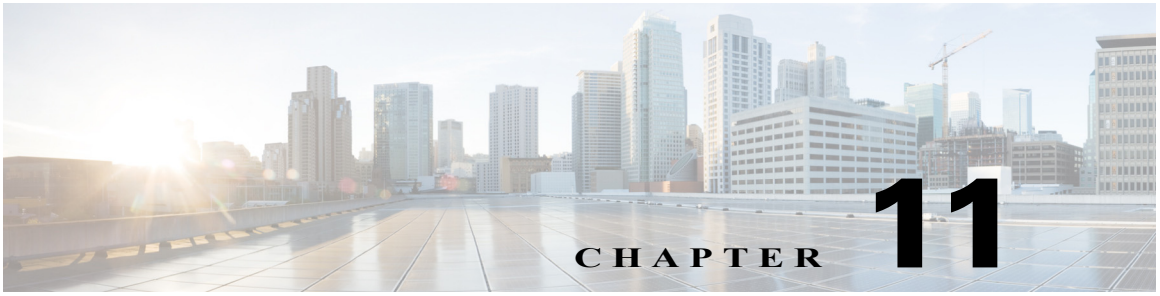

Configuring Security Manager Administrative Settings

Security Manager has default settings for many system functions that you can change if they do not fit the needs of your organization. To view and change these settings, select **Tools > Security Manager Administration**. You can then select items from the table of contents on the left of the window to view the default settings related to that item.

On most pages, when you change a setting, you must click **Save** to save your changes. If you make a mistake, you can click **Reset** to return the values to the previously saved values. You can also click **Restore Defaults** to return the settings to the Security Manager defaults.

Besides the pages that contain system defaults, the Security Manager Administration window includes items that relate to system administration activities, such as taking over another user's work or obtaining access to pages in Common Services to perform server security tasks.

The following topics describe the settings and actions available on each of the pages available in the Security Manager Administration window:

API Settings Page

The Security Manager API settings page enables you to enable or disable the API service and change its settings.

Navigation Path

Click **Tools > Security Manager Administration** and select **API** from the table of contents.

Field Reference

Table 11-1 API Settings Page

Element	Description
Enable API Service	Whether to enable or disable the API service.
Result Set Page Size	Allowed values are 100 through 1000, inclusive.
Active client sessions	Allowed values are 1 through 10, inclusive.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

AutoLink Settings Page

The Security Manager Map view provides a graphical view of your VPN and layer 3 network topology. Using device nodes to represent managed devices and map objects to represent unmanaged objects such as devices, clouds, and networks, you can create topology maps with which to study your network. AutoLink settings enable you to exclude any one of five private or reserved networks from Map view. For example, you might want to exclude any test networks that are not relevant to the management tasks you are using Security Manager to perform.

Navigation Path

Click **Tools > Security Manager Administration** and select **AutoLink** from the table of contents.

Related Topics

- Creating and Managing Layer 3 Links on the Map, page 35-19
- Displaying Your Network on the Map, page 35-14

Field Reference

Table 11-2 AutoLink Page

Element	Description
Enable AutoLink for 10.0.0.0/8 Enable AutoLink for 172.16.0.0/12 Enable AutoLink for 192.168.0.0/16	Whether to automatically include or omit (deselected) these private networks from the maps you create.
Enable AutoLink for 127.0.0.0/8	Whether to automatically include or omit (deselected) the loopback network from the maps you create.
Enable AutoLink for 224.0.0.0/4	Whether to automatically include or omit (deselected) the multicast networks from the maps you create.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

ACL Hit Count Settings Page

The Security Manager ACL Hit Count Settings page enables you to configure and change the settings for Hit Count. This feature is available in Security Manager version 4.9 and higher for ASA and ASASM devices.

Navigation Path

Click **Tools > Security Manager Administration** and select **ACL Hit Count Settings** from the table of contents.

Field Reference

Table 11-3 Hit Count Settings

Element	Description
Hit Count History Persist Limit (per ACE)	The Hit Count History Persist Limit is the limit for the Hit Count history details that can be stored for the particular ACE in the database. The default value is 5 and you can enter a maximum value of 10.
Purge Scheduler Process Time	The Purge Scheduler Process Time is used by the Hit Count Scheduler to schedule the Hit Count purge job at the given time on a daily basis. Select a time from the drop-down list. The default is 12 AM.

CCO Settings Page

Use the CCO Settings page to configure the settings used to connect to Cisco.com.

Also, use the CCO Settings page for certificate trust management. (Security Manager downloads ASA images from Cisco.com over HTTPS, which uses certificates for establishing trust.) The certificate trust management feature on the Image Manager page is new in Security Manager 4.4. It will help you with improved handling of Cisco.com certificates for ASA image downloads:

- You can use it to view a certificate and use discretion in accepting it.
- After you accept a certificate, it is stored on your Security Manager server.
- You can see all your certificates in a summary table on the Image Manager page, and you can use that table to view or remove certificates.

Tip Please be sure to refer to "Retrieve Certificate" in the table below.

For detailed documentation of the certificate trust management feature, refer to Certificate Trust Management, page 10-18.

Navigation Path

Select **Tools > Security Manager Administration** and select **CCO Settings** from the table of contents.

Field Reference

Table 11-4 CCO Settings Page

Element	Description
Use IPS Updates Settings	If checked, the other settings on this page are disabled and the default prevails (the Cisco.com credentials from the IPS Updates page apply). **Caution** If checked, be sure that the Cisco.com credentials from the IPS Updates page are configured correctly. On that page, the default value for "Update From:" is "Local Server." You must choose "Cisco.com" to see certificate settings. Improper or incomplete certificate setting will prevent connectivity to Cisco.com, and all Cisco.com-related operations in this area will fail.
Username	The username Security Manager should use to log in to Cisco.com.
Password Confirm	The password for the username. Enter the password in both fields.
Proxy Server Settings	
Enable Proxy	Enables Image Manager to connect to Cisco.com via a web proxy server. When Enable Proxy is selected, the other proxy fields (including IP or Hostname, Port, Username, and Password) are enabled and used to connect to the web proxy.
Test Connection	Used to test for connectivity and credentials for Cisco.com.
Certificate	
Contact URL	• When selected, "Image Meta-data Locator" is used. This is the URL on Cisco.com that is used to obtain meta-data information about images. Meta-data information consists of the images applicable to a particular product, name, size, checksum, and URL to download for each image. • When selected, "Other" is used. You can enter any valid HTTPS URL. This URL is intended primarily for the HTTPS URL to download the image as obtained from the meta-data information about the image. This URL may be different from the URL of the image meta-data locator described in the previous paragraph; the certificate may be different, as well. **Caution** If you choose "Other," you need to explicitly add "https://dl.cisco.com" [without the quotation marks]: Enter it in the text field adjacent to the "Other" button. Failure to do this will prevent connectivity to Cisco.com, and all Cisco.com-related operations in this area will fail.

Table 11-4 CCO Settings Page (continued)

Element	Description
Retrieve Certificate	Used to connect to and retrieve the certificate from the selected ‘"Contact URL’." After retrieving the certificate it opens the Certificate Verification dialog, which along with a brief summary of the certificate, i.e., who the certificate is issued to, by whom, and the validity period of the certificate, gives you the following choices: • **View Certificate**—Opens the Certificate Viewer, where you can see all the details of the certificate: Certificate Authority, version, serial number, thumbprint, and other details. It shows the complete certificate chain information all the way up to the root issuing certificate Authority. • **Accept**—Accepts the certificate and adds it to the Cisco Security Manager. • **Reject**—Rejects the certificate and no action is taken. • **Cancel**—Closes the Certificate Verification dialog with no action taken. You must view and accept the following recommended certificates: • https://www.cisco.com • https://www.dl3.cisco.com • https://www.cloudsso.cisco.com • https://www.api.cisco.com
Certificates	A table that displays, for each certificate in your Security Manager installation, Subject, Issued By, and Accepted By.
View	Opens the Certificate Viewer for a certificate selected in the Certificate table.
Remove	Removes a certificate selected in the Certificate table.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Configuration Archive Page

Use the Configuration Archive page to define the default settings for the Configuration Archive tool, including how many configuration versions to save and the TFTP server to use for rolling back Cisco IOS software device configurations.

Navigation Path

Click **Tools > Security Manager Administration** and select **Configuration Archive** from the table of contents.

Related Topics

- Configuration Archive Window, page 8-23

- Rolling Back Configurations, page 8-63

Field Reference

Table 11-5 Configuration Archive Page

Element	Description
Max. Versions per Device Purge Now button Enable Configuration Archive Versions Auto Purge	The number of configuration versions you want to retain for each managed device, from 1 to 100. If you reduce the number, you can click **Purge Now** to immediately delete extra versions. Security Manager automatically deletes extra versions during its normal cleanup cycle if you select the **Enable Configuration Archive Versions Auto Purge** option.
TFTP Server for Rollback	The fully-qualified DNS hostname or IP address of the server to use for TFTP file transfers. TFTP is used during rollback for IOS devices when the configuration cannot be updated using the **configure replace** command, which does not force a system reload. Enter **localhost** to use the Security Manager server. By default, a TFTP server is enabled on the Security Manager server. If you specify a remote TFTP server, you must configure that server appropriately to provide TFTP services.
TFTP Root Directory	The root directory for configuration file transfers if you are using the Security Manager server as the TFTP server. Click **Browse** to select a directory on the Security Manager server. If you specify a server other than the Security Manager server as the TFTP host, Security Manager always uses the root directory of that TFTP server. You cannot specify a non-root directory for remote TFTP servers.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

CS-MARS Page

Use the CS-MARS page to register the Cisco Security Monitoring, Analysis and Response System servers that are monitoring your devices with Security Manager. By registering your CS-MARS servers, you can view messages and events captured in CS-MARS based on a device's firewall access rules or IPS signature rules configured in Security Manager. You must register a CS-MARS server before users can see events collected from it.

Tip If you are using CS-MARS global controllers, add them instead of the individual local controllers. By adding global controllers, Security Manager can identify the correct local controller for a device automatically, without you having to add each of the local controllers. This simplifies your CS-MARS configuration in Security Manager.

Navigation Path

Select **Tools > Security Manager Administration** and select **CS-MARS** from the table of contents.

Related Topics

- Registering CS-MARS Servers in Security Manager, page 72-38

Field Reference

Table 11-6 CS-MARS Page

Element	Description
CS-MARS Devices	The CS-MARS servers that are registered with Security Manager. • To add a server, click the Add (+) button and fill in the New or Edit CS-MARS Device Dialog Box, page 11-8. • To edit a server, select it and click the Edit (pencil) button. • To delete a server, select it and click the Delete (trash can) button. When you delete a server, the device properties for all devices that use the server are updated to remove the server connection. If a device is also monitored by another CS-MARS server on the list, its properties are updated to point to the other server.
When Launching CS-MARS Allow User to Save Credentials	The type of credentials Security Manager should use to log into CS-MARS when obtaining event information: • **Prompt users**—When the user tries to get event information from CS-MARS, prompt the user to log into CS-MARS. If you select this option, you can also select **Allow User to Save Credentials**, which gives users the option to save their credentials so they do not have to log into CS-MARS again the next time they request event status. • **Use CS-Manager Credentials**—When the user tries to get event information from CS-MARS, log into CS-MARS using the same username and password the user used to log into Security Manager.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.

New or Edit CS-MARS Device Dialog Box

Use the New or Edit CS-MARS Device dialog box to register a CS-MARS server with Security Manager. Users can obtain messages or event status for a device's firewall or IPS policies from the CS-MARS server that is monitoring the device. For more information, see Registering CS-MARS Servers in Security Manager, page 72-38.

Navigation Path

From the CS-MARS Page, page 11-7, click the Add button to add a new server, or select a server and click the Edit button.

Field Reference

Table 11-7 Add or Edit CS-MARS Device Dialog Box

Element	Description
CS-MARS Hostname/IP	The IP address or fully-qualified DNS host name of the CS-MARS server. **Tip** If you add a CS-MARS global controller, do not add any of the local controllers that the global controller monitors. Security Manager will automatically determine the local controller that is monitoring a specific device. Adding global controllers simplifies your CS-MARS configuration.
Username Password User Type	The username and password for logging into the server to validate that the CS-MARS server is running the appropriate software version and to obtain other basic information. Security Manager also uses this account to determine which CS-MARS server is monitoring a particular device. For CS-MARS local controllers, you can enter either a global or local user account. For global controllers, you must enter a global account. Identify the type of account in the User Type field.
Certificate Thumbprint Retrieve From Device button	The CS-MARS server certificate, a hexadecimal string that is unique to the device. Click **Retrieve From Device** to have Security Manager retrieve the certificate from the CS-MARS server. If the certificate is retrieved successfully, it is displayed. After verifying the certificate, click **Accept** to save it on the Security Manager server. You must have a correct certificate to use the CS-MARS server from Security Manager.

CSM Mobile Page

Use the CSM Mobile page of the Security Manager Administration window to enable or disable the CSM Mobile feature in Cisco Security Manager. If the CSM Mobile feature is enabled, users can access device health and summary information from mobile devices by navigating to the following link, where <SecManServer> is the DNS name or IP address of the Security Manager server:

https://<*SecManServer*>/mobile/

or

https://<*SecManServer*>/mobile

For more information about the types of information provided, see Dashboard Overview, page 72-1.

For more information about CSM Mobile, see CSM Mobile, page 72-11.

Navigation Path

Click **Tools > Security Manager Administration** and select **CSM Mobile** from the table of contents.

Field Reference

Table 11-8 CSM Mobile Page

Element	Description
Enable CSM Mobile Feature	Lets you enable or disable the CSM Mobile feature. If you disable this feature, you cannot access device health summary information from mobile devices.
Save button	Saves and applies changes. If you change whether the service is enabled, it stops or starts, as appropriate. You are shown a progress indicator.
Reset button	Resets changes to the last saved values.

Customize Desktop Page

Use the Customize Desktop page to control whether Security Manager applications close automatically after being idle for a specified time, to reset whether you are prompted to verify your actions in certain circumstances, and to control whether certain file operations can be performed on the Security Manager client.

Navigation Path

Select **Tools > Security Manager Administration** and select **Customize Desktop** from the table of contents.

Related Topics

- Installing Security Manager License Files, page 10-16
- Importing Policies or Devices, page 10-13
- Exporting the Device Inventory from the Security Manager Client, page 10-6
- Exporting Shared Policies, page 10-12
- Selecting IPS License Files, page 11-61

Field Reference

Table 11-9 Customize Desktop Page

Element	Description
Reset ‘Do Not Ask’ on Warnings button	Click this button to reestablish ‘Are you sure...?’ pop-up warnings. When you perform some actions, you are warned about the consequences and you are given the option to not be warned again. If you selected Do Not Ask Me Again for any of these warnings, clicking this button reenables the warning.

Table 11-9 Customize Desktop Page (continued)

Element	Description
Enable Idle Timeout Idle Timeout (minutes)	Whether to have the Security Manager client applications close automatically if you do not use them for the specified period of time. The timeout applies across all applications; working in one application resets the timer in all applications. If you select this option, enter the number of minutes that must elapse before closing the client in the Idle Timeout field. The default is to close the client after 120 minutes of inactivity.
Enable Client side file browser	Whether to allow file operations on the Security Manager client. If you select this option, you will be able to choose between client and server file systems when performing the following file operations: • Installing Security Manager license files • Installing IPS license files • Importing/exporting device inventory files • Importing/exporting shared policies • Creating the following file objects: – Cisco Secure Desktop Package – Plug-In—For browser plug-in files. – AnyConnect Profile – AnyConnect Image – Hostscan Image This option is enabled by default.
Global Search	
Enable Global Search	Whether to enable or disable the Global Search feature. This feature is enabled by default. **Tip** You can disable Global Search before performing bulk discovery or rediscovery of devices to improve performance. You can reenable Global Search and then recreate the index after discovery is complete or when users are least likely to be using the system.
Recreate Index	Click this button to regenerate the search index. The global search feature is not available while the index is being recreated.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Debug Options Page

Use the Debug Options page to configure the severity level of messages to include in debugging logs and to determine what other debugging information is collected.

You should change debugging levels only if the Cisco Technical Assistance Center (TAC) asks you to change them. This makes it possible for you to include more detailed information in the CSMDiagnostics.zip file.

After you change the message level for the appropriate subcomponent, redo the actions that are resulting in system problems. After the problems occur, create the CSMDiagnostics.zip file (or the CSMDiagnostics_light.zip file) by selecting **Tools > Security Manager Diagnostics... > General Diagnostics...** (or **Tools > Security Manager Diagnostics... > Light Diagnostics...**). You can then reset the debug options to the default levels so that the Security Manager server does not become bogged down collecting extra debug information. For more information about generating the CSMDiagnostics.zip file, see Creating Diagnostics Files for the Cisco Technical Assistance Center, page 10-28.

By default, logs contain messages of the Error severity or worse. The severity levels in order of severity are:

- Severe—Problems that make the system unusable.
- Error—Problems from which Security Manager cannot recover.
- Warning—Unexpected conditions from which Security Manager can recover.
- Info—Informational messages.
- Debug—Internal status information.

Navigation Path

Select **Tools > Security Manager Administration**, then select **Debug Options** from the table of contents.

Field Reference

Table 11-10 Debug Options Page

Element	Description
Capture Discovery/Deployment Debugging Snapshots to File	Whether Security Manager generates data files about configuration generation, deployment, and discovery as these functions are performed. The temporary data files are stored in the MDC\temp directory in the Security Manager installation folder on the server, and you can use these files for debugging purposes. Enable this setting if you encounter problems with deployment or discovery. If you need to send these files to Cisco TAC for debugging, encrypt the files, because they can contain sensitive data such as passwords. **Note** Selecting this check box slows down Security Manager response time. Enable this option only in limited circumstances.
Deployment Debug Level	The message severity level for deployment-related actions such as device communication.
Event Manager Debug Level	The message severity level for the Event Manager subsystem.
Health and Performance Monitor Debug Level	The message severity level for the Health and Performance Monitor subsystem.
Image Manager Debug Level	The message severity level for the Image Manager subsystem.

Table 11-10 Debug Options Page (continued)

Element	Description
Firewall Services Debug Level	The message severity level for firewall-related policies.
IOS Platform Debug Level	The message severity level for Cisco IOS Software platform policies.
PIX Platform Debug Level	The message severity level for PIX, ASA, and FWSM platform policies.
Report Manager Debug Level	The message severity level for the Report Manager subsystem.
VPN Services Debug Level	The message severity level for VPN services policies.
API Debug Level	The message severity level for the Application Programming Interface subsystem.
Save button	Saves your changes.
Reset button	Restores all fields to their previous values.
Restore Defaults button	Resets values to Security Manager defaults.

Deployment Page

Use the Deployment page to define the default methods by which Security Manager deploys configurations to devices. You can override some of these settings when you create deployment jobs.

Navigation Path

Select **Tools > Security Manager Administration** and select **Deployment** from the table of contents.

Related Topics

- Chapter 8, "Managing Deployment"
- Chapter 6, "Managing Policy Objects"

Field Reference

Table 11-11 Deployment Page

Element	Description
General Parameters	
Purge Debugging Files Older Than (days)	The maximum number of days the system should keep debugging files. Debug files are automatically deleted. If you decrease the number of days, you can click **Purge Now** to immediately delete all debugging files older than the number of days specified.

Table 11-11 Deployment Page (continued)

Element	Description
Default Deployment Method Directory	The method to use as the default method for deploying configurations to devices: • Device—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see Deploying Directly to a Device, page 8-9. • File—Deploys the configuration file to a directory on the Security Manager server. If you select File, specify the directory to which you want to deploy the configuration file in the Destination column. Even if you select file as the default, the setting does not apply to IPS devices; you can use device deployment only for IPS devices. For more information, see Deploying to a File, page 8-11. You can override this method when you create deployment jobs.
When Out of Band Changes Detected	How Security Manager should respond when it detects that changes were made directly on the device CLI since a configuration was last deployed to the device. Out of band change detection works correctly only when deploying to device, not to file, and applies only when the deployment method is configured to obtain the reference configuration from the device (see below for a description of the Reference Configuration setting). This setting specifies the default action, which you can override when you create deployment jobs. You can choose one of the following: • **Overwrite changes and show warning** (default)—If changes were made to the device manually, Security Manager continues with the deployment, overwrites the changes, and displays a warning notifying you of this action. • **Cancel deployment**—If changes were made to the device manually, Security Manager cancels the deployment and displays a warning notifying you of this action. • **Do not check for changes**—Security Manager does not check for changes and deploys the changes to the device, overwriting any local modifications. For a more complete discussion of out-of-band change handling, see Understanding How Out-of-Band Changes are Handled, page 8-12. **Note** For devices in which failover is not configured, if you select the **Cancel Deployment** option when Out of Band changes are detected, the bootstrap configuration may cause deployments to fail. For deployments to be successful, you must configure failover before discovering the device in Security Manager.

Table 11-11 Deployment Page (continued)

Element	Description
Deploy to File Reference Configuration	The configuration that Security Manager uses to compare new policies against the previous configuration for the device, if you are deploying the configuration to a file on the Security Manager server. • Archive (default)—The most recently archived configuration. • Device—The current running device configuration, which is obtained from the device. After comparing the configurations, Security Manager generates the correct CLI for deployment.
Deploy to Device Reference Configuration	The configuration that Security Manager uses to compare new policies against the previous configuration for the device, if you are deploying the configuration directly to the device (or to a transport server). • Archive—The most recently archived configuration. • Device (default)—The current running device configuration, which is obtained from the device. After comparing the configurations, Security Manager generates the correct CLI for deployment.
Allow Download on Error	Whether deployments to devices should continue even if there are minor device configuration errors.
Save Changes Permanently on Device	Whether to save the running configuration to the startup configuration (using the **write memory** command) after deploying a configuration to a device. This applies to PIX, FWSM, ASA, or Cisco IOS devices. If you deselect this check box, the startup configuration is not changed, which means your configuration changes will be lost if the device reloads for any reason.
Preselect Devices with Undeployed Changes	Whether the list of changed devices you see when you create a deployment job has all changed devices preselected. If you deselect this option, users must manually select the devices to include in the deployment job.
Enable Auto Refresh in Deployment Main Panel	Whether the deployment job and schedule status information should be automatically refreshed in the Deployment Manager window. If you deselect this option, you must click the Refresh button to refresh the information manually.
Remove Unreferenced SSL VPN Files on Device (ASA Only)	Whether to have Security Manager delete files related to the SSL VPN configuration from the device if the files are no longer referred to by the device's SSL VPN configuration. If you deselect this option, unused files remain on the device after deployment.

Table 11-11 Deployment Page (continued)

Element	Description
Mask Passwords and Keys When Viewing Configs and Transcripts Mask Passwords and Keys When Deploying to File	The conditions, if any, under which Security Manager will mask the following items so that they cannot be read: passwords for users, enable mode, Telnet, and console; SNMP community strings; keys, including those for TACACS+, Preshared Key, RADIUS server, ISAKMP, failover, web VPN attributes, logging policy attributes, AAA, AUS, OSPF, RIP, NTP, logging FTP server, point-to-point protocol, Storage Key, single sign-on server, load balancing, HTTP/HTTPS proxy, and the IPSEC shared key. • Mask Passwords and Keys When Viewing Configs and Transcripts—This option affects only the screen display of the credentials, which guards against unauthorized personnel viewing them. If you do not select this option, credentials in full transcripts might still be masked depending on how the device handles them. • Mask Passwords and Keys When Deploying to File—This option affects the contents of configuration files that are deployed to file, making them undeployable to actual devices. Select this option only if you will never need to actually deploy these configurations to real devices. Selecting this option has no effect on whether credentials are masked when viewed.
Deploy only new or modified Flexconfigs	Whether to deploy FlexConfigs only one time after creation or modification of a FlexConfig, or to deploy all FlexConfigs with each deployment. This option is selected by default. **Note** If you have FlexConfigs that need to be deployed with each deployment, then you will need to disable this option. After changing this setting, you will need to manage one-time FlexConfigs by deleting them after they have been deployed.

Table 11-11 Deployment Page (continued)

Element	Description
ACL Parameters	
Optimize the Deployment of Access Rules For (IPv4 and IPv6 access rules.)	How firewall rules are deployed. You can choose one of the following: • Speed (default)—Increases deployment speed by sending only the delta (difference) between the new and old ACLs. This is the recommended option. By making use of ACL line numbers, this approach selectively adds, updates, or deletes ACEs at specific positions and avoids resending the entire ACL. Because the ACL being edited is still in use, there is a small chance that some traffic might be handled incorrectly between the time an ACE is removed and the time that it is added to a new position. The ACL line number feature is supported by most Cisco IOS, PIX and ASA versions, and became available in FWSM from FWSM 3.1(1). • Traffic—This approach switches ACLs seamlessly and avoids traffic interruption. However, deployment takes longer and uses more device memory before the temporary ACLs are deleted. First, a temporary copy is made of the ACL that is intended for deployment. This temporary ACL binds to the target interface. Then the old ACL is recreated with its original name but with the content of the new ACL. It also binds to the target interface. At this point, the temporary ACL is deleted. **Note** For FWSM devices, this option affects processing only if you also select the Let FWSM Decide When to Compile Access Lists option.
Firewall Access-List Names (IPv4 and IPv6 access rules.)	How ACL names are deployed to devices if the access rule does not have a name in Security Manager. • Reuse existing names—Reuse the ACL name that is configured in the reference configuration (which is usually from the device). • Reset to CS-Manager generated names—Reset the name to a Security Manager auto-generated ACL name.

Table 11-11 Deployment Page (continued)

Element	Description
Enable ACL Sharing for Firewall Rules (IPv4 and IPv6 access rules.)	Whether Security Manager should share a single access control list (ACL) for an access rule policy with more than one interface. If you do not select this option, Security Manager creates unique ACLs for every interface to which you apply an IPv4 or IPv6 access rule policy. The sharing of ACLs is done only for ACLs created by access rule policies. If you select this option, Security Manager evaluates the access rules policy for each interface and deploys the minimum number required to implement your policy while preserving your ACL naming requirements. For example, if you use an interface role to assign the same rules to four interfaces, you specify **Reset to CS-Manager generated names** for the Firewall Access-List Names property, and you do not specify ACL names for the interfaces in the access control settings policy, only a single ACL is deployed, and each interface uses that ACL. If you select this option, keep the following in mind: • An interface might use an ACL that is named for a different interface. • If you specify a name for the ACL in the access control settings policy, an ACL by that name is created even if it is otherwise identical to one used by another interface. Names specified in this policy have precedence over any other settings. • If you select **Reuse existing names** for the Firewall Access-List Names property, the existing names are preserved (unless you override them in the access control settings policy). This means that you might end up with duplicate ACLs under different names if duplicate ACLs already exist on the device. • Hit count statistics are based on ACL, not on interface, so a shared ACL provides statistics that are combined from all interfaces that share the ACL. • Sharing ACLs is primarily beneficial for memory-constrained devices such as the FWSM.
Let FWSM Decide When to Compile Access Lists (IPv4 access rules only.)	Whether to have the Firewall Services Module (FWSM) automatically determine when to compile access lists. Selecting this option might increase deployment speed but traffic might be disrupted and the system might become incapable of reporting ACL compilation error messages. If you select this option, you can use the Optimize the Deployment of Access Rules For Traffic setting to mitigate potential traffic disruptions. When deselected, Security Manager controls ACL compilation to avoid traffic interruption and to minimize peak memory usage on the device. **Caution** You should not select this option unless you are experiencing deployment problems and you are an advanced user.

Table 11-11 Deployment Page (continued)

Element	Description
Remove Unreferenced Access-lists on Device (IPv4 and IPv6 access rules.)	Whether to delete any access lists that are not being used by other CLI commands managed by Security Manager from devices during deployment. **Note** After enabling this option, Security Manager will remove access lists during deployment that are not used in any policies managed or discovered by Security Manager. If any policy that is NOT discovered or managed by Security Manager is using such an access list, Security Manager will still attempt to delete that object during deployment. This also applies to access lists that are used in FlexConfigs but are not used in any other policies managed by Security Manager.
Generate ACL Remarks During Deployment (IPv4 and IPv6 access rules.)	Whether to display ACL warning messages and remarks during deployment.
Preserve Sections for Access Rules	Whether to deploy the section name under which access rules are organized. This option ensures that if a device is discovered or rediscovered, the section names will not be lost.
Generate CSM Rule Number	Whether to deploy the rule number used in the Cisco Security Manager user interface. This option helps in correlating an access rule in a device configuration to its position in rule table.
Object Group Parameters	
Remove Unreferenced Object Groups from Device (PIX, ASA, FWSM, IOS 12.4(20)T+) (IPv4 and IPv6 objects.)	Whether Security Manager should remove object groups that are not being used by other CLI commands managed by Security Manager from devices during deployment. Object groups include network/host, service, and identity user groups. **Note** After enabling this option, Security Manager will remove objects during deployment that are not used in any policies managed or discovered by Security Manager. If any policy that is NOT discovered or managed by Security Manager is using such an object, Security Manager will still attempt to delete that object during deployment. In such cases, deployment will fail with a transcript error indicating that it was unable to delete the object. **Tip** Network/host objects that include object NAT configurations on ASA 8.3+ devices are never considered unreferenced.

Table 11-11 Deployment Page (continued)

Element	Description
Create Object Groups for Policy Objects (PIX, ASA, FWSM, IOS 12.4(20)T+) Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM, IOS 12.4(20)T+) Optimize Network Object Groups During Deployment (PIX, ASA, FWSM, IOS 12.4(20)T+) (IPv4 and IPv6 objects.)	Whether Security Manager should create object groups, such as network objects, service group objects, and identity user group objects, to replace comma-separated values in a rule table cell for the indicated devices. When deselected, Security Manager flattens the object groups to display the IP addresses, sources and destinations, users, ports, and protocols for these devices. **Tip** These options do not apply to host, network, or address range network/host objects, or to service objects (as opposed to service group objects), which are always created as objects. Multiple FQDN network objects can be grouped into a single network object. If you select this option, you can also select these options: • Create Object Groups for Multiple Sources, Destinations or Services in a Rule—Whether to automatically create network objects, service objects, and identity user group objects to replace comma-separated values in a rule table cell that resulted when multiple rules were combined. The objects are created during deployment and are in the format of 'CSM_INLINE...' for example, 'CSM_INLINE_src_rule_8589960758'. For more information, see Combining Rules, page 12-22. • Optimize Network Object Groups During Deployment—Whether to optimize network object groups by making them more succinct. For more information on optimizing policy objects, see Optimizing Network Object Groups When Deploying Firewall Rules, page 12-35.
IPS Parameters	
Generate transcripts for IPS Auto-Update Jobs	
Attach transcripts to email for IPS Auto-Update Jobs	

Table 11-11 Deployment Page (continued)

Element	Description
Remove Unreferenced Signature and Event Action Variables from IPS Device (IPS Parameters object group)	Whether to delete the unused variables from the sensor (IPS device) configuration during the next deployment. IPS Event and Signature Variables are defined as policy objects in Security Manager. Disabled by default (checkbox is cleared by default); that is, do not remove the unreferenced variables. Applies to the following variables; applies to both IPv4 and IPv6: • signature source and destination addresses • signature service port variables in signature engine parameters • victim and attacker addresses in event action filters • network information target addresses Does not apply to the following variables: • signature source port • OS identification address • signature destination port
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Device Communication Page

Use the Device Communication page to define default settings for communicating with devices. These settings mainly affect device inventory and policy discovery and configuration deployment. You can override the transport settings for individual devices in the device properties for the device.

If you change the transport protocol settings, ensure that your devices are appropriately configured to accept those types of connections.

Navigation Path

Select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents.

Related Topics

- Adding Devices to the Device Inventory, page 3-7
- Chapter 3, “Managing the Device Inventory”
- Chapter 2, “Preparing Devices for Management”
- Viewing or Changing Device Properties, page 3-40

Field Reference

Table 11-12 Device Communication Page

Element	Description
Device Connection Parameters	
Device Connection Timeout	The number of seconds that Security Manager has to establish a connection with a device before timing out.
Retry Count	The number of times that Security Manager should try to establish a connection to a device before concluding that the connection cannot be completed. The default value is 3.
Socket Read Timeout	For SSH and Telnet sessions, the maximum number of seconds Security Manager can wait for incoming data before concluding that the connection is lost.
Transport Protocol (IPS)	The default transport protocol for IPS sensors and routers that include the IPS feature. The default is HTTPS.
Transport Protocol (IOS Routers 12.3 and above)	The default transport protocol for routers that run Cisco IOS software release 12.3 and above. The default is HTTPS.
Transport Protocol (Catalyst Switch/7600)	The default transport protocol for Catalyst 6500/7600 devices and all other Catalyst switches, regardless of the Cisco IOS software version running on the devices. The default is SSH.
Transport Protocol (IOS Routers 12.2, 12.1)	The default transport protocol for routers that run Cisco IOS software releases 12.1 and 12.2. The default is Telnet.
Connect to Device Using	The type of credentials Security Manager should use when accessing devices. For more information, see Understanding Device Credentials, page 3-4. • **Security Manager User Login Credentials**—Security Manager contacts the device using the credentials that you entered while logging in to Security Manager. The same set of credentials are used for all devices regardless of the credentials configured for each device on the Device Credentials page. • **Security Manager Device Credentials**—Security Manager contacts the device using the credentials specified in the Device Properties Credentials page. This is the default. **Caution** You must use Security Manager Device Credentials, not Security Manager User Login Credentials, if a connection to an IPS sensor is involved. When Security Manager contacts an IPS sensor, it must use device credentials whether or not someone is logged in to Security Manager.
SSL Certificate Parameters	

Table 11-12 Device Communication Page (continued)

Element	Description
Device Authentication Certificates (IPS) Device Authentication Certificates (Router) PIX/ ASA/ FWSM Device Authentication Certificates Add Certificate button	How to handle device authentication certificates for SSL (HTTPS) communications. You can configure different behaviors for different types of devices, but the settings have the same meaning: • **Retrieve while adding devices**—Security Manager automatically obtains certificates from the devices while you add devices from the network or from an export file. • **Manually add certificates**—Security Manager does not automatically accept certificates from the device. Click **Add Certificate** to open the Add Certificate dialog box (see Add Certificate Dialog Box, page 11-24) where you can manually add the thumbprint before you try to add the device from the network or from an export file. You can also add certificates for devices that you create manually from the Device Properties Credentials page to be successful. For more information, see Manually Adding SSL Certificates for Devices that Use HTTPS Communications, page 9-5. • **Do not use certificate authentication**—Security Manager ignores device authentication certificates. This option leaves your system vulnerable to third-party interference with device validation. We recommend that you do not use this option.
Accept Device SSL Certificate after Rollback	For devices that use SSL, whether to obtain the certificate installed on an IPS device, firewall device, FWSM, ASA, or Cisco IOS router from the device when you roll back the configuration on the device.
HTTPS Port Number	The default port number that the device uses for secure communication with Security Manager (as well as other management applications that use these protocols). This value overrides the HTTPS port number that you configure in the HTTP policy for a device. **Note** If you configure the local HTTP policy to be a shared policy and assign the HTTP policy to multiple devices, the HTTPS port number setting in the shared policy overrides the port number configured in the Device Properties Credentials page for all devices to which the policy is assigned. In addition to providing access to the device through the Cisco web browser user interface, the HTTPS port number is used by device management applications (such as the Cisco Router and Security Device Manager (SDM)) and monitoring tools to communicate with the device. **Note** The security appliance can support both SSL VPN connections and HTTPS connections for device manager administrative sessions simultaneously on the same interface. Both HTTPS and SSL VPN use port 443 by default. Therefore, to enable both HTTPS and SSL VPN on the same interface, you must specify a different port number for either HTTPS or WebVPN. An alternative is to configure SSL VPN and HTTPS on different interfaces.

Table 11-12 Device Communication Page (continued)

Element	Description
Overwrite SSH Keys	Whether Security Manager can overwrite the SSH key for a device when it changes on the device. For SSH connections, a correct key is required for successful communication. Deselect this check box with caution, and only if you require a greater level of security. Security Manager does not communicate with the device if keys are changed on the device.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Add Certificate Dialog Box

Use the Add Certificate dialog box to add device certificates manually for devices that use the SSL transport protocol (firewall devices, FWSMs, ASAs, IPS devices, and Cisco IOS devices). Adding the device certificates manually gives you the highest level of security because then an intruder is prevented from introducing a fraudulent certificate thumbprint. Device certificates are stored in the database to be used for device authentication.

For more information about manually adding SSL certificates, see Manually Adding SSL Certificates for Devices that Use HTTPS Communications, page 9-5.

Navigation Path

Select **Tools > Security Manager Administration**, select **Device Communication** from the table of content, and click **Add Certificate**.

Field Reference

Table 11-13 Add Certificate Dialog Box

Element	Description
Host Name or IP Address	The hostname or IP address of the device for which you are adding the certificate.
Certificate Thumbprint	The certificate thumbprint, which is a string of hexadecimal digits that is unique to the device.

Device Groups Page

Use the Device Groups page to manage the device groups and group types defined in the device inventory.

Navigation Path

Select **Tools > Security Manager Administration**, then select **Device Groups** from the table of contents.

Related Topics

- Understanding Device Grouping, page 3-60
- Working with Device Groups, page 3-59

Field Reference

Table 11-14 Device Groups Page

Element	Description
Groups	Displays the device groups and group types. To rename a group or type, select it and then click it again to make the text editable. Type in the new name and press Enter.
Add Type button	Click this button to create a new group type. The type is added with a default name. Overtype the name and press Enter.
Add Group to Type button	Click this button to add a device group to the selected device group or group type.
Delete button (trash can)	Click this button to delete the selected device group or group type and all device groups that it contains. Deleting a device group or group type does not delete any devices it contains.
Save button	Saves your changes.
Reset button	Restores all fields to their previous values.

Discovery Page

Use the Discovery page to define how Security Manager should handle certain types of objects or events during inventory and policy discovery. You can also control how long Security Manager keeps discovery tasks.

Navigation Path

Select **Tools > Security Manager Administration** and select **Discovery** from the table of contents.

Field Reference

Table 11-15 Discovery Page

Element	Description
Prepend Device Name when Generating Security Context Names	Whether the name of the device that contains the security context should be added to the front of the security context's name. For example, if a security context is named admin, and it is contained in the device with the display name 10.100.15.16, the name that will appear in the Device selector is 10.100.15.16_admin. If you do not prepend the device name, the security context name appears in the inventory by itself. Because Security Manager does not place security contexts in a folder related to the parent device, the only way to easily see contexts that are related to a device is to prepend the device name. If you do not prepend device names, Security Manager adds a numbered suffix to distinguish identically named devices. For example, if the admin context exists in more than one firewall, you will see admin_01, admin_02, and so on, in the Device selector.
Purge Discovery Tasks Older Than	The number of days to save discovery and device-import tasks. Tasks older than the number of days you enter are deleted.
Reuse Policy Objects for Inline Values	Whether to substitute any named policy objects, such as network/host or identity user group objects already defined in Security Manager, for inline values in the CLI. For more information on policy objects, see Chapter 6, "Managing Policy Objects". **Tip** Although this option generally applies to network/host objects, it does not apply to FQDN network/host objects because you cannot specify a fully-qualified domain name (FQDN) as an inline value.
Allow Device Override for Discovered Policy Objects	For the types of objects for which overrides are possible, whether to allow users to override the parent object values at the device level for policy objects that are discovered. For example, if you select this option, if you run policy discovery on a device that has an ACL with the same name as an ACL policy object in Security Manager, the name of the discovered policy object is reused, but a device-level override is created for the object. If you deselect this option, a new policy object is created with a number appended to the name. **Tip** For objects that have subtypes, such as network/host and service, overrides are limited to within a type. For example, an override can be created for a network/host group when discovering a same-named network/host group, but no override would be created when discovering a same-named network/host address range. Instead, the newly-discovered object will have a number appended to the name. For more information, see Understanding Policy Object Overrides for Individual Devices, page 6-18.

Table 11-15 Discovery Page (continued)

Element	Description
On Error, Rollback Discovery for Entire Device	Whether Security Manager should roll back all discovered policies if even one error is encountered for a single policy during policy discovery. When deselected, Security Manager keeps the policies successfully discovered and discards only those policies with errors. For more information on policy discovery, see Discovering Policies, page 5-12.
Auto-Expand Object Groups with Prefixes	Expands object groups, such as network or identity user group, with the listed prefixes during the device import process. Separate the prefixes with a comma. This expansion causes the elements of the object group to display as separate items in the discovered policies. For more information, see Expanding Object Groups During Discovery, page 12-35. **Tip** This option does not apply to policy objects created from the **object network** or **object service** commands from ASA 8.3+ devices. These commands create host, FQDN, network, or address range network/host objects or service objects.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Event Management Page

Use the Event Management page to enable event management, which allows you to view ASA, FWSM, and IPS events using the Event Viewer. You can also configure settings required for event collection.

The Event Manager service is also required by the Report Manager application, which allows you to view reports that aggregate information collected by the service.

Tip If you get a message that Event Viewer is unavailable when you select Launch > Event Viewer, but the **Enable Event Management** option is selected on this page, try restarting the Event Manager Service. First, deselect the Enable option and click Save. Wait for the service to stop. Then, select the Enable option, click Save, and wait for the service to finish restarting. You can then try opening Event Viewer again.

Navigation Path

Click **Tools > Security Manager Administration** and select **Event Management** from the table of contents.

Field Reference

Table 11-16 Event Management Page

Element	Description
Event Management Options	
Enable Event Management	Whether to enable the Event Manager service, which allows Security Manager to collect event information. If you disable this feature, you cannot use the Event Viewer or Report Manager applications. **Tip** If you change this setting and click **Save**, you are prompted to confirm that you want to start or stop the Event Manager Service. If you click Yes, the service is started or stopped immediately, and you are shown a progress indicator and told when the change is completed. Wait until the status change is completed before continuing.
Event Data Store Location	The directory to use for collecting event information. This is known as the primary event store. Click **Browse** to select a directory on the Security Manager server. If the directory does not yet exist, create it in Windows Explorer. You cannot create the directory from within Security Manager. **Tip** If you change the location after you have started using the Event Manager service, you cannot query old events.
Event Data Store Disk Size	The amount of disk space you want to allocate for storing event data, in gigabytes (GB). Events are incrementally deleted (rotated out) from the extended store when it becomes 90% full. Before changing this setting, consider the following: • If you reduce the size below the amount of disk space already used by event data, the oldest events are deleted until your new size limit is reached. • You can see a visual representation of the amount of space currently used for event data. Open the Event Viewer (**Launch > Event Viewer**), then from Event Viewer, select **Views > Show Event Store Disk Usage**.
Event Syslog Capture Port	The port on which you want to enable syslog event capture. The default is 514. You must ensure that the Security Manager server, and intervening firewalls, allow incoming traffic on this port for Security Manager to collect the events. Managed devices must be configured to send syslog information to this port on the Security Manager server. **Tip** If you change this port, you must also change the Syslog Servers policies for all ASA and FWSM devices and security contexts that send events to Security Manager. For more information, see Syslog Servers Page, page 54-27.
Event Data Pagination Size	The maximum number of events per page each query response can contain. The default is 20000, but you can select a different size from the list of supported values. **Note** In Security Manager 4.10, the maximum number of events per page has been increased to 100000.

Table 11-16 Event Management Page (continued)

Element	Description
Extended Store Management Options	
Auto Copy Events to Extended Store	Whether you want to define an extended storage location for event storage. Events are copied from the regular event storage location to the extended location so that they remain available for use. When you query for historical events in Event Viewer, events in the extended storage location are automatically retrieved if they are needed. **Tip** You are prompted to verify that you want to start the extended service and to make changes to the extended storage location.
Extended Data Store Location	The location of the extended data store for events. This location can be on directly-attached storage that appears as a drive on the server and that uses DAS protocols. For example, SAN storage attached through fiber channel. CIFS storage is not supported. Click **Browse** to select the desired drive and directory. **Tips** • When you select an extended storage location and save your changes, Security Manager checks that it can be accessed and that it has write permissions. The primary storage location is used as a reference, and any data that exists in the primary storage location that does not exist in the extended storage location is copied to the extended storage location. Any data that already exists in the extended storage location is not evaluated and is left untouched, although it can be deleted later to make room for new data. • If you change the extended data store location, you cannot query events that exist only in the previous extended data store location (that is, you cannot query events that have already be removed from the primary location). If you want to preserve these events, copy the data from the old location to the new location.
Extended Data Store Disk Size	The amount of space you want to allocate to the extended event storage location, in gigabytes (GB). Events are incrementally deleted (rotated out) from the extended store when it becomes 90% full. The size must be equal to or larger than the primary event data storage location. You can see a visual representation of the amount of space currently used for event data. Open the Event Viewer (**Launch > Event Viewer**), then from Event Viewer, select **Views > Show Event Store Disk Usage**.

Table 11-16 Event Management Page (continued)

Element	Description
Error Notification Email IDs	The email addresses that should receive notifications if problems arise with the use of the extended storage location. Separate multiple addresses with commas. For notifications to be sent successfully, you must also configure an SMTP server as described in Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26. The message indicates the problem, cause, and recommended action. For example, you get notifications if the extended storage is chronically unreachable, if data copy fails repeatedly, or if a partition was deleted from the primary storage area before it could be copied to the extended storage area (which might happen if the storage is chronically unreachable or if there are persistent copy problems).
Syslogs for Failover Devices	
Process Syslogs from Failover Standby Device	Enables or disables processing of syslog messages from the standby ASA. When enabled, syslog messages generated by the standby or failover ASA will be displayed in the Device Identifier column in the Event Monitoring window. **Note** By default, the processing of syslog messages from the standby ASA is disabled.
Syslog Relay Service **Note** Staring with version 4.13, Cisco Security Manager supports syslogs over IPv6 in Event Viewer but the Syslog Relay Service will not be supported for syslogs over IPv6.	
Enable Syslog Relay Service	Enables or disables the Syslog Relay Service. Select the Enable Syslog Relay Service check box to enable the fields required for configuring the Syslog Relay Service.

Table 11-16 Event Management Page (continued)

Element	Description
Syslog Relay Capture Port	Specifies the UDP port on which the Syslog Relay Service listens for syslogs. The default is 514. If the Syslog Relay Service is enabled, devices must send syslogs to the Syslog Relay Capture Port so that they can be forwarded to the local collector and remote collectors. If the Syslog Relay Service is turned off, devices should send syslogs to the Event Syslog Capture Port. **Note** The Syslog Relay Capture Port and the Event Syslog Capture Port cannot be the same. When enabling the Syslog Relay Service, if devices are currently configured to send syslogs to the Event Syslog Capture Port, you should instead use that port number for the Syslog Relay Capture Port and then change the Event Syslog Capture Port to something else. You must ensure that the Security Manager server, and intervening firewalls, allow incoming traffic on this port for Security Manager to collect the events. Managed devices must be configured to send syslog information to this port on the Security Manager server. **Tip** If you change this port, you must also change the Syslog Servers policies for all ASA and FWSM devices and security contexts that send events to Security Manager. For more information, see Syslog Servers Page, page 54-27.
Relay to Local Event Collector	Enables or disables syslog relay for the local event collector.
Relay to Remote Collector 1	Enables or disables syslog relay for Remote Collector 1.
Collector 1 IP address	Specifies the IP address to which syslogs should be sent for Remote Collector 1.
Collector 1 Syslog Capture Port	Specifies the UDP port on which Remote Collector 1 is listening for relayed syslogs.
Relay to Remote Collector 2	Enables or disables syslog relay for Remote Collector 2.
Collector 2 IP address	Specifies the IP address to which syslogs should be sent for Remote Collector 2.
Collector 2 Syslog Capture Port	Specifies the UDP port on which Remote Collector 2 is listening for relayed syslogs.

Table 11-16 Event Management Page (continued)

Element	Description
Device Filter	You can filter the devices for which syslogs should be relayed for a specific collector. Using this feature, you can configure syslogs for one set of devices to go to one collector and syslogs for a different set of devices to go to another collector: 1. Select the tab (Local Collector, Remote Collector 1, or Remote Collector 2) for which you want to filter devices. 2. To specify the devices for which you want relay syslogs for this collector, select **Permit Relay**. If instead you want to specify the devices for which you want to disable syslog relay for this collector, clear the **Permit Relay** check box. If the Permit Relay check box is **not** selected, then syslogs for the devices you add to the filter will not be relayed; however, syslogs for all other devices will be relayed. **Note** For each enabled collector, syslog relays from all devices are enabled by default. **Note** When adding a cluster to the filter list, the IP addresses for the cluster management pool will be included as part of filter configuration. 3. Select the devices or device groups from the Available Devices list that you want to add to the filter and click >> to move them to the Selected Devices list. For more information on selecting devices, see Using Selectors, page 1-45. 4. To add a device that is not managed in Security Manager, enter the IP address of the device in the Add Special Device field and then click the bottom >> to move the device to the Selected Devices list.
Restart	Restarts the Syslog Relay Service.
CPU Throttle Settings	Opens the CPU Throttling Policy dialog box in which you can control the CPU load used by the syslog relay service. For more information, see CPU Throttling Policy Dialog Box, page 11-33.
View Statistics	Opens the Syslog Relay Statistics dialog box in which you can see the average CPU and memory usage of the syslog relay service process as well as traffic rates for the different collectors. For more information, see Syslog Relay Statistics Dialog Box, page 11-35.
Save button	Saves and applies changes. Most changes related to the Event Viewer settings require that the Event Manager service briefly stop and then restart. If you change whether the service is enabled, it stops or starts, as appropriate. You are shown a progress indicator. Changes to Syslog Relay Service settings require that the Syslog Relay Service briefly stop and then restart. If you change whether the service is enabled, it stops or starts, as appropriate.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Troubleshooting Syslog Relay Servers

If the Syslog Relay Service is enabled, devices must send syslogs to the Syslog Relay Capture Port so that they can be forwarded to the local collector and remote collectors. If the Syslog Relay Service is turned off, devices should send syslogs to the Event Syslog Capture Port.

Syslog Relay Servers act as an intermediate connection between device events and Security Manager Event Manager application. It receives device event packets and forwards them to the Local Collectors and Remote Collectors.

Device Management via IP

To manage devices in Security Manager via IP (using IPv4 or IPv6), the Device Management interface must have the appropriate IP information.

For example, see the following sample configuration.

```
!
interface Management1/1
management-only
nameif management
security-level 100
ip address 10.197.87.95 255.255.255.0
ipv6 address 2016::b2aa:77ff:fe7c:a068/64
ipv6 enable
```

In this configuration, the Device Management IP address has both IPv4 and IPv6 management addresses. So you can manage a device via IPv4 or IPv6.

Problem:

If a device is managed via IPv6 Management Address in Security Manager, the communication between Security Manager and the device would occur only via IPv6 address and not IPv4 address.

However, Event Syslog server still sends the Event Syslog packets only to IPv4 address, therefore in this scenario Security Manager cannot map the equivalent device for the received IPv4 Event Syslog packets.

When you add a filter device in Local Collector or Remote Collector for Syslog Relay Services in **Tools > Security Manager Administration > Event Management - Syslog Relay Service**, Security Manager tries to extract the device Management IPv4 address instead of the IPv6 management address.

However, there is no IPv4 Management Interface configured in the device. Therefore, Security Manager displays the following error:

```
Device selection – Ipv4 address not found for device(s)
```

Solution:

Go to **Device View > Policies > Interfaces**, to configure the device Management Interface with IPv4 address.

CPU Throttling Policy Dialog Box

Use the CPU Throttling Policy dialog box to specify settings for controlling the CPU load used by the syslog relay service.

After CPU throttling is enabled, if the syslog relay service's average CPU usage over the time period selected in the Average Max CPU Usage Time field is greater than the Maximum CPU Usage threshold, then CPU throttling will take place for the collectors specified in the Stop Forwarding To field for the time specified in the Stop Forwarding For field.

Note You can use the Syslog Relay Statistics dialog box to see the number of syslog packets dropped per collector due to the throttle policy (see Syslog Relay Statistics Dialog Box, page 11-35).

Navigation Path

Click **Tools > Security Manager Administration**, select **Event Management** from the table of contents, and then click **CPU Throttle Settings**.

Field Reference

Table 11-17 CPU Throttling Policy Dialog Box

Element	Description
Enable CPU Throttling	Whether to enable throttling for the syslog relay service. CPU throttling for the syslog relay service is disabled by default.
Maximum CPU Usage	Specify the maximum CPU usage for the syslog relay service as a percentage of total CPU capacity. This is threshold at which CPU throttling will be initiated.
Average Max CPU Usage Time (Minutes)	Specifies the time in minutes for which CPU usage by the syslog relay service is calculated. Options are 1 minute, 5 minutes, and 15 minutes. This average is compared to the Maximum CPU Usage value to determine whether throttling should take place.
Stop Forwarding To	Specify the collectors for which you want to stop forwarding syslogs when throttling is engaged.
Stop Forwarding For	Specify how long, in minutes, throttling should be enabled when the threshold is hit. After the specified interval of time has elapsed, if the CPU usage is still above the Maximum CPU Usage threshold, throttling will remain in effect.
Enable Email Notifications	Whether to send email notifications when the syslog relay service enters or exits throttle mode. Email notifications are disabled by default. For the e-mails to be sent, you must configure an SMTP server as described in Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26.
Notification Email IDs	Enter one or more valid addresses in the Notification Email IDs field; separate multiple addresses with commas.

Table 11-17 CPU Throttling Policy Dialog Box (continued)

Element	Description
Send Email	Specify how often to send notification emails: • **Every time**—Select this option to have a notification sent every time the syslog relay service enters or exits throttle mode. If the CPU usage is still above the Maximum CPU Usage threshold after the Stop Forwarding For timer has elapsed, throttling will remain in effect and an additional notification will be sent. • **Every**—Select this option to have at most one notification sent when the syslog relay service enters or exits throttle mode during a specific period of time. If you select this option, specify the time period by entering the number of minutes or hours and then selecting the corresponding option (Min/Hour) from the drop-down list.

Syslog Relay Statistics Dialog Box

Use the Syslog Relay Statistics dialog box to view the average CPU and memory usage of the syslog relay service process as well as traffic rates for the different collectors.

Navigation Path

Click **Tools > Security Manager Administration**, select **Event Management** from the table of contents, and then click **View Statistics**.

Field Reference

Table 11-18 Syslog Relay Statistics Dialog Box

Element	Description
Log Relay Service	
Memory Usage Average (last 1 min.)	Shows the amount of memory used by the syslog relay service on average over the last minute.
CPU Usage Average (last 1 min.)	Shows the percentage of CPU capacity used by the syslog relay service on average over the last minute. **Tip** If the average CPU usage is too high, you might consider enabling CPU throttling for the syslog relay service (see CPU Throttling Policy Dialog Box, page 11-33).
Total sylog packets received	Shows the total number of syslog packets that have been received by the syslog relay service since the service was started.
Average syslog received per second since start	Shows the average number of syslog packets that have been received by the syslog relay service per second since the service was started.
Average syslog received per second for last 1 minute	Shows the average number of syslog packets that have been received by the syslog relay service per second over the last minute.
Average syslog received per second for last 5 minute	Shows the average number of syslog packets that have been received by the syslog relay service per second over the last five minutes.

Table 11-18 Syslog Relay Statistics Dialog Box (continued)

Element	Description
Average syslog received per second for last 15 minute	Shows the average number of syslog packets that have been received by the syslog relay service per second over the last fifteen minutes.
Period (in mins.) for which throttle policy is active	Shows how long, in minutes, the CPU throttle policy for the syslog relay service has been active. For more information, see CPU Throttling Policy Dialog Box, page 11-33.
Local Collector/Remote Collector 1/Remote Collector 2	
Total syslog packets sent successfully	Shows the total number of syslog packets that have been sent by the syslog relay service since the service was started.
Total syslog packets dropped (filter policy)	Shows the total number of syslog packets that have been dropped by the syslog relay service in accordance with the defined filter policy since the service was started.
Total syslog packets dropped (throttle policy)	Shows the total number of syslog packets that have been dropped by the syslog relay service in accordance with the throttle policy since the service was started.
Total syslog packets failed during transmit	Shows the total number of syslog packets that were not able to be forwarded by the syslog relay service since the service was started.
Average syslog sent per second since start	Shows the average number of syslog packets that have been sent by the syslog relay service per second since the service was started.
Average syslog sent per second for last 1 minute	Shows the average number of syslog packets that have been sent by the syslog relay service per second over the last minute.
Average syslog sent per second for last 5 minute	Shows the average number of syslog packets that have been sent by the syslog relay service per second over the last five minutes.
Average syslog sent per second for last 15 minute	Shows the average number of syslog packets that have been sent by the syslog relay service per second over the last fifteen minutes.
Refresh	Refreshes the statistics displayed on the Syslog Relay Statistics dialog box.

Health and Performance Monitor Page

Use the Health and Performance Monitor page of the Security Manager Administration window to enable network-wide health and performance monitoring. The Health and Performance Monitor (HPM) is a stand-alone application that lets you monitor key health and performance data for ASA devices, IPS devices, and VPN services by providing network-level visibility into device status and traffic information.

Tip If you get a message that the application is unavailable when you attempt to launch the Health and Performance Monitor, but the **Enable Health and Performance Monitor** option is selected on this page, try restarting Health and Performance Monitoring. First, deselect the Enable option and click Save. Wait for the service to stop. Then, select the Enable option, click Save, and wait for the service to finish restarting. You can then try opening the HPM application again.

Navigation Path

Click **Tools > Security Manager Administration** and select **Health and Performance Monitor** from the table of contents.

Field Reference

Table 11-19 Health and Performance Monitor Page

Element	Description
Enable Health and Performance Monitor	Lets you enable or disable the Health and Performance Monitoring service, which allows Security Manager to collect event information. If you disable this feature, you cannot use the HPM application. **Tip** If you change this setting and click **Save**, you are prompted to confirm that you want to start or stop the Health and Performance Monitoring service. If you click Yes, the service is started or stopped immediately, and you are shown a progress indicator and told when the change is completed. Wait until the status change is completed before continuing.
OOB Notification Settings **Note** To receive email notifications make sure that an SMTP server has been configured on the Security Manager Server. For more information, see, Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26 Cisco Security Manager considers an out-of-band (OOB) change to be any change made to a device manually or outside of Security Manager control, for example, by logging into the (monitored) device directly and entering configuration commands through the CLI. For devices monitored by the HPM application, Cisco Security Manager monitors the OOB changes, detected by the HPM periodically. If any out-of-band changes are detected, HPM generates an alert displayed on the **Device Status View** page and sends an email, to the configured recipients. **Note** If a Cisco Security Manager restart occurs during the update time, after an OOB change is detected and an email notification has already been sent, the same email maybe sent again after Cisco Security Manager starts up.	
Enable OOB Email Notification	Lets you enable or disable email notifications for Out of Band changes. **Note** When the email notification is disabled, only an alert is displayed on the **Device Status View** page. **Note** When HPM detects the OOB change and syncs with the Configuration Manager, a separate email alert notification is sent for each device being monitored. To prevent duplication, emails sent for each OOB change are tracked and stored in a file, once in 5 minutes. **Tip** The default tracking time is set as 5 minutes in the Cisco Security Manager properties file. You can update this as needed.
Recipient E-mail(s)	Specify the recipients who must be notified of the OOB change.

Table 11-19 Health and Performance Monitor Page (continued)

Element	Description
Save button	Saves and applies changes. Most changes require that the Health and Performance Monitoring service briefly stop and then restart. If you change whether the service is enabled, it stops or starts, as appropriate. You are shown a progress indicator.
Reset button	Resets changes to the last saved values.

Report Manager Page

Use the Report Manager page of the Security Manager Administration window to enable or disable the Report Manager feature in Cisco Security Manager. Report Manager is a stand-alone application that lets you view security and usage reports for devices and remote access IPsec and SSL VPNs.

Navigation Path

Click **Tools > Security Manager Administration** and select **Report Manager** from the table of contents.

Field Reference

Table 11-20 Health and Performance Monitoring Page

Element	Description
Enable Report Manager	Lets you enable or disable the Report Manager service. If you disable this feature, you cannot use the Report Manager application. **Tip** If you change this setting and click **Save**, you are prompted to confirm that you want to start or stop the Report Manager service. If you click Yes, the service is started or stopped immediately, and you are shown a progress indicator and told when the change is completed. Wait until the status change is completed before continuing.
Save button	Saves and applies changes. If you change whether the service is enabled, it stops or starts, as appropriate. You are shown a progress indicator.
Reset button	Resets changes to the last saved values.

Identity Settings Page

Use the Identity Settings page to configure the Active Directory (AD) server group to use for a NetBIOS domain for use with identity-aware firewall policies on ASA devices. These settings enable you to use the Find feature when selecting users or user groups for identity-aware policies or identity user group policy objects.

Tip You can also add entries by configuring the Identity Options policy on an ASA. When you save the policy, you are asked if you want to update the identity settings administrative page. Keep in mind that you can have a single domain-to-AD server match on the settings page, whereas you can configure different ASAs to use different server groups for a domain. Username lookup always selects the AD servers defined in the identity settings administrative page, regardless of what server group is configured for the individual ASA that you are configuring.

Navigation Path

Select **Tools > Security Manager Administration** and select **Identity Settings** from the table of contents.

Related Topics

- Creating Identity User Group Objects, page 13-19
- Selecting Identity Users in Policies, page 13-21

Field Reference

Table 11-21 Identity Settings Page

Element	Description
Domain-AD Server Group Mapping table.	Each row in the table defines the Active Directory (AD) server group to use for a NetBIOS domain for use with identity-aware firewall policies on ASA devices. • To add an entry, click the **Add Row (+)** button and fill in the Add AD Domain Server dialog box. See Domain AD Server Dialog Box, page 13-10. You need to enter the domain name and select the AAA server group object that specifies the LDAP AD servers. • To edit an entry, select it and click the **Edit Row (pencil)** button. • To delete an entry, select it and click the **Delete Row (trash can)** button. • To test whether Security Manager can successfully contact the servers defined in a server group, select the row and click **Test.**

Table 11-21 Identity Settings Page (continued)

Element	Description
Default Domain	The NetBIOS domain to use when you do not type in a domain when specifying a user or group name in a firewall policy or an identity user group policy object. The default is LOCAL, which means the name is defined on the ASA itself, either as a local user or as a VPN user who was authenticated by a means other than an LDAP server group associated with a domain name. Other than LOCAL, only domains configured in the Domain-AD Server Group Mapping table appear in this list. **Tip** This setting is not related to the default domain configured on the ASA using the user-identity default-domain command. This setting is a convenience setting to allow you to type in usernames without always having to include the domain name. Select the domain for which you will most often type user names.
Route query via	When you use the Find feature while selecting users or user groups, Security Manager must query the AD server. Select whether the query comes from the Security Manager client (the workstation on which you are running the client) or the server. By default, LDAP queries come from the client.
For user strings without domain	If you select something other than LOCAL for the default domain, how to handle username or user group names that you type in without a domain name: • **Auto determine user/user-group from AD**—Check the AD server associated with the default domain to determine whether the name is for a user or user group, and add the appropriate string: Default-Domain\user or Default-Domain\\user-group. If the name cannot be found, you must manually type in the domain name and the one or two \ characters to indicate whether the name is for a user or a group. • **Change it to Default-Domain/user**—Assume that typed in names are user names, not user group names, and add the default domain: Default-Domain\user. **Tip** When typing, if you precede the name with \ or \\, the default domain is automatically added. Thus, if you select the Change it to Default-Domain/user option, you can still enter group names without typing the domain by first entering \\.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Image Manager Page

Use the Image Manager page to control the administrative settings for Image Manager within Security Manager.

Navigation Path

Select **Tools > Security Manager Administration** and select **Image Manager** from the table of contents.

Field Reference

Table 11-22 Image Manager Page

Element	Description
Edit CCO Settings	Use the Edit CCO Settings link to quickly navigate to the CCO Settings page. For information on the CCO Settings page, see CCO Settings Page, page 11-4.
Purge Jobs Older Than	Enter the length of time in days to hold Image Manager jobs before purging them. The default is 365 days. Select **Purge Now** to immediately clear previous Image Manager job specifications.
Include Repository	If checked, the image repository is part of Security Manager backup. The default is to exclude images.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

IP Intelligence Settings Page

Use the IP Intelligence Settings page to control the administrative settings for the IP Intelligence features within Security Manager.

Navigation Path

Select **Tools > Security Manager Administration** and select **IP Intelligence Settings** from the table of contents.

Field Reference

Table 11-23 IP Intelligence Settings Page

Element	Description
Edit CCO Settings	Credentials for connecting to Cisco.com are required for automatic updates of the GeoIP database. You can use the **Edit CCO Settings** link to quickly navigate to the CCO Settings page where these credentials are configured. You can also configure settings for a proxy server on the CCO Settings page. For information on the CCO Settings page, see CCO Settings Page, page 11-4.

Table 11-23 IP Intelligence Settings Page (continued)

Element	Description
Reverse DNS (FQDN)	
Enable Reverse DNS (FQDN) Lookup Service	Whether to enable or disable the Reverse DNS (FQDN) lookup service. Enable this service if you want to be able to determine the fully qualified domain name (FQDN) for an IPv4 address using the IP Intelligence tool.
Use CSM Server's DNS Server	Select this option to use the DNS server defined on the Cisco Security Manager server for reverse DNS lookup requests.
Use custom DNS servers	Select this option to manually specify the DNS servers to use for reverse DNS lookup requests. You can enter up to three DNS server addresses in the fields provided. **Note** Security Manager does not support the use of external DNS servers configured inside of a virtual machine.
Enable Load Balancing	Whether to distribute reverse DNS lookup requests amongst the DNS servers when multiple DNS servers are available.
Default Blocking Ranges	Lists the IP address ranges that are excluded from Reverse DNS lookup by default: 0.0.0.0, 255.255.255.255, 127.0.0.1, 169.254.0.0-169.254.255.255, 224.0.0.0-239.255.255.255
User-defined Blocking Ranges	Specifies additional IP addresses or address ranges that should be excluded from reverse DNS lookup requests. Click the Edit (pencil) button to open the Edit IPv4 Blocking Range Addresses dialog box in which you can specify the IPv4 addresses or address ranges to be excluded. Separate multiple entries using a comma ",".
GeoIP	
Enable GeoIP Lookup Service	Whether to enable or disable the GeoIP lookup service. Enable this service if you want to be able to retrieve geographic location information for an IPv4 address using the IP Intelligence tool. **Note** You will need to download the geographic location database from Cisco.com before GeoIP information will be included in the IP intelligence data. You will also need to download the geographic location database from Cisco.com after restoring the Security Manager database from a backup. Beginning with version 4.9, Security Manager mandates you to read and accept the End User License Agreement (EULA) before you can proceed to downloading updates from cisco.com.
GeoIP Manual Upload Use the GeoIP Manual Upload fields to update the geographic location database in Security Manager using a MaxMind GeoLite City update package downloaded from Cisco.com. **Note** New update packages are made available on Cisco.com on a monthly basis.	

Table 11-23 IP Intelligence Settings Page (continued)

Element	Description
GeoIP Database Artifact Location	Click **Browse** and then navigate to and select the MaxMind GeoLite City update package that you downloaded from Cisco.com. Then, click **Upload** to upload the selected database to Cisco Security Manager. **Note** Geolocation updates obtained directly from MaxMind or any other source are not supported in Cisco Security Manager.
GeoIP Maxmind Database Update Settings MaxMind GeoLite City update packages are updated monthly on Cisco.com. Use the GeoIP Maxmind Database Update Settings to download an update package automatically from Cisco.com and to configure scheduled updates. **Note** Credentials for connecting to Cisco.com are required for automatic updates of the geographic location database. You can use the **Edit CCO Settings** link to quickly navigate to the CCO Settings page where these credentials are configured. For information on the CCO Settings page, see CCO Settings Page, page 11-4.	
Run immediate database update	Click **Update Now** to update the geographic location database in Security Manager using the latest update package from Cisco.com.
Enable scheduled update	Whether to enable or disable automatic updates of the geographic location database on a regular schedule. After enabling scheduled updates, click **Edit Settings** to specify the schedule for when the update should take place. Using the Weekly option, you can specify the days of the week on which the automatic update should take place. Using the Monthly option, you can specify the day of the month on which the automatic update should take place. For either option, you can specify the time of day that the update should take place. **Tip** The geographic location database is updated by MaxMind on the first Tuesday of every month. New update packages are typically available on Cisco.com approximately one week after they are issued by MaxMind. We recommend configuring your update schedule to occur monthly on day 15 or later. However, you can schedule the updates to take place more frequently if you want to ensure that the updated database is made available in Security Manager as close to the time it is available on Cisco.com as possible. **Note** Beginning with version 4.9, Security Manager mandates you to read and accept the End User License Agreement (EULA) before you can proceed to downloading updates from cisco.com.
Default Blocking Ranges	Lists the IP address ranges that are excluded from GeoIP lookup by default: 0.0.0.0, 255.255.255.255, 127.0.0.1, 10.0.0.0-10.255.255.255, 169.254.0.0-169.254.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255, 224.0.0.0-239.255.255.255

Table 11-23 IP Intelligence Settings Page (continued)

Element	Description
User-defined Blocking Ranges	Specifies additional IP addresses or address ranges that should be excluded from GeoIP lookup requests. Click the Edit (pencil) button to open the Edit IPv4 Blocking Range Addresses dialog box in which you can specify the IPv4 addresses or address ranges to be excluded. Separate multiple entries using a comma ",".
Whois	
Enable Whois Lookup Service	Whether to enable or disable the Whois lookup service. Enable this service if you want to be able to retrieve WHOIS information for an IPv4 address using the IP Intelligence tool.
Enable External Proxy	Whether to enable or disable use of an external proxy for Whois requests. Proxy server configuration is specified on the CCO Settings page. **Tip** You can use the **Edit CCO Settings** link to quickly navigate to the CCO Settings page where the proxy server settings are configured. For information on the CCO Settings page, see CCO Settings Page, page 11-4.
Default Blocking Ranges	Lists the IP address ranges that are excluded from Whois lookup by default: 0.0.0.0, 255.255.255.255, 127.0.0.1, 10.0.0.0-10.255.255.255, 169.254.0.0-169.254.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255, 224.0.0.0-239.255.255.255
User-defined Blocking Ranges	Specifies additional IP addresses or address ranges that should be excluded from Whois lookup requests. Click the Edit (pencil) button to open the Edit IPv4 Blocking Range Addresses dialog box in which you can specify the IPv4 addresses or address ranges to be excluded. Separate multiple entries using a comma ",".
View Statistics	Opens the IP Intelligence Statistics dialog box which shows statistics for the IP Intelligence feature. Information provided in the IP Intelligence Statistics dialog box includes: • Average number of IP Intelligence lookup requests during the last 5 minutes and last 15 minutes • Average lookup time for all IP Intelligence service requests • Average lookup times for each individual service that is currently enabled • Counts of the number of lookups, both successful and failed, for each individual service that is currently enabled • Cache hit ratios for each individual service that is currently enabled • Upload information for GeoIP updates: last update time, status, and version information for the update Click **Refresh** to update the data in the IP Intelligence Statistics dialog box.
Save button	Saves your changes.

Table 11-23 IP Intelligence Settings Page (continued)

Element	Description
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Eventing Notification Settings Page

Use the Eventing Notification Settings page to receive email notifications for IPS events and critical ASA events. You can configure the time interval at which you want to receive the email notifications.

The events are sent in the form of .CSV files in a .zip file format. By default, email notification is disabled. When you enable email notification, only the notification for IPS events is enabled. To receive email notification for critical events you must enable the additional settings for critical events.

Note For notifications to be sent successfully by Security Manager, you must configure an SMTP server, as described in Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26.

Tip You can also use the Security Manager Event Viewer application or the Dashboard to view and monitor all events.

Navigation Path

Select **Tools > Security Manager Administration** and select **Eventing Notification Settings** from the table of contents.

Field Reference

Table 11-24 Eventing Notification Settings Page

Element	Description
Enable Eventing Email Notification	Select to enable notification of IPS events through email.
Notification Interval (15 - 60 minutes)	Enter the interval at which you want Security Manager to send email notifications for IPS events or critical events. **Note** If Security Manager receives more than 50000 events during the configured time interval, only the first 50000 events are selected and sent through email.
Notification Settings (IPS)	
Email IDs (for IPS Events)	Enter one or more email addresses (comma separated).
Select Severity of Events	The severity level that the IPS signature reports: High, Medium, Low, or Informational. By default, High and Medium severity are selected.
Notification Content	Whether to send summarized or detailed notifications through email. If you select Detailed Notifications, select the fields that you want information for, in the email notification. Some fields are selected by default.

Table 11-24 Eventing Notification Settings Page (continued)

Element	Description
Fields	
Event ID	A unique sequential number for each event, assigned internally.
Severity	The Firewall or IPS severity values.
Device	The source of the event; usually the device ID. A device identified as Not Available has been deleted from the Security Manager inventory.
Application Name	The name of the application originating the event.
Receive Time	The time the event was received by Security Manager.
Event Time	The time the event was generated by the device.
Sensor Local Time	The local time of the sensor where the event originated.
Sig ID	The Sig ID value is used by the alert originator to identify the activity. It identifies the pre-defined signature defined for this activity.
Sub Sig. ID	Identifies the unique numerical value assigned to the sub signature. The Sub Sig. Id identifies a more granular version of a broad signature.
Sig. Name	The name assigned to the signature.
Sig. Details	The details of the reported signature that was triggered and resulted in the generation of the alert.
Sig. Version	The version of the signature definition used to generate an alert.
Attacker IP	The IP address of the host that sent the offending packet.
Attacker Port	The port used by the attacker host. This is the port from which the offending packet originated.
Attacker Locality	Identifies whether the attacker address is located inside or outside of a given network, as specified by the intrusion detection device's configuration.
Victim IP	The IP address of the host being attacked.
Victim Port	The port of the host being attacked (the recipient of the offending packet). This is the port to which the offending packet was sent.
Victim OS	The OS of the host being attacked.
Victim Locality	Identifies whether the target address is located inside or outside of a given network, as specified by the intrusion detection device's configuration.
Summary Count	Specifies that this is a summary alert, representing one or more alerts with common characteristics. The numeric value indicates the number of times the signature fired since the last summary alert with a matching initialAlert attribute value.
Initial Alert	This field applies to a summary alert, representing one or more alerts with common characteristics. The value of InitialAlert provides the event ID of the last nonsummary evIdsAlert with the same characteristic (sigid/ subsigid).
Summary Type	Defines the common characteristics of all alerts in a summary alert.

Table 11-24 Eventing Notification Settings Page (continued)

Element	Description
Is Final	Applies to a summary alert, representing one or more alerts with common characteristics. It indicates whether this is the last event alert containing the same value in the initialAlert attribute.
Interface	Name of the IPS interface.
VLAN	The VLAN number associated with packets involved in the activity that triggered the alert.
Virtual Sensor	The name of the virtual sensor associated with the event.
Action Taken	The action performed on the flow. For example: Terminated or denied.
Alert Details	The details regarding the alerts.
Risk Rating	A value that represents the calculated risk associated with the event.
Threat Rating	The threat rating of the event, if any.
Reputation	The attacker's reputation score in the range -10.0 to +10.0. A lower (more negative) score indicates a greater likelihood that the host is malicious.
Reputation Details	Deny Attacker: Whether a deny-attacker action occurred (or would have occurred) because an internal override was exceeded due to the calculated risk rating: true or false.
Protocol	The Level-3 or Level-4 protocol.
Notification Settings (Critical Events only)	
Enable Email IDs	Whether to send email notification for critical events. If you select this option, also enter one or more email addresses (comma separated).
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

IPS Updates Page

Use the IPS Updates page to perform administrative tasks associated with keeping your sensors up to date with regard to signatures, minor version updates, and service packs. You can use the IPS Updates page to:

- Monitor update status.
- Check the availability of updates and download them.
- Configure an IPS update server.
- Configure automatic update settings.

Note Beginning with Security Manager version 4.9, only the latest sensor and signature packages for IPS will be available for download from CCO. The older packages will not be available for download from CCO.

Tips

- To apply IPS updates manually, select **Tools > Apply IPS Update**. For more information, see Manually Applying IPS Updates, page 44-7.
- If you later decide that you did not want to apply a signature update, you can revert to the previous update level by selecting the Signatures policy on the device, clicking the **View Update Level** button, and clicking **Revert**.

Beginning with version 4.4, Security Manager has a certificate trust management feature. This feature helps you with improved handling of Cisco.com certificates. For detailed documentation of this feature, refer to Certificate Trust Management, page 10-18.

Navigation Path

Select **Tools > Security Manager Administration** and select **IPS Updates** from the table of contents.

Related Topics

- Configuring the IPS Update Server, page 44-4
- Checking for IPS Updates and Downloading Them, page 44-5
- Automating IPS Updates, page 44-6
- Selecting a Signature Category for Cisco IOS IPS, page 45-6

Field Reference

Table 11-25 IPS Updates Page

Element	Description
Update Status group Refresh button	Displays the following items. Click **Refresh** to update the information. • Latest Available—The most recent signature and sensor update available on Cisco.com or the local HTTP server when you last checked for updates. • Latest Downloaded—The most recent signature and sensor update downloaded to Security Manager. • Latest Applied—The most recent signature and sensor update applied to any device in Security Manager. • Latest Deployed—The most recent signature and sensor update deployed to any device in Security Manager. • Last Check On—The time that the last check of Cisco.com was performed. • Last Download On—The time that the last update was downloaded to Security Manager. • Last Deployed On—The time that the last update was deployed to any of the devices.

Table 11-25 IPS Updates Page (continued)

Element	Description
Check for Updates button Download Latest Updates button	These buttons check for updates, or download signature and sensor updates that have not already been downloaded to the Security Manager server, from the IPS Update server. You must configure an IPS Update server before checking for updates or downloading them (click **Edit Settings** in the Update Server group). When you click one of these buttons, a dialog box opens to display the results of the operation. Security Manager logs into the IPS Update server, checks for updates, and downloads them if you clicked the Download button. If a Cisco.com download fails, ensure that the account you are using has applied for eligibility to download strong encryption software. For details, see the description of User Name in Edit Update Server Settings Dialog Box, page 11-52. **Tip** If you configure a server, and then try to check for updates, and you are told you did not configure a server, click **Save** at the bottom of the page and try again. **Note** Beginning with version 4.9, Security Manager mandates you to read and accept the End User License Agreement (EULA) before you can proceed to downloading updates from cisco.com.
Update Server group	Displays the settings used to access Cisco.com or the local server that contains the IPS update packages. The fields indicate whether the update server is Cisco.com or a locally-configured HTTP server, the name of the local server if you are using one, the user account for logging into the server, and the name of the proxy server, if any. To configure or change the IPS Update server, click **Edit Settings** to open the Edit Update Server Settings dialog box (see Edit Update Server Settings Dialog Box, page 11-52). For more information, see Configuring the IPS Update Server, page 44-4 Beginning with version 4.4, Security Manager has a certificate trust management feature. This feature helps you with improved handling of Cisco.com certificates. For detailed documentation of this feature, refer to Certificate Trust Management, page 10-18.
Signature Filter Settings group	Enables you to download IPS signature updates selectively. Click **Edit Settings** to open the Edit Signature Download Filter Settings dialog box (see Edit Signature Download Filter Settings Dialog Box, page 11-55).
Auto Update Settings group	Contains the settings specific to automatic updates. For more information, see Automating IPS Updates, page 44-6.

Table 11-25 IPS Updates Page (continued)

Element	Description
Auto Update Mode	Establishes whether, and to what extent, automatic updates are performed. Contains the following options: • Download, Apply, and Deploy Updates • Disable Auto Update • Check for Updates • Download Updates • Download and Apply Updates By default, auto update is disabled. The other options are a combination of one or more of the following options: • Check for Updates—Security Manager contacts the IPS Update server to check if an update is available and sends e-mail if e-mail notification is configured. No files are downloaded. • Download Updates—Security Manager downloads the latest updates from the IPS Update server, and sends e-mail notification if e-mail notification is configured. • Apply Updates—Security Manager modifies the configuration of the devices selected in the Apply Update To list based on the downloaded update packages. You have to separately deploy these updates unless you also select Deploy Updates. • Deploy Updates—Security Manager starts a deployment job to send the applicable update packages to the devices selected in the Apply Update To list. The device must have the required license for a signature update to be successful.
Update Schedule Edit Update Schedule button	The schedule for the actions selected in the Auto Update Mode field. To change the schedule, click **Edit Update Schedule** and define the schedule in the Edit IPS Updates Schedule dialog box. You can specify that Security Manager perform the updates based on hourly, daily, weekly, or monthly schedules, or specify a one-time event. When entering the start time, use the 24-hour clock and the *hh:mm* format. **Note** If you schedule an update to occur in less than 10 minutes from your Security Manager server time, the "Next Update" field will show tomorrow's date and the job will run accordingly. This is a safety feature designed to guarantee the first occurrence to run. **Tip** Cisco recommends scheduling automatic downloads during off hours so that they do not conflict with other user operations, such as device discovery. **Tip** Cisco recommends using an account other than the admin account for routine user operations.

Table 11-25 IPS Updates Page (continued)

Element	Description
Notify Email	The e-mail address to which notifications of automatic updates are sent. If you enter more than one address, separate the addresses with commas. A notification is sent when an update: • Is available for download. • Has been downloaded. • Has been downloaded and applied. • Has been downloaded, applied, and deployed.
Apply Update To Type Edit Row button Devices to be Auto Updated	The selector includes the IPS devices that have local signature policies and the shared signature policies that are defined in Security Manager. The columns in the selector indicate whether a local device policy or a shared policy is selected for these types of updates: • Signature—For auto updating the signature update level. • Minor—For minor updates and service packs. • S.P.—For service pack updates. For shared policies, a partial grey checked box indicates that some, but not all, of the devices that use the policy are selected. If you change the devices assigned to the shared policy between automatic update events, the shared policy is grayed out, and only the old assignments are shown on this page. After the update runs, the assignment list will be synchronized with the shared policy device assignments. To update the device list proactively prior to the next auto update run, select the policy and edit it (to select auto update settings), and the device assignment list will be corrected. **Note** Also for shared policies: You can select only the shared policy assigned to the default virtual sensor (vs0). If you attempt to select the shared policy for a different virtual sensor, your changes will not be applied, and you will not receive an error message. Use the Type field to toggle between viewing local and shared policies. Changing the view does not change your auto update selections. To select a local or shared policy for auto update, select it in the selector and click the **Edit Row** button below the selector. This opens the Edit Auto Update Settings dialog box, where you can select the types of updates for the policy. When you select any type of auto update for a policy, the affected devices are listed in the **Devices to be Auto Updated** list to the right of the selector.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Edit Update Server Settings Dialog Box

Use the Edit Update Server Settings dialog box to configure the server to use for obtaining IPS updates. If necessary, you can configure a proxy server for communicating with the update server.

Also, use the Edit Update Server Settings dialog box for certificate trust management. (Security Manager downloads IPS packages from Cisco.com over HTTPS, which uses certificates for establishing trust.) The certificate trust management feature on the Image Manager page is new in Security Manager 4.4. It will help you with improved handling of Cisco.com certificates for IPS package downloads:

- You can use it to view a certificate and use discretion in accepting it.
- After you accept a certificate, it is stored on your Security Manager server.
- You can see all your certificates in a summary table on the Image Manager page, and you can use that table to view or remove certificates.

Tip Please be sure to refer to "Retrieve Certificate" in the table below.

Navigation Path

Select **Tools > Security Manager Administration > IPS Updates** and click **Edit Settings** in the Update Server group.

Field Reference

Table 11-26 Edit Update Server Settings Dialog Box

Element	Description
Update From	Whether to get IPS updates from Cisco.com or from a local HTTP/HTTPS server. Your selection changes the fields on the dialog box. If you select local, you must configure an HTTP or HTTPS server to use as the IPS update server. **Caution** The default value for "Update From:" is "Local Server." You must choose "Cisco.com" to see certificate settings. Improper or incomplete certificate setting will prevent connectivity to Cisco.com, and all Cisco.com-related operations in this area will fail.
IP Address/ Host Name (Local server only.)	The hostname or IP address of the local IPS update web server.
Web Server Port (Local server only.)	The port number that your local server listens to for connection requests. The default is 80.

Table 11-26 Edit Update Server Settings Dialog Box (continued)

Element	Description
User Name	The username to log into the IPS update server. If you are configuring a local server that does not require a user login, leave this field blank. If you are specifying a Cisco.com username, the user account on Cisco.com must be eligible for downloading strong encryption software. If you are not certain that the account has the required permissions, use the account to log into Cisco.com and try to download an IPS update file (http://www.cisco.com/cgi-bin/tablebuild.pl/ips5-system). If the account does not have the appropriate permissions, you are prompted to read and accept the required conditions. If you meet the eligibility requirements, you can accept them. Otherwise, talk to your Cisco sales representative for help.
Password Confirm	The password for the specified username, entered in both fields. If you are configuring a local server that does not require a password, leave these fields blank.
Path to Update Files (Local server only.)	The path to the IPS update files location on your local server. For example, if update files can be accessed at http://local-server-ip:port/update_files_path/, then enter update_files_path in this field.
Connect Using HTTPS (Local server only.)	Whether to use SSL when connecting to the local IPS Update server.
Certificate Thumbprint	Displays the certificate thumbprint after it is calculated from the certificate on the local server.
Retrieve From Server	Used to connect to the local server specified in this dialog box, retrieve the certificate from the local server given, and calculate the certificate thumbprint, which is displayed in the Certificate Thumbprint field.
Contact URL	• When selected, "Image Meta-data Locator" is used. This is the URL on Cisco.com that is used to obtain meta-data information about images. Meta-data information consists of the images applicable to a particular product, name, size, checksum, and URL to download for each image. • When selected, "Other" is used. You can enter any valid HTTPS URL. This URL is intended primarily for the HTTPS URL to download the image as obtained from the meta-data information about the image. This URL may be different from the URL of the image meta-data locator described in the previous paragraph; the certificate may be different, as well. ⚠ **Caution** If you choose "Other," you need to explicitly add "https://dl.cisco.com" [without the quotation marks]: Enter it in the text field adjacent to the "Other" button. Failure to do this will prevent connectivity to Cisco.com, and all Cisco.com-related operations in this area will fail.

Table 11-26 Edit Update Server Settings Dialog Box (continued)

Element	Description
Retrieve Certificate	Used to connect to and retrieve the certificate from the selected '"Contact URL'." After retrieving the certificate it opens the Certificate Verification dialog, which along with a brief summary of the certificate, i.e., who the certificate is issued to, by whom, and the validity period of the certificate, gives you the following choices: • **View Certificate**—Opens the Certificate Viewer, where you can see all the details of the certificate: Certificate Authority, version, serial number, thumbprint, and other details. It shows the complete certificate chain information all the way up to the root issuing certificate Authority. • **Accept**—Accepts the certificate and adds it to the Cisco Security Manager. • **Reject**—Rejects the certificate and no action is taken. • **Cancel**—Closes the Certificate Verification dialog with no action taken.
Certificate	A table that displays, for each certificate in your Security Manager installation, Subject, Issued By, and Accepted By.
View	Opens the Certificate Viewer for a certificate selected in the Certificate table.
Remove	Removes a certificate selected in the Certificate table.
Proxy Server Group	
Enable Proxy Server	Whether a proxy server is needed to connect to Cisco.com or to your local server.
IP Address/ Host Name	The hostname or IP address of the proxy server. You can configure the proxy server to use basic, digest, NT LAN Manager (NTLM) V1, or NTLM V2 authentication. NTLM V2 is the most secure scheme.
Port	The port number that the proxy server listens to for connection requests. The default is 80.
User Name	The username to log into the proxy server. If the proxy server does not require a user login, leave this field blank.
Password Confirm	The password for the specified username, entered in both fields. If the proxy server does not require a password, leave these fields blank.

Edit Auto Update Settings Dialog Box

Use the Edit Auto Update Settings dialog box to configure the automatic update options for the device or policy selected in the Apply Update To table on the IPS Updates page. For information on configuring automatic updates, see Automating IPS Updates, page 44-6.

Navigation Path

Select a device or policy on in the Apply Update To table on the IPS Updates page (see IPS Updates Page, page 11-47) and click the Edit Row button.

Field Reference

Table 11-27 Edit Auto Update Settings Dialog Box

Element	Description
Auto Update (IPS sensors and shared policies only)	The type of sensor updates to apply to the selected devices or shared policies. You can apply both minor updates and service packs, service packs only, or select None to apply no sensor updates automatically.
Auto Update Signature Update Level	Whether to select the device or policy for automatic signature updates.

Edit Signature Download Filter Settings Dialog Box

The Edit Signature Download Filter Settings dialog box enables you to download IPS signature updates selectively. It applies both to the manual download and to the automated download.

Note Filtering does not apply to IPS sensor packages or to IPS engine packages; it applies to IPS signature packages only. All the available sensor packages on Cisco.com or on the local server will be downloaded as part of a signature download.

The benefits of selective download are reduced download time, reduced disk storage space, and faster troubleshooting because you can download only what you need.

There are four types of signature download available to you with the Edit Signature Download Filter Settings dialog box:

- No filter
- Download all signatures for engine versions starting with [choose E4, E3, E2, or E1]
- Download all signature versions starting with [enter a signature version such as 1000]
- Download a single signature version number [enter a signature number such as 1000]

The default signature configuration is to download all signatures for engine versions starting with E4.

Tip This default value is the same for a new installation of Security Manager 4.3 and for upgrades from previous versions.

Navigation Path

Select **Tools > Security Manager Administration** and then select **IPS Updates** from the table of contents; then click **Edit Settings** in the Signature Filter Settings group.

Related Topics

- Configuring the IPS Update Server, page 44-4
- Checking for IPS Updates and Downloading Them, page 44-5

- Automating IPS Updates, page 44-6

Field Reference

Table 11-28 Edit Signature Download Filter Settings Dialog Box

Element	Description
Filter Type: No filter	All available signatures for all available engines are downloaded.
Filter Type: Download all signatures for engine versions starting with	All available signatures for the engine that you select (E4, E3, E2, or E1) are downloaded.
Filter Type: Download all signature versions starting with	All available signatures starting with the ID that you enter are downloaded.
Filter Type: Download single signature version number	The single signature having the ID that you enter is downloaded.

ISE Settings Page

Use the ISE Settings page to configure communication between Cisco Security Manager and the Cisco Identity Services Engine (ISE) for use with TrustSec firewall policies.

Note Security Manager supports communications with only one ISE appliance/server for fetching and resolving security group names and tags.

To be PCI compliant, in Cisco Security Manager 4.15 and 4.16, TLS 1.0 and TLS 1.1 were disabled respectively. Hence from 4.16, Cisco Security Manager was using only TLS 1.2 version.

However, the ISE 1.3 server and its lower versions does not support TLS 1.2. This impacts the legacy ISE settings with Cisco Security Manager from release 4.15. This incompatibility prevents integration of ISE server with Cisco Security Manager.

If you are required to use ISE server (versions 1.3 and lower) in the Cisco Security Manager 4.15, 4.16, or 4.17 versions, to integrate ISE 1.3 and lower versions with Cisco Security Manager successfully, refer Resolving errors while integrating ISE server with Cisco Security Manager, page 11-57.

Navigation Path

Select **Tools > Security Manager Administration** and select **ISE Settings** from the table of contents.

Related Topics

- Chapter 14, “Managing TrustSec Firewall Policies”
- Creating Security Group Objects, page 14-14
- Selecting Security Groups in Policies, page 14-16

Field Reference

Table 11-29 Identity Settings Page

Element	Description
Enable ISE feature	Whether to enable communication with the ISE.
Username	The username Security Manager should use to log on to the ISE.
Password	The password for the username.
ISE Server (IP Address/Hostname)	The DNS hostname or IP address of the ISE.
Test Connectivity	Click Test Connectivity to ensure that Security Manager can communicate with the ISE given the settings you have entered.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Resolving errors while integrating ISE server with Cisco Security Manager

If you are using ISE server (versions 1.3 and lower) for resolving security group names and tags from Cisco Security Manager 4.15, 4.16, or 4.17, execute the following procedure to integrate ISE 1.3 and lower versions with Cisco Security Manager successfully:

Step 1 Navigate to the following registry location: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\ Procrun 2.0\Tomcat\Parameters\Java.

Step 2 In the Java file, locate the following content:

```
-Djdk.tls.client.protocols=TLSv1.2
```

Step 3 Replace this content with the following:

```
-Djdk.tls.client.protocols=TLSv1,TLSv1.1,TLSv1.2
```

Step 4 Save the Java file.

Step 5 Restart Cisco Security Manager.

Licensing Page

Use the Licensing page to manage licenses for the Security Manager application and for IPS devices. For more information, see Managing IPS Licenses, page 44-1.

Navigation Path

Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Field Reference

Table 11-30 Licensing Page

Element	Description
CSM tab	The license settings for the Security Manager application. For a description of the fields on this tab, see CSM Tab, Licensing Page, page 11-58.
IPS tab	The license settings for IPS devices managed by Security Manager. For a description of the fields on this tab, see IPS Tab, Licensing Page, page 11-58.

CSM Tab, Licensing Page

Use the CSM tab on the Licensing page to view the list of installed Security Manager licenses and to install new licenses. For more information, see Installing Security Manager License Files, page 10-16.

Navigation Path

Select **Tools > Security Manager Administration**, select **Licensing** from the table of contents, and click **CSM**.

Field Reference

Table 11-31 CSM Tab, Licensing Page

Element	Description
License Information	Displays information about the license registered with the product: the edition, license type, expiration date, the number of licensed devices, the number of devices in use, and the percentage of the device count used.
Install License	The list of installed licenses with their installation dates.
Install a License button	Click this button to install a license file. The dialog box that is opened includes links to Cisco.com, where you can obtain licenses if you have not already obtained them. You must copy license files to a local drive on the Security Manager server before you can install them.

IPS Tab, Licensing Page

Use the IPS tab on the Licensing page to view the list of installed IPS device licenses, to install new or updated licenses, or to redeploy licenses. The license list shows current licenses, unlicensed devices, devices with expired licenses, and devices with invalid licenses. You can also use the settings on this page to send a report of all those IPS devices whose license would expire within a specified number of days.

Navigation Path

Select **Tools > Security Manager Administration**, select **Licensing** from the table of contents, and click **IPS**.

Related Topics

- Updating IPS License Files, page 44-1
- Redeploying IPS License Files, page 44-2
- Automating IPS License File Updates, page 44-3
- License Update Status Details Dialog Box, page 11-62
- Filtering Tables, page 1-48
- Table Columns and Column Heading Features, page 1-49

Field Reference

Table 11-32 IPS Tab, Licensing Page

Element	Description
IPS License Table	Displays all the IPS devices in the device inventory and their license status as of the last time you refreshed the information. Click the **Refresh** button to obtain the latest information from the devices. Information includes the serial number for the device, which is used to register for licenses, the license status, and the expiration date of the license. The list shows not only current licenses, but also unlicensed devices, devices with expired licenses, and devices with invalid licenses. **Tip** The list does not include Cisco IOS IPS devices. You cannot use Security Manager to manage licenses for routers running IPS.
Update Selected via CCO button	Click this button to update the license file for the selected devices by connecting to Cisco.com and retrieving a new license. When you click this button, a dialog box opens listing devices that can be updated from Cisco.com, which might not be all the devices you selected. Click **OK** to perform the update. For successful updates, the updated file is automatically applied to the device. To successfully update the license using this method, you must have a Cisco.com support contract that includes the serial numbers of the selected devices. **Tip** The Cisco software license server (SWIFT) that contains the licenses might block requests from the same server for more than 9 licenses within a three minute period. Thus, you should select fewer than 9 devices at a time when performing manual license updates.
Redeploy Selected Licenses button	Click this button to redeploy licenses to the selected devices. Redeploying licenses might be necessary when you have obtained an updated license file and it was not applied to the device successfully during an automatic update. When you click this button, a dialog box opens listing devices whose licenses you are redeploying. Click **OK** to perform the update. For successful updates, the updated file is automatically applied to the device.

Table 11-32 IPS Tab, Licensing Page (continued)

Element	Description
Update from License File button	Click this button to update licenses by selecting a license file from the Security Manager server. When you click this button, a dialog box opens where you can specify the license files. Click **Browse** to select the files, which must be on a local drive on the Security Manager server. When you click **OK**, the updated files are automatically applied to the devices.
Export As button	Select one or more IPS devices from the list and then click the **Export As** button to export their licenses to a Portable Document Format (PDF) or comma-separated values (CSV) file. You are prompted to select the folder on the Security Manager server and to specify a file name. If you do not select any device from the list, the licenses of all available devices are exported.
Refresh License button	Click this button to refresh the data in the IPS license table for the selected devices. The updated information is retrieved from the device. If you do not select any devices, all devices are refreshed; this can take a long time depending on the number of devices listed.
Download and apply licenses Days before the expiration date.	Whether to automatically download IPS licenses from Cisco.com and apply them to the devices. To successfully configure automatic updates, you must have a Cisco.com support contract that includes the serial numbers of your IPS devices. If you select this option, also specify the number of days before the license expiration date for downloading and applying licenses. Security Manager evaluates only those devices that do not have licenses, have expired licenses, or have valid licenses within this number of days of expiration. Licenses are applied only if they are valid and either have an expiration date farther out than the current one, or that have different license information.
Discover devices daily at	If you select automatic license updates, the time of day when Security Manager should contact devices for current licenses status and evaluate whether there are devices that have licenses that will expire within the specified number of days. Cisco.com is contacted only if one or more device meets the expiration requirements.
Email License Update Results Email Notification	Whether to send email notifications of expiration alerts and license update job results. If you select this option, also enter one or more email addresses (comma separated).
Email License Expiration Status Email Notification	Whether to send a PDF report of those IPS devices whose license would expire within a specified number of days. If you select this option: • Enter the number of days (not more than 100) before the device license expiry date, by which you want Security Manager to send the PDF report. • Select the time and day for Security Manager to check the license expiry. • Enter one or more email addresses (comma separated) to which you want the License Expiration Status PDF report to be sent.

Table 11-32 IPS Tab, Licensing Page (continued)

Element	Description
Save button	Saves your changes to the automatic license update and e-mail notification settings.

Verifying IPS Devices for License Update or Redeployment

When you select a device on the **Licensing > IPS** tab (see IPS Tab, Licensing Page, page 11-58) and try to update the license from Cisco.com (CCO) or redeploy the license, you are first shown a list of devices that will be updated. The name of the dialog box is based on the action you are taking:

- **Updating Licenses via CCO dialog box**—Review the IPS devices you selected to update from Cisco.com. The device list displays the IPS devices for which you can update the license from Cisco.com, which might not be all of the devices you selected.

  To successfully update the license using this method, you must have a Cisco.com support contract that includes the serial numbers of the selected devices.

Tip The Cisco software license server (SWIFT) that contains the licenses might block requests from the same server for more than 9 licenses within a three minute period. Thus, you should select fewer than 9 devices at a time when performing manual license updates.

- **Redeploying Licenses dialog box**—Review the IPS devices you selected for redeploying licenses. Before you can redeploy a license to a device, you must have already deployed the license. Security Manager uses the file already associated with the IPS device to redeploy the license.

When you click **OK**, the License Update Status Details dialog box opens so that you can view the status of the license redeployment task. See License Update Status Details Dialog Box, page 11-62.

Navigation Path

To open these dialog boxes, select one or more device on the **Tools > Security Manager Administration > Licensing > IPS** tab and click **Update Selected via CCO** or **Redeploy Selected Licenses**.

Selecting IPS License Files

If you select one or more devices on the **Tools > Security Manager Administration > Licensing > IPS** tab and click **Update from License File**, you are prompted to select the license file you want to use with the Updating Licenses from File dialog box.

You can store the license file on a local drive on the Security Manager server, and, beginning with Version 4.5 of Security Manager, you can store it on a local drive on a client.

Click **Browse** to select the license file. You can select multiple license files using Ctrl+click or a range of files using Shift+click.

Note If you installed the Security Manager client on a different machine than the one on which Security Manager server is installed, you can choose to select the license file from either the client machine or the server machine. If both the client and the server are installed on the same machine, Security Manager allows you to select the license file only from the server.

When you have selected the license files you want to use, click **OK** to apply them to the IPS devices.

Note If you want to store the license file on a client machine, you must select "Enable Client side file browser" on the Customize Desktop page at Tools > Security Manager Administration > Customize Desktop.

License Update Status Details Dialog Box

Use the License Update Status Details dialog box to view the status of an IPS license update task. This dialog box opens whenever you start an update task from the IPS tab of the Licensing page. For more information, see IPS Tab, Licensing Page, page 11-58.

Field Reference

Table 11-33 License Update Status Details Dialog Box

Element	Description
Progress bar	Indicates what percentage of the license update task on the current device has been completed.
Status	The current state of the update task.
Devices to be updated	The total number of devices being updated during this task.
Devices updated successfully	The number of devices updated without errors.
Devices updated with errors	The number of devices that generated errors during the update.
Device list	The devices that are being updated, including the device name, the status of the update, and summary information about the update. Select a device to see the messages generated during the update for that device in the message list below the summary list.
Messages list	The messages generated during the license update for the selected device. Select a message to see detailed information in the fields to the right of the list.
Description	Additional information about the message selected in the message list.
Action	The steps you should take to resolve the described problem.
Abort button	Aborts the license update task.

Logs Page

Use the Logs page to configure the default settings for the audit and operations logs. The audit log keeps a record of all state changes that occur in Security Manager.

Navigation Path

Select **Tools > Security Manager Administration** and select **Logs** from the table of contents.

Related Topics

- Using the Audit Report Window, page 10-21
- Understanding Audit Reports, page 10-19

- Generating the Audit Report, page 10-20
- Purging Audit Log Entries, page 10-23

Field Reference

Table 11-34 Logs Page

Element	Description
Keep Audit Log For	The maximum number of days to save audit report entries before deleting them. If the number of entries in the log exceeds the number entered in the Purge Audit Log After field, old log entries might be deleted before they reach this age.
Purge Now button	If you reduce the number of days, you can click **Purge Now** to immediately delete the older entries. **Note** The Purge Now button only removes audit report entries from the database. It does not remove the *.csv files from the ***<*install_dir*>**\CSCOpx\MDC\log\audit folder. These *.csv files can be deleted directly.
Purge Audit Log After (entries)	The maximum number of audit report entries to save. If an entry becomes older than the number of days specified in the Keep Audit Log For field, it is deleted even if the log has fewer than the maximum number of entries.
Keep Operation Log For	The number of days that Security Manager keeps operation logs before deleting them. These logs are used for debugging purposes.
Log Level	The level of information, according to severity, that you would like collected in the operation logs. Each level collects different amounts of data. For example, the Info level yields the most data, and the Severe level collects the least.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Policy Management Page

Use the Policy Management page to select the types of router and firewall policies you will manage in Security Manager. These selections apply to routers and firewall devices, but do not apply to IPS devices. By default, all policies are selected for management.

Unmanaged policies are removed from both Device view and Policy view. Any unmanaged policies, local or shared, are removed from the Security Manager database. The only exception is interface policies, which continue to appear in Security Manager but are marked as read-only policies. For firewall devices, interface and failover settings are considered a unit and are managed or unmanaged together.

For detailed information on managing and unmanaging policy types, including what you should do before and after changing these settings, see Customizing Policy Management for Routers and Firewall Devices, page 5-11.

Caution If you use AUS or CNS to deploy configurations to ASA or PIX devices, be aware that the device downloads a full configuration from AUS or CNS. Thus, reducing the policies managed by Security Manager actually removes the configurations from the device. If you intend to deselect some ASA/PIX policies for management to use other applications along with Security Manager to configure devices, do not use AUS or CNS.

Navigation Path

Select **Tools > Security Manager Administration** and select **Policy Management** from the table of contents.

Field Reference

Table 11-35 Policy Management Page

Element	Description
Policies to Manage	The policy types are organized in folders, with router and firewall (which includes all ASA, PIX, and FWSM devices) handled separately, and then by category (NAT, Interfaces, and Platform). Select or deselect policy types as desired and click **Save**. Deselecting the check box for a group of policies deselects all policies in that group. By default, all policies are selected.
Display a warning on all shared policies and imported objects	Whether to add a message to all shared policies and to objects that were imported using the **File > Import** command. If you select this option, messages appear on the following: • All shared policies, whether they were imported or locally created. • Policy objects that were created by importing devices or shared policies using the **File > Import** command, but not imported policy objects created by the PolicyObjectImportExport.pl command (described in Importing and Exporting Policy Objects, page 6-23. If you regularly import shared policies, the imported policies and objects replace any same-named policies and objects, so any changes made locally are removed. This message can notify users that policies might be imported and help users identify policy objects that they might not want to edit. **Tip** When importing policies or devices, you are prompted to select a setting for this option. Thus, users who import policies or devices can change this setting without accessing this page provided they have the required authorization. The change is effective only after the importer submits (and if necessary, approves) the changes. For more information, see Importing Policies or Devices, page 10-13.

Table 11-35 Policy Management Page (continued)

Element	Description
Save button	Saves your changes. If you are unmanaging a policy, you are shown a list of devices that have the policy assigned to them. Security Manager must be able to obtain the required locks to unassign the policy from all devices, or you must manually unassign the policies (or remove the locks) before unmanaging the policy. If you are managing a previously unmanaged policy, be sure to rediscover all affected devices to bring the existing configurations into Security Manager.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Policy Objects Page

Use the Policy Objects page to define system defaults related to policy object creation.

Navigation Path

Select **Tools > Security Manager Administration** and select **Policy Objects** from the table of contents.

Related Topics

- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Chapter 6, "Managing Policy Objects"

Field Reference

Table 11-36 Policy Objects Page

Element	Description
When Redundant Objects Detected	The action you want Security Manager to take when you try to create a policy object that has the same definition as an existing object: • Ignore—You can freely create objects with identical definitions. Any conflicts are ignored by Security Manager. • Warn—Security Manager displays a warning if you attempt to create an object that is identical to an existing object. You may proceed to create the object, if you wish. • Enforce—Security Manager prevents you from creating an object that is identical to an existing object. An error message is displayed.

Table 11-36 Policy Objects Page (continued)

Element	Description
Default Source Ports	The port range value that is used as the default source port range for service objects. You can choose one of the following: • Use all ports—Includes all ports from 1 to 65535. • Use secure ports—Includes all ports from 1024 to 65535. If you change the default source ports, you must manually redeploy any previously deployed devices that might be affected. These changes might not be reflected in any open activities until you refresh the data. For more information on port list objects, see Configuring Port List Objects, page 6-101.
Enable AutoComplete Dropdown Box	Whether to have Security Manager list matching service and port list names as you type them when you create a service. You can then easily select from names you have already defined. If you deselect AutoComplete, you have to remember the complete service and port list names and type them in yourself.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Process Monitoring Settings Page

Use the Process Monitoring Settings page to enable process monitoring. Here, you can enable or disable monitoring for specific processes and configure notification settings such as monitoring interval and email addresses. This will send an email notification to specified recipients, when a process stops.

Before You Begin

Configure SMTP Server and sender mail in the CS web console, to get email alerts.

Navigation Path

Select **Tools > Security Manager Administration** and select **Process Monitoring Settings** from the table of contents.

Field Reference

Table 11-37 Process Monitoring Settings Page

Element	Description
Enable Process Monitoring	When selected, Security Manager will allow you to specify the processes that you want to monitor. You must proceed to configure other process monitoring settings. By default, the Process Monitoring feature is disabled on the Cisco Security Manager Server. **Note** Enabling or disabling the process monitor modifies the Windows registry and may generate a system alert.

Table 11-37 Process Monitoring Settings Page (continued)

Element	Description
Monitoring Interval (in minutes)	Specify the interval, at which, the process will be monitored. Valid values are between 1-60 minutes. The default monitoring interval is 5 minutes. **Note** If the monitoring interval is changed, the monitoring task in progress stops and the new monitoring task starts with the updated interval.
Notification Recipient(s) E-mail(s)	Enter email IDs for the notification recipients.You can enter multiple email IDs, separated by a comma. These are the recipients that will be notified, when a process being monitored, stops.
Maximum Mail Alerts	Enter the maximum number of emails that will be sent to the recipients during the course of Security Manager runtime. The default value here, is 10.
Process List	Select one or more processes that you want to monitor. Whenever any of these selected processes stop, a notification email will be sent to the specified recipients. **Note** When Event Management, Health and Performance Monitor and Report Manager are disabled from **Tools > Security Manager Administration,** email notifications will not be sent, even if, the VmsEventServer, CsmHPMServer and CsmReportServer processes are enabled in the process monitoring settings page.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Single Sign-on Configuration Page

Use the Single Sign-on Configuration page of the Security Manager Administration window to enable and configure a “single sign-on” (SSO) shared key to use for cross-launching Cisco Prime Security Manager or FireSIGHT Management Center.

Note Single sign-on allows users to cross-launch Prime Security Manager or FireSIGHT Management Center from Security Manager without logging into Prime Security Manager or FireSIGHT Management Center separately. However, SSO is not required to cross-launch Prime Security Manager or FireSIGHT Management Center.

Tip Cisco Prime Security Manager is used to manage ASA CX modules. FireSIGHT Management Center is used to manager ASA FirePOWER modules.

Related Topics

- Detecting ASA CX and FirePOWER Modules, page 72-21

- Launching Cisco Prime Security Manager or FireSIGHT Management Center, page 72-20
- Sharing Device Inventory and Policy Objects with PRSM, page 72-22

Navigation Path

1. Click **Tools > Security Manager Administration** and select **Single Sign-on Configuration** from the table of contents.
2. Select **Enable for Prime Security Manager** [checkbox] or **Enable for FireSIGHT Management Center** [checkbox].

Field Reference

Table 11-38 Single Sign-on Configuration Page

Element	Description
Enable for Prime Security Manager	[checkbox] Lets you enable or disable the SSO feature for Prime Security Manager. When disabled, the shared key is retained.
Enable for FireSIGHT Management Center	[checkbox] Lets you enable or disable the SSO feature for FireSIGHT Management Center. When disabled, the shared key is retained.
Shared Key for Single Sign-on	Use the features in this section to generate and view an encryption key for cross-launching Prime Security Manager or FireSIGHT Management Center. Click the **Generate** button to randomly generate a 128-bit AES key, which is then displayed as a 32 hexadecimal string in the SSO Shared Key field. **Note** This key must be provided when configuring single sign-on cross-launching in Prime Security Manager or FireSIGHT Management Center. Also, each allowed Security Manager user must be configured in the Prime Security Manager database or the FireSIGHT Management Center user database with the same username as that in the Security Manager user database (the password can be different). **Tip** Refer to "Configuring Single Sign-On for Cisco Security Manager" in the *User Guide for ASA CX and Cisco Prime Security Manager* (Cisco ASA CX Context-Aware Security End-User Guides) for information about configuring SSO in PRSM.

Rule Expiration Page

Use the Rule Expiration page to define the default values for policy rule expiration. When you create policies for some types of policy rules (such as access rules), you can set an expiration date for the rule, and Security Manager can notify you by e-mail of the approaching expiration date.

You must configure an SMTP server to enable e-mail notifications. For more information, see Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-26.

Navigation Path

Select **Tools > Security Manager Administration** and select **Rule Expiration** from the table of contents.

Field Reference

Table 11-39 Rule Expiration Page

Element	Description
Notify Email	The default e-mail address that should receive notifications of rule expiration. Users can override this address when configuring individual rules.
Notify Before Expiration	The default number of days before a rule expires that Security Manager should send the e-mail message. Users can override this value when configuring individual rules.
Sender	The e-mail address that Security Manager will use for sending e-mail notifications.
Email Format	The format of the e-mail message: • Text—The e-mail is sent in HTML and plain text formats. • XML—The e-mail is sent using an XML markup. This option might be appropriate if you decide to write a program to automatically process and respond to notifications.
Save button	Saves your changes.
Reset button	Restores all fields to their previous values.
Restore Defaults button	Resets values to Security Manager defaults.

Server Security Page

Use the Server Security page to open specific pages in the CiscoWorks Common Services application, where you can configure various security features on the Security Manager server. CiscoWorks Common Services controls the basic functions of the Security Manager server, including user access control and system security.

When you log in to Security Manager, your username and password are compared with the account information stored in the CiscoWorks or Cisco Secure Access Control Server (ACS) database, depending on which system you established at installation as your AAA provider. After the authentication of your credentials, you have access according to the role you have been assigned.

For more information on Security Manager roles and privileges, including descriptions of how Common Services roles translate to user functions in Security Manager, see the *Installation Guide for Cisco Security Manager*.

Navigation Path

Select **Tools > Security Manager Administration** and select **Server Security** from the table of contents.

Field Reference

Table 11-40 Server Security Page

Element	Description
AAA Setup button	Opens Common Services and displays the AAA Mode Setup page. From this page, you can set AAA as your fallback sign-on method. For more information about AAA, click **Help** from the AAA Mode Setup page.
Certificate Setup button	Opens Common Services and displays the Self-Signed Certificate Setup page. CiscoWorks enables you to create self-signed security certificates, which you can use to enable SSL connections between your client browser and management server. For more information about self-signed certificates, click **Help** from the Certificate Setup page.
Single Sign On button	Opens Common Services and displays the Single Sign-On Setup page. With Single Sign On (SSO), you can use your browser session to transparently navigate to multiple CiscoWorks servers without having to authenticate to each of them. Communication between multiple CiscoWorks servers is enabled by a trust mode addressed by certificates and shared secrets. For more information about setting up SSO, click **Help** from the Single Sign-On page.
Local User Setup	Opens Common Services and displays the Local User Setup page, from which you can add and delete users, edit user settings, and assign roles or permissions. For more information, click **Help** from the Local User Setup page and see the *Installation Guide for Cisco Security Manager*.
System Identity Setup	Opens Common Services and displays the System Identity Setup page. Communication between multiple CiscoWorks servers is enabled by a trust mode addressed by certificates and shared secrets. System Identity setup helps you to create a trust user on servers that are part of a multi-server setup. For more information about system identity setup, click **Help** from the System Identity Setup page.
Native RBAC Parameters	
Allow logon for user ids not available in Local User Database	For Security Manager installations integrated with an external authentication server like Active Directory, TACACS+, or RADIUS, specifies whether users can log in even when their user name is not defined in the Security Manager user list. When enabled, users are allowed to log in using the default role specified in Role Management Setup. If a default role is not configured, the user is not allowed to log in.

Take Over User Session Page

Use the Take Over User Session page to take over another user's configuration session. A user with administrative privileges can take over the work of another user in non-Workflow mode. Taking over a session is useful when a user is working on devices and policies, causing the devices and policies to be locked, and another user needs access to the same devices and policies. However, when you take over another user's session, your current session is discarded, so make sure that you submit your changes before taking over a session.

The table shows all current configuration sessions, listing the user name and the state of the session, whether the user is currently logged in or logged out. Select the configuration session you want to take over and click **Take over session**. The session is transferred to you in its current state, including any saved changes the user made during the session.

If the selected user is logged in at the time you take over the session, the user receives a warning message, loses any unsaved changes in progress, and then is logged out.

For more information, see Taking Over Another User's Work, page 10-23.

Navigation Path

Select **Tools > Security Manager Administration** and select **Take Over User Session** from the table of contents.

Ticket Management Page

Use the Ticket Management page to enable Ticket Management, to configure a ticketing system URL for integration with an external change management system, and to configure purge settings for ticket information.

When Ticket Management is enabled, every Image Management installation job must have an assigned ticket or it will not be performed.

Navigation Path

Select **Tools > Security Manager Administration** and select **Ticket Management** from the table of contents.

Related Topics

- Changing Workflow Modes, page 1-27
- Comparing Workflow Modes, page 1-22

Field Reference

Table 11-41 Ticket Management Page

Element	Description
Enable Ticketing	Whether to enable Ticket Management.
System Generated Default Ticket Name	By default, this check box is checked. Clear the check box, if you do not want the ticket name to be appended with the system generated default name. The ticket name field in the activity creation dialog is left blank.

Table 11-41 Ticket Management Page (continued)

Element	Description
Ticketing System URL	
Ticketing System URL	The URL to use for launching an external change management system. When this field is configured, the Ticket ID is a hyperlink that will launch the URL specified. The URL must be formatted as a template that accepts the Ticket ID as part of the URL. The template format uses {0} in place of the actual Ticket ID. For example, if the URL to launch an external ticket management system for a ticket with the ticket ID of *TKT12345* is http://ticketsystem/displayticket?ticketid=TKT12345, then the template URL you would use would be **http://ticketsystem/displayticket?ticketid={0}**. When you create a ticket, the Ticket ID you specify will be used in the hyperlink in place of the {0}.
Generate	Click to display the Generate Template URL dialog box that can be used to create a Ticketing System URL. Using the example above, you would enter **TKT12345** in the Ticket ID field and **http://ticketsystem/displayticket?ticketid=TKT12345** in the Ticket URL field. When you click **OK**, the appropriate template URL is created and entered into the Ticketing System URL field.
Ticket History Ticket History settings are only available in non-Workflow mode. In Workflow mode, purge settings are controlled via the settings for Activities (see Workflow Page, page 11-75).	
Purge Tickets (including change report) Older than	The number of days that ticket information should be kept in the Ticket Manager table. The default is 30. You can specify from 1 to 120 days. Click **Purge Now** to delete all tickets older than the number of days specified.
Purge Change Report older than	The number of days that change reports should be maintained. The default is 30. You can specify a value that is less than the Purge Tickets (including change report) Older than setting. Click **Purge Now** to delete all change reports older than the number of days specified.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Token Management Page

Use the Token Management page to identify the Token Management System (TMS) server to use for deploying configurations to Cisco IOS routers that use TMS as the communication protocol. Security Manager uses the settings on this page to contact the TMS server.

Security Manager uses FTP to deploy the delta configuration file to the TMS server, from which the configuration file can be downloaded and encrypted onto an eToken.

To use TMS with Cisco IOS routers, you must specify TMS as the transport protocol. You can do this for all routers on the Device Communication page (see Device Communication Page, page 11-21), or for a specific router in its device properties (see Device Properties: General Page, page 3-41). You must also configure the TMS server as an FTP server, otherwise deployment will fail.

Navigation Path

Select **Tools > Security Manager Administration** and select **Token Management** from the table of contents.

Related Topics

- Deploying Configurations to a Token Management Server, page 8-43
- Understanding Deployment Methods, page 8-8

Field Reference

Table 11-42 Token Management Page

Element	Description
Server Name or IP Address	The DNS hostname or IP address of the TMS server.
Username	The username Security Manager should use to log on to the TMS server.
Password Confirm Password	The password for the username. Enter the password in both fields.
Directory in the TMS Server for Config Files	The directory on the TMS server where deployed configuration files will be downloaded. The root FTP directory (".") is the default FTP location on the TMS server.
Public Key File Location	The location of the public and private key files on the Security Manager server, as copied from the TMS server. Security Manager uses the public key to encrypt data sent to the TMS server. Then the server uses its private key to decrypt the data. Security Manager comes with a default public key that matches the default private key on the server. **Note** If needed, you can generate a new pair of public and private keys using the TMS server. If you do this, you need to copy the new public key to the Security Manager server.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

VPN Policy Defaults Page

Use the VPN Policy Defaults page to view or assign the default VPN policies that Security Manager uses for each IPsec technology. Before you can select a policy as a default, you must create the policy as a shared policy, submit it to the database and have it approved. You cannot create policies from this page. For detailed information on how to configure these defaults, see Understanding and Configuring VPN Default Policies, page 25-12.

For each tab that relates to a VPN topology, the drop-down lists for each policy type list the existing shared policies that you can select. You can select a policy and click the **View Content** button to see the definition of that policy. In some cases, you are allowed to make changes, but you cannot save them.

Security Manager uses VPN policy defaults to simplify VPN configuration while ensuring that policy consistency is maintained. Security Manager provides factory default policies for mandatory policies, which provide values for settings that must be configured on the devices in your VPN topology for the VPN to work. Mandatory policies differ depending on the assigned IPsec technology. Factory default policies with their default configurations enable you to deploy to your devices immediately after creating the VPN topology. Default settings are not provided for optional policies. You might want to create shared policies to provide different default settings instead of using the factory default settings.

Navigation Path

Select **Tools > Security Manager Administration** and select **VPN Policy Defaults** from the table of contents.

Related Topics

- Assigning Initial Policies (Defaults) to a New VPN Topology, page 25-61
- Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (ASA and PIX 7.0+ Devices), page 30-25
- Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (IOS and PIX 6.3 Devices), page 30-36

Field Reference

Table 11-43 VPN Policy Defaults Page

Element	Description
DMVPN tab	Lists the policy types for which you can configure default policies for the Dynamic Multipoint VPN technology.
Large Scale DMVPN tab	Lists the policy types for which you can configure default policies for the Large Scale Dynamic Multipoint VPN technology.
Easy VPN tab	Lists the policy types for which you can configure default policies for the Easy VPN technology.
IPsec/GRE tab	Lists the policy types for which you can configure default policies for the IPsec/GRE VPN technology.
GRE Dynamic IP tab	Lists the policy types for which you can configure default policies for the GRE Dynamic IP VPN technology.
Regular IPsec tab	Lists the policy types for which you can configure default policies for regular IPsec VPN technology.
Regular IPsec VTI tab	Lists the policy types for which you can configure default policies for regular, tunnel-based IPSEC VPN technology.
GET VPN	Lists the policy types for which you can configure default policies for the Group Encrypted Transport (GET) VPN technology.
Remote Access VPN	Lists the policy types for which you can configure default policies for IPsec remote access VPNs.
S2S Endpoints tab	The interface roles that define the default endpoints for internal and external interfaces in site-to-site VPNs.

Workflow Page

Use the Workflow page to select the workflow mode that Security Manager enforces and to define the default settings for activity and deployment job notifications and logging.

Before changing the workflow mode, read the following topics to understand how the modes differ and the effects of changing the modes:

- Working in Workflow Mode, page 1-21
- Working in Non-Workflow Mode, page 1-22
- Comparing Workflow Modes, page 1-22
- Changing Workflow Modes, page 1-27

Navigation Path

Click **Tools > Security Manager Administration** and select **Workflow** from the table of contents.

Related Topics

- Chapter 4, "Managing Activities"
- Chapter 8, "Managing Deployment"

Field Reference

Table 11-44 Workflow Page

Element	Description
Workflow Control	
Enable Workflow	Whether to enable Workflow mode. When Workflow mode is enabled, you can select whether or not to have an approver for activities and deployment jobs.
Require Activity Approval	Whether to require that activities be approved explicitly by an assigned approver. For more information about the differences between working with and without an approver, see Activity Approval, page 4-3.
Submitter can Approve Activity	Activities can be approved by submitter.
Require Deployment & Install Image Approval	Whether to require that deployment jobs and install image jobs be approved explicitly by an assigned approver. For more information about the differences between working with and without an approver, see Understanding Deployment, page 8-1.
Submitter can Approve Deployment Jobs	Deployment jobs can be approved by submitter.
System Generated Default Activity Name	By default, this check box is checked. Clear the check box, if you do not want the activity name to be appended with the system generated default name. The activity name field in the activity creation dialog is left blank.
Email Notifications	
Sender	The e-mail address that Security Manager will use for sending e-mail notifications.

Table 11-44 Workflow Page (continued)

Element	Description
Activity Approver	The default e-mail address for the person responsible for approving activities. Users can override this address when submitting an activity for approval. For more information, see Submitting an Activity for Approval (Workflow Mode with Activity Approver), page 4-20.
Job/Schedule Approver	The default e-mail address of the person responsible for approving deployment jobs or schedules. Users can override this address when submitting a job or schedule for approval. For more information, see Submitting Deployment Jobs, page 8-38.
Require Deployment Status Notification Include Job Deployer Job Completion Notification	Whether to have e-mail notifications sent whenever the status of a deployment job changes. If you select this option, enter the e-mail addresses that should receive notification in the Job Completion Notification field. Separate multiple addresses with commas. You can also select Include Job Deployer to include the e-mail address of the person who deployed the job on the notification e-mail message.
Workflow History	
Keep Activity for	The number of days that activity information should be kept in the Activity table. The default is 30. You can specify from 1 to 180 days. Click **Purge Now** to delete all activities older than the number of days specified. **Note** If ticketing is enabled in non-Workflow mode, purge settings are controlled via the settings for Tickets (see Ticket Management Page, page 11-71).
Keep Job for	The number of days that deployment job information should be kept in the Deployment Job table. The default is 30. You can specify from 1 to 180 days. Click **Purge Now** to delete all jobs older than the number of days specified.
Keep job per schedule for	The number of days that deployment job information should be kept in the Deployment Job table for each job schedule. This setting applies only to jobs that were initiated by a schedule. The default is 30. You can specify from 1 to 180 days. Click **Purge Now** to delete all jobs older than the number of days specified.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Wall Settings Page

The Security Manager Wall Settings page is where you can enable or disable the Wall feature.

The "Wall" feature is also called the "ShoutBox" feature. You can use it to send messages to all users who are logged in on the same Security Manager server. First, however, it must be enabled on the Wall Settings page.

Note Only admin users have permission to enable or disable the Wall feature, but all users have permission to send messages.

You would want to use the Wall feature, for example, to interact with other users while making some changes in your Security Manager installation, perhaps about the changes being made or certain immediate actions to be performed on the changes. The message being sent is broadcast to all users who are logged in. The Wall feature allows users to enter basic profile information that can be viewed by others when logged in. A significant use of the Wall feature is that it can be used to view a list of all users who are currently logged in. (A user is removed from the Wall window after idle timeout or logging out through the Security Manager client.)

You cannot use the Wall feature to send *.pdf, *.xls, or other file attachments.

Navigation Path

Click **Tools > Security Manager Administration** and select **Wall Settings** from the table of contents.

Field Reference

Table 11-45 Wall Settings Page

Element	Description
Enable users to send messages to others	Whether to enable or disable the Wall feature.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

When the Wall feature is enabled, you can open the Wall window by clicking **Tools > Wall...** or by clicking the Wall icon in Configuration Manager.

You can also open the Wall window by clicking the Wall icon in Health and Performance Monitor or Image Manager. You cannot open the Wall window in Event Viewer or Report Manager.

Detailed Wall feature help is available on the Wall window by clicking the help icon.

The Wall window contains the following elements:

- Left-hand pane, which shows the users who are logged in on the same Security Manager server and an expand/collapse button.
- Right-hand pane, which occupies most of the page and contains the text of the messages that users have sent. The right-hand pane also has a button to enable or disable wall alerts and the help icon, which you can click to see detailed help.

Summary of the Wall Window

Message Display	Messages are displayed in the right-hand pane of the Wall window. The latest messages are always displayed at the top. Selective copy of text is allowed from the messages. You are allowed to type a maximum of 280 characters in the message panel, and after completing this number of characters you are alerted by a beep sound.
Message Log	You can see a log of previous messages. The message log keeps 100 messages. The messages become visible to you when you launch the Wall window.
Profile Picture	You can upload a picture for your profile. Valid image types such as JPG, PNG, BMP, and GIF types are supported. To upload a picture, use the **upload** link in the user profile window. To open the user profile window, click on the username or user picture in the Wall window. The user profile window also has an icon that toggles between Edit profile information and Save profile information.
User Profile Window	To open the user profile window, click on the username or user picture in the Wall window. The user profile window contains the following information: • Profile Name (maximum 20 characters) • Designation (maximum 15 characters) • Email (maximum 15 characters) • Phone Click the corresponding email link to send the mail.
Notification Alert	On receipt of a new message and when the Wall window is not focused, a new notification alert popup is shown to you. You can simply click on the notification to launch the Wall window. When the notification alert popup is shown to you, the Wall window icon also flashes with the message count displayed. You can turn off the notifications alert from the settings options provided on the alert popup or in the Wall window.

Figure 11-1 Wall Window