



## CHAPTER 5

# Preparing Devices for Management

---

Before you start to manage a device using Security Manager, you should prepare the device with at least a minimal configuration. The following sections describe the basic device configurations needed for various transport protocols or device types. Before configuring transport protocols, determine the requirements for your devices by reading [Understanding Device Communication Requirements, page 5-1](#).

- [Understanding Device Communication Requirements, page 5-1](#)
- [Setting Up SSL, page 5-4](#)
- [Setting Up SSH, page 5-9](#)
- [Setting Up AUS, page 5-13](#)
- [Setting Up CNS, page 5-16](#)
- [Setting Up TMS, page 5-22](#)
- [Initializing IPS Devices, page 5-23](#)

## Understanding Device Communication Requirements

Security Manager provides many different ways for you to manage devices. The easiest methods involve Security Manager directly contacting the devices. Security Manager might access a device during inventory or policy discovery, during configuration deployment, or in response to actions you take in Security Manager that request device contact (such as testing connectivity).

Because you can use off-line methods to add devices to the Security Manager inventory or to deploy configuration changes to the devices, configuring device communication settings for Security Manager's use is optional. However, you typically need to configure basic device communication settings on the devices to implement your off-line or customized configuration deployment tools.

In Security Manager, you can configure which transport protocol to use as the default for a type of device, and change it for specific devices that are configured to respond to a different protocol. Security Manager is configured with default protocols that are the most commonly-used protocols for that type of device. To change the default device communication setting for a type of device, select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents (for more information, see [Device Communication Page, page A-14](#)). To change the transport setting for a specific device, modify its device properties as described in [Viewing or Changing Device Properties, page 6-23](#).

Security Manager can use these transport protocols:

- **SSL (HTTPS)**—Secure Socket Layer, which is an HTTPS connection, is the only transport protocol used with PIX Firewalls, Adaptive Security Appliances (ASA), and Firewall Services Modules (FWSM). It is also the default protocol for IPS devices and for routers running Cisco IOS Software release 12.3 or higher.

If you use SSL as the transport protocol on Cisco IOS routers, you must also configure SSH on the routers. Security Manager uses SSH connections to handle interactive command deployments during SSL deployments.



---

**Note** DES encryption is not supported on Common Services 3.0 and later. Ensure that all PIX Firewalls and Adaptive Security Appliances that you intend to manage with Security Manager have a 3DES/AES license.

---

For information on configuring SSL, see [Setting Up SSL, page 5-4](#).

- **SSH**—Secure Shell is the default transport protocol for Catalyst switches and Catalyst 6500/7600 devices. You can also use it with Cisco IOS routers.

For information on configuring SSH, see [Setting Up SSH, page 5-9](#).

- **Telnet**—Telnet is the default protocol for routers running Cisco IOS software releases 12.1 and 12.2. You can also use it with Catalyst switches, Catalyst 6500/7600 devices, and routers running Cisco IOS Software release 12.3 and higher. See the Cisco IOS software documentation for configuring Telnet.
- **HTTP**—You can use HTTP instead of HTTPS (SSL) with IPS devices. HTTP is not the default protocol for any device type.
- **TMS**—Token Management Server is treated like a transport protocol in Security Manager, but it is not a real transport protocol. Instead, by configuring TMS as the transport protocol of a router, you are telling Security Manager to deploy configurations to a TMS. From the TMS, you can download the configuration to an eToken, plug the eToken into the router's USB bus, and update the configuration. TMS is available only for routers running Cisco IOS Software 12.3 or higher.

For information on downloading configurations using TMS, see [Setting Up TMS, page 5-22](#).

Security Manager can also use indirect methods to deploy configurations to devices, staging the configuration on a server that manages the deployment to the devices. These indirect methods also allow you to use dynamic IP addresses on your devices. The methods are not treated as transport protocols, but as adjuncts to the transport protocol for the device. You can use these indirect methods:

- **AUS (Auto Update Server)**—When you add a device to Security Manager, you can select the AUS server that is managing it. You can use AUS with PIX Firewalls, ASA devices, and Cisco IOS routers.

If you configure the AUS server to support the CNS Gateway protocol, you can use it with Cisco IOS routers that have dynamic IP addresses. However, you must also configure SSH and SSL on the routers.

For information on configuring a device to use an AUS server, see [Setting Up AUS, page 5-13](#).

- **CNS-Configuration Engine**—When you add a router to Security Manager, you can select the Configuration Engine that is managing it.

For more information on configuring a router to use a CNS-Configuration Engine server, see [Setting Up CNS, page 5-16](#).

For information on adding devices that use AUS or CNS servers to Security Manager, and how to add the servers, see these topics:

- [Adding Devices to the Device Inventory, page 6-8](#)
- [Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-19](#)

## Setting Up SSL

Security Manager deploys the configuration to the device using a Secure Socket Layer (SSL) protocol. With this protocol, Security Manager encrypts the configuration file and sends it to the device.

The following topics describe how to set up SSL on devices:

- [Setting Up SSL on PIX Firewall, ASA and FWSM Devices, page 5-4](#)
- [Setting Up SSL on Cisco IOS Routers, page 5-6](#)

## Setting Up SSL on PIX Firewall, ASA and FWSM Devices

[Table 5-1](#) describes the tasks to complete before you use SSL as the transport protocol for device management on PIX Firewall, ASA and FWSM devices.

Table 5-1 *Setting Up SSL on PIX Firewall, ASA, and FWSM Devices*

Steps	Enter	Result
1. Step 1	hostname# <b>config terminal</b>	<p>Enters configuration mode from the terminal.</p> <p>Respond to the prompts appropriately. Here are some tips:</p> <ol style="list-style-type: none"> <li>1. Enter <b>y</b> when the prompt asks if you want to preconfigure using interactive prompts.</li> <li>2. Enter the current enable password.</li> <li>3. Specify the time zone, year, month, day, and time.</li> <li>4. If the device: <ul style="list-style-type: none"> <li>- Is new—Specify the network interface IP address of the device and the network mask that applies to the inside IP address.</li> <li>- Exists—Verify that the interface IP address and mask are correct.</li> </ul> </li> <li>5. If the device: <ul style="list-style-type: none"> <li>- Is new—Specify the hostname and the domain name.</li> <li>- Exists—Verify that the hostname and domain name are correct.</li> </ul> </li> <li>6. When prompted for the IP address of the host that runs the PIX Device Manager, specify the IP address of the Security Manager server.</li> <li>7. Enter <b>yes</b> when the prompt asks if you want to write the above changes to Flash.</li> </ol>
Step 2	hostname(config)# <b>http server enable</b>	Enables the HTTP server.

**Table 5-1** Setting Up SSL on PIX Firewall, ASA, and FWSM Devices (Continued)

Steps	Enter	Result
Step 3	hostname(config)# <b>http</b> <i>ip_address</i> [ <i>netmask</i> ] [ <i>if_name</i> ]	Specifies the host or network authorized to initiate an HTTP connection to the device. <ul style="list-style-type: none"> <li><i>ip_address</i>—IP address of the Security Manager server.</li> <li><i>netmask</i>—Network mask for the <i>http ip_address</i>.</li> <li><i>if_name</i>—Device interface name (default is <b>inside</b>) from which Security Manager initiates the HTTP connection.</li> </ul>
Step 4	hostname(config)# <b>write memory</b>	Stores the current configuration in Flash memory.

## Setting Up SSL on Cisco IOS Routers

Table 5-2 describes the tasks to complete before you use SSL as the transport protocol for device management on Cisco IOS routers.

**Table 5-2** Setting Up SSL on Cisco IOS Routers

Steps	Enter	Result
Step 1	router# <b>config terminal</b>	Enters configuration mode from the terminal.
Step 2	router(config)# <b>hostname</b> < <i>name</i> >	Configures the hostname.  If the device is new, you must configure its hostname.  After you configure the hostname, the device prompt changes to <i>hostname</i> (config)#. For example, if the hostname is <i>router1</i> , the device prompt changes to <i>router1</i> (config)# (see Step 3).

Table 5-2 Setting Up SSL on Cisco IOS Routers (Continued)

Steps	Enter	Result
Step 3	router1(config)# <b>ip domain-name</b> <your_domain>	Specifies the IP domain name of the router. If the device is new and is not configured with a domain name, you must specify the IP domain name of the router.
Step 4	router1(config)# <b>username</b> <username> <b>privilege 15 password 0</b> <password>	Configures level 15 privilege. SSL requires that you must have level 15 privileges to log in to a Cisco IOS router.
Step 5	router1(config)# <b>no aaa authorization network</b> <list-name>	(Optional) Disables AAA authorization. If you are using AAA for authorization but would like to use local authorization, use this command to disable the AAA authorization. <ul style="list-style-type: none"> <li><i>list-name</i>—Character string used to name the list of authorization methods.</li> </ul>
Step 6	router1(config)# <b>no aaa authentication login</b> <list-name>	(Optional) Disables AAA authentication at login. If you are using AAA for authentication but would like to use local authentication, use this command to disable the AAA authentication. <ul style="list-style-type: none"> <li><i>list-name</i>—Character string used to name the list of authentication methods activated when a user logs in.</li> </ul>

Table 5-2 Setting Up SSL on Cisco IOS Routers (Continued)

Steps	Enter	Result
Step 7	router1(config)# <b>ip http authentication local</b>	<p>(Optional) Enables local authentication for SSL. Enables Security Manager to authenticate with the local username you created in Step 4.</p> <p><b>Note</b> If you do not enter this command, the default enable password is used for authentication.</p> <p><b>Note</b> You can either enable AAA authentication or local authentication. To enable AAA authentication, enter the commands in Step 8 and Step 9. To enable local authentication, enter the command in this step.</p>
Step 8	router1(config)# <b>ip http authentication aaa</b>	<p>(Optional) Enables AAA authentication/authorization for SSL.</p> <p><b>Note</b> You can either enable AAA authentication or local authentication. To enable AAA authentication, enter the commands in Step 8 and Step 9. To enable local authentication, enter the command in Step 7.</p>

Table 5-2 Setting Up SSL on Cisco IOS Routers (Continued)

Steps	Enter	Result
Step 9	<pre>router1(config)#ip http authentication aaa login-authentication&lt;list-name&gt; &gt; router1(config)# ip http authentication aaa exec-authorization&lt;list-name&gt;</pre>	<p>(Optional) If multiple AAA lists are defined, you must enter these commands.</p> <p>These commands authenticate the user that is contacting the device using the HTTPS protocol. The authentication uses AAA.</p> <ul style="list-style-type: none"> <li><i>list-name</i>—Character string used to name the list of AAA server groups.</li> </ul> <p><b>Note</b> You can either enable AAA authentication or local authentication. To enable AAA authentication, enter the commands in Step 8 and Step 9. To enable local authentication, enter the command in Step 7.</p>
Step 10	<pre>router1(config)# ip http secure-server</pre>	Enables the HTTPS server.
Step 11	<pre>router1(config)# exit</pre>	Exits configuration mode and returns to Exec mode.
Step 12	<pre>router1# show ip http server secure status</pre>	Verifies that SSL is set up on the device. Device responds with an “enabled” status.

## Setting Up SSH

Security Manager deploys the configuration to Cisco IOS Routers, Catalyst switches, and Catalyst 6500/7600 devices using a Secure Shell (SSH). This provides strong authentication and secure communications over insecure channels. Security Manager supports both SSHv1.5 and SSHv2. Once connected to the device, Security Manager determines which version to use and downloads using that version.



### Note

Security Manager supports Catalyst 6500/7600 devices running the Cisco IOS software only.

The following topics describe the tasks required to set up SSH on Cisco IOS routers, Catalyst switches, and Catalyst 6500/7600 devices:

- [Critical Line-Ending Conventions for SSH, page 5-10](#)
- [Testing Authentication, page 5-10](#)
- [Setting Up SSH on Cisco IOS Routers, Catalyst Switches, and Catalyst 6500/7600 devices, page 5-11](#)
- [Preventing Non-SSH Connections—Optional, page 5-13](#)

## Critical Line-Ending Conventions for SSH

The following line-ending conventions for SSH must be observed to avoid system failure:

1. Do not end banner message lines with “#”, “# ”, “>”, or “> ”. If your system requires a pound sign or greater-than sign at the end of a banner message, ensure that it is followed by two spaces.
2. Do not use banner message lines that contain only “Username: ” or “Password: ”
3. Do not customize the device user-mode prompt to not end with “>” or “#”.

## Testing Authentication

Before you set up SSH, you must test authentication without SSH to make sure the device can be authenticated. You can authenticate with a local username and password or with an authentication, authorization, and accounting (AAA) server running TACACS+ or RADIUS.

To test authentication without SSH using a local or AAA server username and password, enter the commands described in [Table 5-3](#).

**Table 5-3**      **Testing Authentication Without SSH**

Steps	Enter	Result
Step 1	hostname# <b>config terminal</b>	Enters configuration mode from the terminal.
Step 2	hostname(config)# <b>aaa</b> <b>new-model</b>	Uses the local username and password in the absence of aaa statements.  <b>Note</b> On Cisco IOS routers, you can use the login local command on vty lines instead of the aaa new-model command.
Step 3	hostname(config)# <b>username&lt;name&gt;password</b> <b>0&lt;password&gt;</b>	Configures the user in the local database of the device. This command is optional.
Step 4	hostname(config)# <b>exit</b>	Exits configuration mode.
Step 5	hostname# <b>write memory</b>	Saves the configuration changes.

**Related Topics**

- [Setting Up SSH, page 5-9](#)
- [Setting Up SSH on Cisco IOS Routers, Catalyst Switches, and Catalyst 6500/7600 devices, page 5-11](#)
- [Preventing Non-SSH Connections—Optional, page 5-13](#)

## Setting Up SSH on Cisco IOS Routers, Catalyst Switches, and Catalyst 6500/7600 devices

[Table 5-4](#) describes the tasks required to set up SSH on Cisco IOS routers, Catalyst switches, and Catalyst 6500/7600 devices.

**Note**

You must configure SSH on Cisco IOS routers because Security Manager uses SSH connections to handle interactive command deployments during SSL deployments.

**Table 5-4** *Setting Up SSH on Cisco IOS Routers, Catalyst Switches, and Catalyst 6500/7600 Devices*

Steps	Enter	Result
Step 1	router# <b>config terminal</b>	Enters configuration mode from the terminal.
Step 2	router(config)# <b>hostname</b> <name>	Configures the hostname.  If the device is new, you must configure its hostname. Configuring the host name changes the command prompt to use the name (for example, router1).
Step 3	router1(config)# <b>ip domain-name</b> <your_domain>	Specifies the IP domain name of the router.  If the device is new and is not configured with a domain name, you must specify the IP domain name of the router.
Step 4	router1(config)# <b>crypto key generate rsa</b>	Generates the RSA key pair for the SSH session.  When the device prompts you to enter the size of the modulus, we recommend that you enter 1024.
Step 5	router1(config)# <b>ip ssh timeout</b> <time>	(Optional) Sets the timeout interval in minutes.
Step 6	router1(config)# <b>ip ssh authentication-retries</b> <n>	(Optional) Sets the number of retries.
Step 7	router1(config)# <b>exit</b>	Exits configuration mode and returns to Exec mode.
Step 8	router1# <b>write memory</b>	Saves the configuration changes.

#### Related Topics

- [Setting Up SSH, page 5-9](#)
- [Testing Authentication, page 5-10](#)
- [Preventing Non-SSH Connections—Optional, page 5-13](#)

## Preventing Non-SSH Connections—Optional

After configuring SSH, you can configure the Cisco IOS routers, Catalyst switches, and Catalyst 6500/7600 devices to use SSH connections only. To prevent non-SSH connections, enter the commands described in [Table 5-5 on page 5-13](#).

**Table 5-5** *Preventing Non-SSH Connections (Optional)*

Steps	Enter	Result
Step 1	hostname# <b>config terminal</b>	Enters configuration mode from the terminal.
Step 2	hostname(config)# <b>line vty</b> <first line number> <last line number>	Sets up the router for Telnet access. <ul style="list-style-type: none"> <li>• <i>first line number</i>—valid values are 0 to 1180.</li> <li>• <i>last line number</i>—valid values are 1 to 1180.</li> </ul>
Step 3	hostname(config-line)# <b>transport input ssh</b>	Prevents non-SSH connections, such as Telnet.
Step 4	hostname(config-line)# <b>end</b>	Exits configuration mode.
Step 5	hostname# <b>write memory</b>	Saves the configuration changes.

### Related Topics

- [Setting Up SSH, page 5-9](#)
- [Testing Authentication, page 5-10](#)
- [Setting Up SSH on Cisco IOS Routers, Catalyst Switches, and Catalyst 6500/7600 devices, page 5-11](#)

## Setting Up AUS

Security Manager deploys configuration files to the Auto Update Server, where they are stored for later retrieval by the device.

The following topics provide more information:

- [Setting Up AUS on PIX Firewall and ASA Devices, page 5-14](#)
- [Setting Up CNS Gateway on an Auto Update Server, page 5-15](#)

## Setting Up AUS on PIX Firewall and ASA Devices

Devices, such as PIX Firewall and ASA, use the AUS protocol to contact the Auto Update Server for configuration (and image) updates. See the Auto Update Server product documentation for more information.

Table 5-6 describes the tasks to complete before you use AUS as the transport protocol for device management on PIX Firewall and ASA devices.

**Table 5-6**      **Setting Up AUS on PIX Firewall and ASA Devices**

Steps	Enter	Result
Step 1	hostname# <b>config terminal</b>	Enters configuration mode from the terminal.
Step 2	hostname(config)# <b>auto-update server</b> <b>https://username:password@AUSserver_IP_address:port/auto-update/AutoUpdateServlet</b>	Connects to the AUS. <ul style="list-style-type: none"> <li>• <i>username</i>—The username is the one you enter when you use Security Manager.</li> <li>• <i>password</i>—The password is the one you enter when you use Security Manager.</li> <li>• The port number is typically 443.</li> </ul>
Step 3	hostname(config)# <b>auto-update poll-period</b> <i>poll_period</i> [ <i>retry_count</i> ] [ <i>retry_period</i> ]	Specifies the polling period for AUS. <ul style="list-style-type: none"> <li>• <i>poll_period</i>—Polling period interval between two updates. Default is 720 minutes (12 hours).</li> <li>• <i>retry_count</i>—(Optional) Number of times to retry if the server connection attempt fails. Default is 0.</li> <li>• <i>retry_period</i>—(Optional) Number of minutes between retries. Default is 5.</li> </ul>
Step 4	hostname(config)# <b>auto-update device-id hardware-serial   hostname   ipaddress</b> [< <i>if_name</i> > ]  <b>mac-address</b> [< <i>if_name</i> > ]   <b>string</b> < <i>text</i> >	Configures the device to use the specified unique device ID to identify itself. <ul style="list-style-type: none"> <li>• <i>if_name</i>—Device interface name (default is <b>inside</b>).</li> <li>• <i>text</i>—A unique string name.</li> </ul>
Step 5	hostname(config)# <b>write memory</b>	Saves the configuration changes.

## Setting Up CNS Gateway on an Auto Update Server

An Auto Update Server can provide the CNS event-bus feature to Cisco IOS routers that have dynamic IP addresses obtained from a DHCP server. Security Manager communicates with the Auto Update Server that is running the CNS Gateway protocol to determine the IP address of the device. To configure CNS on a Cisco IOS router in event-bus mode, see [Table 5-7 on page 5-17](#).

If you changed the CNS password on a Cisco IOS router, you must also change the password in the Auto Update Server, as described in the next paragraph.

### Changing the Default CNS Bootstrap Password in the Auto Update Server

The default CNS bootstrap password configured in an Auto Update Server is **callhome**. If you changed the CNS password on the router (Step 7 in [Table 5-7 on page 5-17](#)), you must change the default CNS bootstrap password in the Auto Update Server also.

This procedure describes how to change the default CNS bootstrap password in an Auto Update Server.

### Related Topics

- [Setting Up CNS on Cisco IOS Routers, page 5-16](#)

- 
- Step 1** Open the Windows command prompt on the machine where you installed AUS.
- Step 2** Enter `set NMSROOT=<dir>`  
where `<dir>` is the directory where you installed AUS. For example, set `NMSROOT=C:\Progra~1\CSCOpX`.
- Step 3** Enter `cd %NMSROOT%\MDC\autoupdate\bin\eventgateway`.
- Step 4** Enter `cnspassword<password>`  
where `<password>` is the password you set on the device.
- Step 5** Restart the Daemon Manager if it is running.
-

# Setting Up CNS

Security Manager deploys the configuration file to the Cisco Configuration Engine, where it is stored for later retrieval from the device. Devices, such as Cisco IOS router, PIX Firewall, and ASA that use a Dynamic Host Configuration Protocol (DHCP) server, contact the Cisco Configuration Engine for configuration (and image) updates. See the Cisco Configuration Engine product documentation for more information.

The following topics describe how to set up CNS on devices:

- [Setting Up CNS on PIX Firewall and ASA Devices, page 5-16](#)
- [Table 5-7 on page 5-17](#)

## Setting Up CNS on PIX Firewall and ASA Devices

If PIX Firewall and ASA devices are configured for CNS, they use the AUS protocol. The required steps are identical to the steps that you follow when you configure PIX Firewall and ASA for AUS. See [Setting Up AUS, page 5-13](#).

## Setting Up CNS on Cisco IOS Routers

The following tables describes the tasks to complete before you use CNS as the transport protocol for device management on Cisco IOS routers. You can configure CNS in the event-bus mode or the call-home mode.

- To configure CNS in event-bus mode, see [Table 5-7 on page 5-17](#).
- To configure CNS in call-home mode, see [Table 5-8 on page 5-19](#).

**Table 5-7** *Setting Up CNS on Cisco IOS Routers in Event-Bus Mode*

Steps	Enter	Result
<b>Step 1</b>	router# <b>config terminal</b>	Enters configuration mode from the terminal.
<b>Step 2</b>	router(config)# <b>hostname</b> <name>	Configures the hostname.  If the device is new, you must configure its hostname.  After you configure the hostname, the device prompt changes to <i>hostname</i> (config)#. For example, if the hostname is <i>router1</i> , the device prompt changes to <i>router1</i> (config)# (see step 3).
<b>Step 3</b>	router1(config)# <b>ip</b> <b>domain-name</b> <your_domain>	Specifies the IP domain name of the router.  If the device is new and is not configured with a domain name, you must specify the IP domain name of the router.
<b>Step 4</b>	router1(config)# <b>cns</b> <b>trusted-server</b> <b>all-agents</b> <ip_address>	Specifies the trusted server for the CNS agent. <ul style="list-style-type: none"> <li><i>ip_address</i>—The IP address of the trusted server.</li> </ul>
<b>Step 5</b>	router1(config)# <b>cns</b> <b>event</b> <ip_address> [ <i>port</i> ]	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients. <ul style="list-style-type: none"> <li><i>ip_address</i>—IP address of the event gateway.</li> <li><i>port</i>—The port is an optional parameter, and by default it is either 11011 (with no encryption) or 11012 (with encryption).</li> </ul>

Table 5-7 Setting Up CNS on Cisco IOS Routers in Event-Bus Mode (Continued)

Steps	Enter	Result
Step 6	router1(config)# <b>cns config partial</b> <ip_address>	Starts the CNS configuration agent and accepts a partial configuration.
Step 7	router1(config)# <b>cns password</b> <password>	<p>Sets the CNS password.</p> <p>&lt;password&gt;—The password you want to set on the router.</p> <p>You can set the CNS password to <b>callhome</b> (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 the Auto Update Server. For instructions, see <a href="#">Setting Up CNS Gateway on an Auto Update Server, page 5-15</a>.</p> <p><b>Note</b> 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	router1(config)# <b>cns exec</b>	Enables and configures the CNS execute agent.
Step 9	router1(config)# <b>exit</b>	Exits configuration mode and returns to Exec mode.
Step 10	router1# <b>copy running startup</b>	Saves the configuration changes to NVRAM.

**Table 5-8** *Setting Up CNS on Cisco IOS Routers in Call-Home Mode*

Steps	Enter	Result
<b>Step 1</b>	router# <b>config terminal</b>	Enters configuration mode from the terminal.
<b>Step 2</b>	router(config)# <b>hostname</b> <name>	Configures the hostname.  If the device is new, you must configure its hostname.  After you configure the hostname, the device prompt changes to <i>hostname</i> (config)#. For example, if the hostname is router1, the device prompt changes to router1(config)# (see step 3).
<b>Step 3</b>	router1(config)# <b>ip</b> <b>domain-name</b> <your_domain>	Specifies the IP domain name of the router.  If the device is new and is not configured with a domain name, you must specify the IP domain name of the router.
<b>Step 4</b>	router1(config)# <b>cns</b> <b>trusted-server</b> <b>all-agents</b> <ip_address>	Specifies the trusted server for the CNS agent. <ul style="list-style-type: none"> <li><i>ip_address</i>—IP address of the trusted server.</li> </ul>

Table 5-8 Setting Up CNS on Cisco IOS Routers in Call-Home Mode (Continued)

Steps	Enter	Result
Step 5	<pre>router1(config)# <b>kron</b> <b>occurrence</b><i>occurrence-name</i> [<b>user</b><i>username</i> ] {<b>in</b> [[<i>numdays:</i>]<i>numhours:</i>]<i>nummin</i>   <b>at</b><i>hours:min</i> [[<i>month</i>] <i>day-of-month</i>] [<i>day-of-week</i>]} {<b>oneshot</b>   <b>recurring</b>}</pre>	<p>Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.</p> <ul style="list-style-type: none"> <li>• <i>occurrence-name</i>—Name of occurrence. Length of occurrence-name is from 1 to 31 characters. If the occurrence-name is new, an occurrence structure will be created. If the occurrence-name is not new, the existing occurrence will be edited.</li> <li>• <i>username</i>—(Optional) Name of user.</li> <li>• <i>numdays:</i>—(Optional) Number of days. Identifies that the occurrence is to run after a specified time interval. The timer starts when the occurrence is configured. If used, add a colon after the number.</li> <li>• <i>numhours:</i>—(Optional) Number of hours. If used, add a colon after the number.</li> <li>• <i>nummin</i>—Number of minutes.</li> <li>• <i>hours:</i>—Hour as a number using the 24-hour clock. Identifies that the occurrence is to run at a specified calendar date and time. Add a colon after the number.</li> <li>• <i>min</i>—Minute as a number.</li> <li>• <i>month</i>—(Optional) Month name. If used, you must also specify day-of-month.</li> <li>• <i>day-of-month</i>—(Optional) Day of month as a number.</li> <li>• <i>day-of-week</i>—(Optional) Name of the day of the week.</li> </ul>

Table 5-8 Setting Up CNS on Cisco IOS Routers in Call-Home Mode (Continued)

Steps	Enter	Result
		<ul style="list-style-type: none"> <li>• <b>oneshot</b>—Identifies that the occurrence is to run only once. After the occurrence runs, the configuration is removed.</li> <li>• <b>recurring</b>—Identifies that the occurrence is to run on a recurring basis.</li> </ul>
<b>Step 6</b>	router1(config-kron-occurrence) # <b>policy-list</b> <list-name>	<p>Specifies the policy list associated with a Command Scheduler occurrence.</p> <p>Use the kron occurrence and policy-list commands to schedule one or more policy lists to run at the same time or interval.</p> <ul style="list-style-type: none"> <li>• <i>list-name</i>—Name of policy. Length of list-name is from 1 to 31 characters. If the list-name is new, a policy list structure will be created. If the list-name is not new, the existing policy list will be edited.</li> </ul>
<b>Step 7</b>	router1(config-kron-occurrence) # <b>exit</b>	Exits kron-occurrence and returns to configuration mode.
<b>Step 8</b>	router1(config)# <b>kron</b> <b>policy-list</b> <list-name>	<p>Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.</p> <ul style="list-style-type: none"> <li>• <i>list-name</i>—Name of policy. Length of list-name is from 1 to 31 characters. If the list-name is new, a policy list structure will be created. If the list-name is not new, the existing policy list will be edited.</li> </ul>
<b>Step 9</b>	router1(config-kron-policy)# <b>cli</b> <b>cns config</b> <b>retrieve</b> <ip_address> <b>page</b> <b>/cns/JobbedDynaConfig status</b> <b>http://</b> <ip_address> <b>/cns/PostSt</b> <b>atus</b>	<p>Retrieves the config from the staged CNS job.</p> <ul style="list-style-type: none"> <li>• <i>ip address</i>—IP address of the CNS server.</li> <li>• <b>JobbedDynaConfig status</b>—You must use JobbedDynaConfig status so that the device retrieves the config from the staged CNS job; otherwise, the device retrieves the template associated with the device.</li> </ul>

**Table 5-8** *Setting Up CNS on Cisco IOS Routers in Call-Home Mode (Continued)*

Steps	Enter	Result
Step 10	router1(config-kron-policy)# <b>exit</b>	Exits kron-policy configuration mode and returns to configuration mode.
Step 11	router1(config)# <b>cns exec</b>	Enables and configures the CNS execute agent.
Step 12	router1(config)# <b>exit</b>	Exits configuration mode and returns to Exec mode.
Step 13	router1# <b>copy running startup</b>	Saves the configuration changes to NVRAM.

**Related Topics**

- [Setting Up CNS Gateway on an Auto Update Server, page 5-15](#)

## Setting Up TMS

Security Manager uses FTP to deploy the configuration file to the Token Management Server (TMS), from which it can be downloaded and encrypted onto an eToken. The eToken can then be connected to the USB port of a router and the configuration downloaded. See TMS product documentation for more information.

To download the configuration from the eToken to the router, plug the eToken into the router, then enter the commands as described in [Table 5-9 on page 5-23](#).

**Table 5-9** *Setting Up TMS on Cisco IOS Routers*

Steps	Enter	Result
Step 1	router# <b>crypto pki token</b> <usb_token_id> <b>login</b> <PIN>	Logs into the eToken. <ul style="list-style-type: none"> <li><i>usb_token_id</i>—Depending on the port in which the e-token is inserted, <i>usb_token_id</i> could either be <i>usbtoken0</i> or <i>usbtoken1</i>.</li> <li><i>PIN</i>—The default is 1234567890.</li> </ul>
Step 2	router# <b>config terminal</b>	Enters configuration mode from the terminal.
Step 3	router(config)# <b>crypto pki token default secondary config</b> CCCD	Enables configuration provisioning with eToken. CCCD is the private sector on the eToken where the configuration file resides. When you enter this command, the CLI on the e-token merges with the CLI on the router.
Step 4	router(config)# <b>exit</b>	Exits configuration mode and returns to Exec mode.
Step 5	router# <b>write memory</b>	Keeps the CLI on the router after you disconnect the eToken.

## Initializing IPS Devices

To initialize an IPS device, you must configure the following settings. These are network settings, and only a user with administrator privileges on the IPS device can configure them:

- Sensor name
- IP address
- Netmask
- Default route
- Enable TLS/SSL (to enable TLS/SSL in the web server on the device)
- Web server port
- Use default ports

You configure these settings through the **setup** command in Intrusion Prevention System Device Manager (IDM) or in a command-line session, depending upon which platform is used by your IPS device. The platform is one of the following:

- Sensor appliance
- IDSM-2
- AIP-SSM
- NM-CIDS

For detailed information on these settings, refer to the technical documentation for your IPS device.

**Note**

---

For information on preparing an IOS IPS device for use, see [Preparation for Use, page 14-26](#).

---