



APPENDIX **D**

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, page D-1](#)
- [Bootstrapping CNS Devices, page D-6](#)

Bootstrapping Security Appliances

Before you can manage a PIX security appliance or an ASA device using AUS, you must set up the PIX security appliance or ASA device with a minimum configuration that provides basic connectivity. See the *User Guide for Cisco Security Manager 3.2* 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 PIX security appliance or ASA device command line interface.



Note

You can also use the PIX Firewall Device Manager (PDM) Setup wizard to configure the PIX security appliance running PIX security appliance software version 6.3. See PDM documentation for more information. Use the Adaptive

Security Device Manager (ASDM) Startup Wizard to configure PIX security appliance running PIX security appliance software version 7.0 and ASA devices. See ASA and ASDM 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 D-4.

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

	Command	Purpose
Step 1	enable <i>password</i>	Enters privileged mode from which you can configure the PIX security appliance and ASA devices.
Step 2	config terminal	Enters configuration mode from the terminal.
Step 3	http server enable	Enables the PIX security appliance or ASA device to be monitored or have its configuration modified from a browser.
Step 4	http <i>ip_address</i> [<i>netmask</i>] [<i>if_name</i>]	<p>Specifies the host or network authorized to initiate an HTTP connection to the PIX security appliance or ASA device.</p> <ul style="list-style-type: none"> <i>ip_address</i> - IP address of the host or network authorized to initiate an HTTP connection to the PIX security appliance and ASA devices. <i>netmask</i> - Network mask for the <i>http ip_address</i>. <i>if_name</i> - PIX security appliance or ASA interface name on which the host or network initiating the HTTP connection resides. <p>Note This setting must be configured for the Auto Update Immediate feature to work.</p>

	Command	Purpose
Step 5	auto-update server https://username: <i>password@AUSserver_</i> <i>IP_address:port/</i> autoupdate/AutoUpdateServlet	Connects the device to AUS. <ul style="list-style-type: none"> • <i>username</i>—Login name used to enter the CiscoWorks2000 Server. • <i>password</i>—Password used to enter the CiscoWorks2000 Server. • <i>AUSserver_IP_address</i>—IP address of the AUS server. • <i>port</i>—Port number of the AUS server. Number is typically 443.
Step 6	auto-update poll-period <i>poll_period</i> <i>[retry_count]</i> <i>[retry_period]</i>	Changes the polling period for AUS. <ul style="list-style-type: none"> • <i>poll_period</i>—Period in minutes between poll updates. Default is 720 minutes (12 hours). • <i>retry_count</i>—Number of times to retry if unable to connect to server. Default is 0. (Optional) • <i>retry_period</i>—Time, in minutes, between retries. Default is 5. (Optional)
Step 7	auto-update device-id hardware-serial_ip hostname ip_address <i>[if_name mac-address</i> <i>[if_name] string text]</i>	Configures the device to use the specified device ID to identify itself. <ul style="list-style-type: none"> • <i>if_name</i>—The interface name. • <i>text</i>—Text that identifies the device. <p>Because a PIX security appliance or an ASA device might have more than one interface, the assigned device ID could be the IP address or MAC address of one of the interfaces.</p> <p>In the following example, “outside” is the name of the outside interface of and the device ID is the IP address of that outside interface.</p> <pre>auto-update device-id ipaddress outside</pre>

	Command	Purpose
Step 8	<code>http ip_address [netmask] [if_name]</code>	<p>(Optional) Use this command if you plan to use the Launch Device Manager feature and you want to limit HTTP access to the device for security purposes. Enter this command for each host you want to allow HTTP access.</p> <ul style="list-style-type: none"> <i>ip_address</i>—The host or network authorized to initiate an HTTP connection to the PIX security appliance and ASA devices. <i>netmask</i>—The network mask for the <code>http ip_address</code>. <i>if_name</i>—PIX security appliance or ASA device interface name on which the host or network initiating the HTTP connection resides. <p>In the following example, the host with IP address 10.10.10.10 is permitted access to the device's web server through the outside interface:</p> <pre>http 10.10.10.10 255.255.255.255 outside</pre> <p> Caution We do not recommend that you configure the device with <code>http 0.0.0.0 0.0.0.0 outside</code>. This will allow any external host to connect to your device through the web server.</p>
Step 9	<code>write memory</code>	Stores the current configuration in Flash memory.
Step 10	<code>show auto-update</code>	Shows the AUS URL, poll period, timeout, and device ID. Make sure that the settings match those you entered. If necessary, make any modifications.
Step 11	<code>exit</code>	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 if 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 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,SysObject
Id,IPAddress+,VersionInfo*,Memory*)
```

- 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
```

Bootstrapping CNS Devices

To use AUS and the CNS Event Gateway feature with Security Manager, you must enable and configure CNS services on CNS devices. Use the command line interface from a console terminal connected to the device console port. The following tables describes the tasks to complete before you use CNS as the transport protocol for device management on Cisco IOS routers.



Note

For Cisco IOS routers configured with dynamic IP addresses and associated with the CNS gateway protocol running on AUS, you must configure CNS in event-bus mode on the routers. See the *User Guide for Cisco Security Manager 3.2* for details about setting up basic connectivity.

You can also configure additional CNS Event Gateways to retrieve IP addresses from a large number of Cisco IOS routers managed by Security Manager. For more information, see [Support for Additional IOS Devices to be Managed by the CNS Event Gateway, page D-10](#).

	Command	Purpose
Step 1	<code>enable password</code>	Enters privileged mode from which you can configure the PIX security appliance or ASA device.
Step 2	<code>config terminal</code>	Enters configuration mode from the terminal.

	Command	Purpose
Step 3	cns config partial <i>ip_address</i>	Enables the config agent on the device so that AUS gets the connect and disconnect messages it needs. <ul style="list-style-type: none"> <i>ip_address</i>—IP address of AUS.
Step 4	cns event <i>ip-address</i> [<i>port-number</i>] [keepalive <i>seconds</i> <i>retry-count</i>]	Configures the device to communicate with the event gateway. <ul style="list-style-type: none"> <i>ip_address</i>—IP address of AUS. <i>port-number</i>—Port number device uses to subscribe to the correct events. Use the default, 11011 with no encryption. <i>seconds</i>—Keepalive timeout. Default is 0. <i>retry-count</i>—Number of retries. Default is 0.
Step 5	cns exec [<i>port-number</i>]	Enables and configures the CNS execute agent. The default port number is 80.

Command	Purpose
<p>Step 6 <code>cns id</code> <i>type number</i> {<code>dns-reverse</code> <code>ipaddress</code> <code>mac-address</code>} [<code>event</code>]</p> <p>or</p> <p><code>cns id</code> {<code>hardware-serial</code> <code>hostname</code> <code>string</code> <i>string</i>} [<code>event</code>]</p>	<p>The default (hostname) is recommended for use with AUS. However, you can change the unique event ID to something other than the default.</p> <p>The first command sets the unique event ID to the IP address or MAC address.</p> <ul style="list-style-type: none"> • <i>type number</i>—Type of interface (for example, Ethernet, group-async, loopback, or virtual-template) and the interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID. • dns-reverse—(Optional) Uses DNS reverse lookup to retrieve the hostname and assign it as the unique ID. • ipaddress—(Optional) Uses the IP address specified in the type number arguments as the unique ID. • mac-address—(Optional) Uses the MAC address specified in the type number arguments as the unique ID. • event —Sets this ID to be the event ID value, which identifies the router for CNS event services. If omitted, sets it to be the config ID value, which identifies the router for CNS configuration services. <p>The second command sets the unique event ID to the hardware serial number, hostname, or a string.</p> <ul style="list-style-type: none"> • hardware-serial—(Optional) Uses the hardware serial number as the unique ID. • hostname—(Optional) Uses the hostname as the unique ID. This is the system default. • string <i>string</i>—(Optional) Uses an arbitrary text string—typically the hostname—as the unique ID. • event—Sets this ID to be the event ID value, used to identify the router for CNS event services. If omitted, sets it to be the config ID value, which identifies the router for CNS configuration services.

	Command	Purpose
Step 7	<code>router1(config)# cns password <password></code>	<p>Sets the CNS password.</p> <ul style="list-style-type: none"> • <password> - The password you want to set on the router. <p>You can set the CNS password to callhome (which is the default bootstrap password in AUS) or you can set a different password.</p> <p>If you set a different password on the router, you must change the default CNS bootstrap password in AUS. For instructions, see Changing the Default CNS Bootstrap Password in AUS, page D-9.</p> <p>Note For information on how to authenticate a Cisco IOS router on a Configuration Engine, see the <i>Cisco CNS Configuration Engine Administrator Guide</i>.</p>
Step 8	<code>write memory</code>	Stores the current configuration in Flash memory.
Step 9	<code>show cns event connections</code>	Displays the status of the event agent connection, such as whether it is connecting to the gateway, connected, or active. Also displays the gateway used by the event agent and its IP address and port number.
Step 10	<code>exit</code>	Exits configuration mode.

Changing the Default CNS Bootstrap Password in AUS

If you changed the CNS password on a Cisco IOS router, you must change the password in the AUS also.

The default CNS bootstrap password configured in an AUS is **callhome**. If you changed the CNS password on the router, you must change the default CNS bootstrap password in the AUS also.

This procedure describes how to change the default CNS bootstrap password in an AUS.

-
- Step 1** Open the Windows command prompt on the machine where you installed AUS.
- Step 2** Navigate to the directory `..\CSCOpX\MDC\autoupdate\bin\eventgateway`. For example, enter `cd C:\Progra~1\CSCOpX\MDC\autoupdate\bin\eventgateway` if `C:\Progra~1\CSCOpX\` is the directory where you installed AUS.
- Step 3** Enter `cnspassword.pl <password>`.
 where `<password>` is the same CNS password you set on the device.
 The Perl executable file must be in a directory defined in the `$PATH` environment variable. Otherwise, issue the command from the directory where perl was installed. For example, enter `C:\Progra~1\CSCOpX\bin\perl cnspassword.pl <password>`
- Step 4** Restart the Daemon Manager if it is running.
-

Support for Additional IOS Devices to be Managed by the CNS Event Gateway

The number of Cisco IOS devices that can be served by the CNS Event Gateway in releases of AUS earlier than 3.0.2 and AUS 3.1 was limited to 500. This restriction posed a problem in managing a large number of IOS devices. In AUS 3.0.2 and later in the 3.0.x train, AUS 3.1.1 and later in the 3.1.x train, and AUS 3.2, you can register additional event gateways to the gateway list using a perl script and configure the devices to communicate with the event gateway. This method enables you to increase the number of devices that can be managed by the CNS Event Gateway.

To register a CNS Event Gateway, follow these steps:

-
- Step 1** Open the Windows command prompt on the machine where you installed AUS.
- Step 2** Navigate to the directory `NMSROOT\CSCOpX\MDC\autoupdate\bin`, where `NMSROOT` is the AUS installation directory. For example, enter `cd C:\Progra~1\CSCOpX\MDC\autoupdate\bin` if `C:\Progra~1\CSCOpX\` is the directory where you installed AUS.

Step 3 Enter **regEventGateway.pl** *<CNSEventGatewayName>* *<port_number>*

where:

- *<CNSEventGatewayName>* is the name of the event gateway and must be unique.
- *<port_number>* is the port number on which the event gateway listens for event updates from IOS devices. This port number must be greater than 11011 and must be an odd number.

If the CNS Event Gateway name is not unique, an error message is displayed and the perl script exits. If the port number you specify is already in use by another event gateway, an error message is displayed when you run the script.

After you register a new CNS Event Gateway, you must configure the device to communicate with the gateway using the **cns event** *ip-address port-number* command

where:

- *ip_address* is the IP address of AUS.
- *port-number* is the port number that the device uses to subscribe to the correct events. Use the default, 11011, with no encryption.

To unregister a CNS Event Gateway, follow these steps:

Step 1 Open the Windows command prompt on the machine where you installed AUS.

Step 2 Navigate to the directory *NMSROOT\MDC\autoupdate\bin*, where *NMSROOT* is the AUS installation directory. For example, enter **cd C:\Progra~1\CSCOpX\MDC\autoupdate\bin** if *C:\Progra~1\CSCOpX* is the directory where you installed AUS.

Step 3 Enter **unregEventGateway.pl** *<CNSEventGatewayName>*

where *<CNSEventGatewayName>* is the name of the event gateway and must be unique.

CNSEventGateway is the name of the default event gateway process and cannot be unregistered.
