updates or when the device manager needs to be launched. If you add an AUS-managed device from Security Manager, the enable password that you enter for the device in the primary credentials section of the Device Credentials wizard page is the same as the enable password that you enter on the Add Device page from AUS. When you add an AUS-managed device to Security Manager, you must enter the username and password in the primary credentials section if you want to perform a discovery of the settings that exist on the device. Otherwise, you can leave them blank.

**Note**

The TACACS username and password that you enter in the Add Device Page from AUS do not have an equivalent setting when you add a device from Security Manager.

The credentials that a device requires when it needs to contact AUS for updates comprise the username and password that you enter while bootstrapping the device or using the AUS server access settings policy under the Device Administration section of the Security Manager GUI.

If you discover policies and settings that exist on the device, the username and password that you entered on the device are displayed in the Username and Password fields of the AUS page under the server access settings section in the Security Manager GUI. These credentials are also displayed in the Auto Update Username and Auto Update Password fields of the Add Device Page in the AUS GUI after you deploy the configuration from Security Manager to AUS.

Configuring the Update Type

To help you maintain your configuration files and keep your devices current, AUS provides you with different methods for scheduling configuration updates.

- Any Time—(Default) Enables you to update devices according to user-defined polling information. You configure polling when you bootstrap the PIX security appliance or ASA device; however, you can change the polling setting any time with Security Manager. To change the polling setting, see [Changing the Polling Interval for the Device to Contact AUS, page 3-9](#). The default is 720 minutes.
- One Time—Enables you to schedule an update for devices based on a user-defined time and date. The updates occur only once.
- Daily—Enables you to schedule ongoing, daily updates for devices based on a user-defined date and time.
- Weekly—Enables you to schedule ongoing, weekly updates for devices based on a user-defined day and start time.
- Never—Ignores any update schedule. Selecting the update type as Never is the same as clicking Block Updates on the Device Summary page. For more information, see [Disabling Auto Updates, page 3-13](#).

If you scheduled auto updates for a device and later configure that device to contact AUS immediately for updates, then the Auto Update Immediate request feature takes precedence over the configured auto update schedule. For example, if you configure a device to receive updates every Monday from 10:00 p.m. to 11:00 p.m. (2200 to 2300) but want to instantaneously upgrade the image running on the device with the latest version on some other day of the week, you can use the Auto Update Immediate feature to ensure that the device downloads the latest software image file.

This procedure describes how to schedule an auto update.

-
- Step 1** Select **Devices**. The Device Summary page appears.
- 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 appropriate radio button from the list of update options.
- If you selected Daily or Weekly, go to [Step 6](#).
 - If you selected Any Time or Never, go to [Step 9](#).
 - For all other update types, go to [Step 5](#).
- Step 5** Enter the start date for the update.
- Step 6** Enter the start time in HH:MM format. By default, the start time is midnight.
- Step 7** Enter the length of time that the update session should be in effect in HH:MM format. By default, the duration is 15 minutes.
- If you selected Daily or One Time, go to [Step 9](#).
 - If you selected Weekly, go to [Step 8](#).
- Step 8** Select the appropriate radio button to denote the day of the week that you want the update to occur.
- Step 9** Click **OK**. You are returned to the Device Summary Page.
- The update is scheduled and the date and time are shown in the Update Type column. Updated schedule information is shown in the Events report. For more information, see [Viewing the Event Report, page 6-3](#).
-

Changing the Polling Interval for the Device to Contact AUS

From Security Manager, you can use the AUS page to change the number of minutes the firewall device should wait to poll AUS for new information. The AUS page enables you to configure a firewall device to be managed remotely from a server that supports the Auto Update specification. Auto Update enables you to apply configuration changes to the firewall device and receive software updates from a remote location.

To open this page from the Device view

1. Click the **Device View** button on the toolbar.
2. Select the firewall device for which you want to configure an AUS policy from the Devices selector.
3. Select **Platform > Device Admin > Server Access > AUS** from the Devices selector. The AUS page is displayed.

To open this page from the Policy view

1. Click the **Policy View** button on the toolbar.
2. Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > AUS** from the Policy Types selector.
3. Right-click **AUS** and select **New AUS Policy**, or select an existing AUS policy from the Policies selector. The AUS page is displayed.

In the Poll Period (min) field, change the number of minutes the firewall device should wait to poll AUS.

Canceling the Update Type

You might want to cancel a scheduled update for a device. For example, perhaps you want to update the configuration file on a device this evening instead of waiting for the weekly update. To do this, you must reconfigure the existing schedule using the Configure Update window by specifying the start time and duration of update session, as only one schedule is allowed for any device.

**Note**

If a device on your network imposes a security risk and you want to update the device immediately, you might be able to use the Request Auto Update feature. To see if this feature is supported on the device and to identify configuration requirements, see [Requesting an Auto Update, page 3-12](#).

If, however, you scheduled a weekly update to occur on a device and you want to change the schedule to match the polling time set on the device, simply select the device, then click **Update Any Time**.



Note If you remove a device from AUS, any update schedule assigned to the device is automatically canceled.

This procedure describes how to cancel a scheduled auto update for one or more devices.

Step 1 Select **Devices**. The Device Summary page appears.

Step 2 Select the device for which to cancel a scheduled update.



Note You can cancel the update schedule for more than one device by selecting the check boxes next to the devices for which you want to cancel an auto update.

Step 3 Click **Update Any Time**. A confirmation window is displayed.

Step 4 Click **OK** to exit and return to the Device Summary page.

The schedule for the device is shown as Any Time in the Update Type column, which uses the default PIX security appliance or ASA device polling setting for that device.

You can either keep the default setting or reconfigure the update schedule for the device. For more information, see [Configuring the Update Type, page 3-8](#).

Updated schedule information is shown in the Events report.

Deleting Devices

If you add the device to the Security Manager inventory and deploy it to AUS, you must delete it from Security Manager and AUS separately. For more information on deleting devices from the Security Manager inventory that are managed by AUS, see the *User Guide for Cisco Security Manager 3.2*.

If you added the device directly to AUS, you must delete it from AUS and DCR separately.

This procedure describes how to delete one or more devices from AUS.

-
- Step 1** Select **Devices**. The Device Summary page appears.
 - Step 2** Select the check boxes next to the devices to delete.
 - Step 3** Click **Delete**. A confirmation page is displayed.
 - Step 4** Click **OK**.
-

Requesting an Auto Update

Sometimes, you might want to request that a device immediately contact AUS to ensure that your devices have the newest files running on them, instead of waiting for the device to contact AUS at the specified interval. This is called the Auto Update Immediate feature. For example, you might want to request that a device contact AUS if the security of your network has been compromised.

**Note**

If you scheduled auto updates for a device and you want the device to contact AUS immediately to ensure that the latest software images are running on them, click the **Update Now** button to cause the device to contact AUS now for updates. However, if you set the update schedule type as Never or blocked auto updates, then the Auto Update Immediate feature does not take effect.

**Note**

If you change the HTTPS port number on the device to any port number other than the default value of 443, the Auto Update Immediate feature does not work. 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.

**Caution**

Requesting that a large number of devices immediately contact AUS can result in performance problems.

This procedure describes how to enable a device to request auto updates from AUS immediately.

Before You Begin

- You must configure TACACS or Enable Password credentials on the device. See [Adding a Device Directly to AUS, page 3-6](#).
- The device must be directly addressable (not behind a NAT boundary).
- The device must have contacted AUS previously.

-
- Step 1** Select **Devices**. The Device Summary page appears.
- Step 2** Select the check box next to the device that should contact AUS.
- Step 3** Click **Update Now**. The Request Auto Update Confirmation dialog box appears. Click the Event Report link in the dialog box to open the Event Report and view information about your request. See the [Viewing the Event Report, page 6-3](#) for more information about the Event Report.
- Step 4** Click **OK** to exit the page and return to the Device Summary page.
-

Disabling Auto Updates

You can disable auto updates for selected devices.

This procedure describes how to disable auto updates for one or more devices.

-
- Step 1** Select **Devices**. The Device Summary page appears.
- Step 2** Select the check box next to the device for which you want to disable auto updates.



Note You can disable auto updates on more than one device by selecting the check boxes next to the devices.

- Step 3** Click **Block Updates**. A confirmation window is displayed.

Step 4 Click **OK** to exit and return to the Device Summary page.

The schedule for the device is shown as Never in the Update Schedule column, which means that auto updates will not occur on that device.

Launching Device Manager

You can launch PDM or ASDM to view or modify a particular setting on a device.



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.

For more information on how to launch device manager from Security Manager for devices not managed by AUS, see the *User Guide for Cisco Security Manager 3.2*.



Caution

Consider potential security implications before allowing PDM or ASDM access on the network. An intruder could connect to a device through PDM or ASDM and compromise the device or network. You might consider turning off or limiting web server services on the device to prevent unwanted access to the device. For details, see [Bootstrapping Security Appliances, page D-1](#).

This procedure describes how to launch a device manager.

Before You Begin

- Make sure that the PIX security appliance and ASA devices have access to PDM or ASDM on the network.
 - Make sure that the device has contacted AUS previously.
-

Step 1 Select **Devices**. The Device Summary page appears.

- Step 2** Click the check box next to the device for which you want to launch PDM or ASDM.



Note You can launch PDM or ASDM on only one device at a time.

- Step 3** Click **Launch Device Manager**. When prompted for a login, enter the username and password. A new window opens and PDM starts. For information about PDM and ASDM, see the PIX Device Manager and Adaptive Security Device Manager documentation.
-

■ **Launching Device Manager**