APPENDIX C

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`