CHAPTER 2

Managing Devices and Update Schedules

The Device tab 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

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, 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.

Table 2-1 Device Summary Page (continued)

Element	Description
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.
Update Schedule button	Click this button configure an update schedule for a device. For more information, see Configuring Update Schedules, page 2-4.

Table 2-1 Device Summary Page (continued)

Element	Description
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 **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 **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 **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 **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 **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 **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 **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.