



APPENDIX **A**

Administrative Settings User Interface Reference



Tip

For helpful information on the most important settings to define first, read [Define These Settings First](#), page 2-2.

The following topics describe Security Manager settings administration:

- [AutoLink Settings Page](#), page A-2
- [Configuration Archive Settings Page](#), page A-3
- [Customize Desktop Page](#), page A-4
- [Deployment Page](#), page A-5
- [Device Communication Page](#), page A-10
- [Device Groups Page](#), page A-15
- [Device OS Management Page](#), page A-16
- [Discovery Page](#), page A-17
- [IPS Updates Page](#), page A-19
- [Licensing Page](#), page A-26
- [Logs Page](#), page A-30
- [Policy Management Page](#), page A-32
- [Policy Objects Page](#), page A-33
- [Server Security Page](#), page A-35

- [Status Page, page A-36](#)
- [Take Over User Session Page, page A-41](#)
- [Token Management Page, page A-42](#)
- [VPN Policy Defaults Page, page A-44](#)
- [Workflow Page, page A-48](#)

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 networks that are not relevant to the management tasks you are using Security Manager to perform, for example, test networks. For the procedure, see [Working with AutoLink, page 2-61](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **AutoLink**.

Related Topics

- [Displaying Layer 3 Links on the Map, page 4-21](#)
- [Displaying Your Network on the Map, page 4-16](#)
- [Understanding Maps, page 4-1](#)
- [Working With Maps, page 4-2](#)

Field Reference

Table A-1 *AutoLink Settings Page*

Element	Description
IP addresses	Selected by default and grouped by category. There are five: three internal, one used for loopback testing, and one for multicast routing. Deselect the check box for each IP address you want to omit from any topology 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.

Configuration Archive Settings Page

From the Configuration Archive page, you can purge configuration file versions maintained for devices managed by Security Manager. Here you can also enter the TFTP server and directory information for Cisco IOS and Catalyst OS devices used during configuration rollback. For the procedure, see [Defining Configuration Archive Settings, page 2-62](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Configuration Archive**.

Related Topics

- [Configuration Archive Window, page Q-12](#)
- [Using the Configuration Archive Tool, page 20-11](#)

Field Reference

Table A-2 Configuration Archive Settings Page

Element	Description
Max. Versions per Device	Enter how many versions you want to retain for each device after you click Purge Now . Values are 1 through 100.
Purge Now button	Deletes all configuration versions for each device older than the number you entered in Max. Versions Per Device field.
TFTP Server for Rollback	The server name or IP address for TFTP file transfers to be used for IOS devices only.
TFTP Root Directory	The root directory for configuration file transfers on your TFTP server.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Customize Desktop Page

Adjust your GUI timeout and ‘Do Not Ask’ settings from the Customize Desktop page. For the procedure, see [Customizing Your Desktop, page 2-64](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Customize Desktop**.

Field Reference

Table A-3 Customize Desktop Page

Element	Description
Reset ‘Do Not Ask’ on Warnings button	Reestablishes ‘Are you sure . . .?’ pop-up reminders. You might want to do this if you enabled any Do Not Ask Me Again settings in the application.
Enable Idle Timeout	When selected enables the idle timeout for the user interface.

Table A-3 *Customize Desktop Page (continued)*

Element	Description
Idle Timeout (minutes)	The number of minutes Security Manager waits for input before logging the user out of the system and disconnecting the server. The default is 120 minutes.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Deployment Page

Use the Deployment page to define the methods by which Security Manager deploys configurations to devices. To make changes for only a single device, see [Working with Device Policies, page 5-54](#).

For the procedure, see [Defining Deployment Settings, page 2-65](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Deployment**.

Related Topics

- [Managing Deployment, page 18-1](#)
- [Managing Objects, page 8-1](#)
- [Policy Object Manager User Interface Reference, page F-1](#)

Field Reference

Table A-4 *Deployment Page*

Element	Description
Deployment	
Purge Debugging Files Older Than* (days)	The maximum number of days the system should keep debugging files. You can click Purge Now to immediately delete all debugging files older than the number of days specified.

Table A-4 Deployment Page (continued)

Element	Description
Purge Now button	Immediately deletes debugging files older than the number of days specified in the Purge debugging files older than (days) field. For example, if you change the number of days from 10 to 7 and click Purge Now all debugging files older than 7 days are deleted.
Default Deployment Method	Specifies how configurations are deployed to devices. You can pick one of the following: <ul style="list-style-type: none"> • Device (default)—Configurations deploy directly to a device unless the device is unreachable. • File—Configurations deploy to a file.
Directory	If you selected File as the default deployment method, enter a directory path to which the file should be saved. Or you can click Browse to select the directory to which to save the file.
When Out of Band Changes Detected	Specifies how Security Manager responds when it detects changes made directly to the device CLI and the change is then deployed. You can choose one of the following: <ul style="list-style-type: none"> • Warn—Deployment proceeds, but a warning message is displayed. • Cancel—Deployment stops. • Skip—Deployment proceeds without checking for out-of-band changes.
Deploy to File Reference Configuration	Use when the selected deployment method is File. Specifies the configuration against which changes are compared. You can choose one of the following: <ul style="list-style-type: none"> • Archive (default)—The most recently archived configuration. • Device—The current device configuration. <p>After comparing the configurations, Security Manager generates the correct CLI for deployment.</p>

Table A-4 Deployment Page (continued)

Element	Description
Deploy to Device Reference Configuration	<p>Use when the selected deployment method is Device. Specifies the configuration against which changes are compared. You can choose one of the following:</p> <ul style="list-style-type: none"> • Archive (default)—The most recently archived configuration. • Device—The current device configuration. <p>After comparing the configurations, Security Manager generates the correct CLI for deployment.</p>
Optimize the Deployment of Access Rules For	<p>Specifies how firewall rules are deployed. You can choose one of the following:</p> <ul style="list-style-type: none"> • 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 the ACL line number feature, 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 becomes 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. <p>Note You cannot choose a deployment speed on devices that do not support ACL line numbers.</p>

Table A-4 Deployment Page (continued)


Element	Description
Firewall Access-Lst Names	<p>Determines how ACL names are deployed to devices.</p> <ul style="list-style-type: none"> Reuse existing names—Recognizes user-defined ACL names that were configured on the device. See Preserving User-Defined ACL Names, page 12-56. Reset to CS-Manager generated names—Recognizes Security Manager auto-generated ACL names. See How ACL Names Are Generated, page 12-54.
Disable Access-list Compilation During Deployment (FWSM)	<p>When selected, FWSM automatically determines for itself when to compile access lists. Selecting this option might increase deployment speed but traffic might be disrupted and the system may become incapable of reporting ACL compilation error messages.</p> <p>When deselected, Security Manager controls ACL compilation to avoid traffic interruption and to minimize peak memory usage on the device. For more information, see Understanding Access Rules, page 12-49.</p> <p> Caution You should not select this option unless you are experiencing deployment problems and are an advanced user.</p>
Enable Advanced Debugging	<p>When selected, Security Manager generates data files about configuration generation, deployment, and discovery as these functions are performed. The temporary data files are stored in a temporary directory that you can use for debugging.</p> <p>Note Selecting this check box slows down product response time.</p>
Allow Download on Error	<p>When selected, enables deployments to devices to continue even if there are minor device configuration errors.</p>
Remove Unreferenced Object Groups on Device (PIX, ASA, FWSM)	<p>When selected, any object groups that are not being used by other CLI commands are removed from devices during deployment.</p>

Table A-4 Deployment Page (continued)

Element	Description
Create Object Groups for Policy Objects (PIX, ASA, FWSM)	When selected (default) Security Manager creates object groups, such as network objects and service objects, for PIX, ASA, and FWSM devices. When deselected, Security Manager flattens the object groups to display the IP addresses, sources and destinations, ports, and protocols for PIX/ASA/FWSM devices. Deselecting this check box also disables the check box that follows, Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM).
Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM)	When selected, you can elect to automatically create network objects and service objects to replace comma-separated values in a rule table cell that resulted when multiple rules were combined. The objects are created during deployment. This check box is disabled when the preceding check box, Create Object Groups for Policy Objects (PIX, ASA, FWSM), is deselected. For more information, see Combining Rules, page 12-11 .
Remove Unreferenced Access-lists on Device	When selected, any access lists that are not being used by other CLI commands are removed from devices during deployment.
Save Changes Permanently on Device	When selected, ensures that any changes to the device configuration for PIX, FWSM, ASA, or Cisco IOS devices are copied to the startup configuration for that device. Deselect this check box to keep startup configuration as is.
Generate ACL Remarks During Deployment	When selected, displays ACL warning messages during deployment.
Optimize Network Object Groups During Deployment (PIX, ASA, FWSM)	When selected, optimizes network object groups when you generate configurations for PIX, FWSM, and ASA devices for deployment. For more information, see Optimizing Policy Objects in Rules, page 12-47 .
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults. The default is to enable any configuration changes to be saved to startup configuration.

Device Communication Page

Use the Device Communication page to define these settings:

- The number of seconds that Security Manager has to establish a connection with a device before timing out.
- The number of seconds Security Manager can spend blocked waiting for incoming data.
- Whether to use HTTP or HTTPS as the default transport protocol for contacting Cisco IOS IPS routers and IPS sensors.
- Whether to use SSL, SSH, Telnet, or TMS as the default transport protocol for contacting Cisco IOS devices running IOS versions 12.3 and later.
- Whether to use SSH or Telnet as the default transport protocol for contacting Catalyst 6500 Series switches and Cisco 7600 Series routers.
- Whether to use SSH or Telnet as the default transport protocol for contacting routers running Cisco IOS software release 12.1 or 12.2.
- The credentials that Security Manager uses to contact the device for various operations, such as deployment, discovery, and rollback of configurations.
- Whether and when to authenticate device certificates for devices that use SSL firewall devices, FWSMs, ASAs, IPS devices, and Cisco IOS devices.
- The HTTPS port number to be used for secure communication between Security Manager and a device.
- Whether Security Manager applies changes to SSH keys made directly on the device.

For the procedure, see [Defining Device Communication Settings, page 2-68](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Device Communication**.

Related Topics

- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Managing Devices, page 5-1](#)
- [Preparing the Devices for Security Manager to Manage, page 5-2](#)

Field Reference

Table A-5 Device Communication Page

Element	Description
Device Connection Parameters	
Device Connection Timeout	Enter the number of seconds that Security Manager has to establish a connection with a device before timing out.
Retry Count	Enter the number of times that Security Manager tries to establish a connection before failing. The default value is 3. An error message displays at the third (or whatever number of times you enter) failed attempt of Security Manager to connect to device.
Socket Read Timeout	(For SSH and telnet sessions only.) Enter the maximum number of seconds Security Manager can spend blocked waiting for incoming data. If no incoming data is received within this period an error displays.
Transport Protocol (IPS)	Select HTTPS or HTTP as the transport protocol to use when contacting Cisco IOS routers and IPS devices. For more information, see Preparing the Devices for Security Manager to Manage, page 5-2 .
Transport Protocol (IOS Routers 12.3 and above)	Select HTTPS, SSH, Telnet, or TMS transport protocol to use when contacting Cisco IOS devices. For more information, see Preparing the Devices for Security Manager to Manage, page 5-2 .
Transport Protocol (Catalyst 6500/7600)	Select SSH or Telnet as the transport protocol to use when contacting Catalyst 6500 Series switches and Cisco 7600 Series routers. For more information, see Preparing the Devices for Security Manager to Manage, page 5-2 .
Transport Protocol (IOS Routers 12.2, 12.1)	Select SSH or Telnet as the transport protocol to use when contacting routers running Cisco IOS software release 12.1 and 12.2. For more information, see Preparing the Devices for Security Manager to Manage, page 5-2 . Note This selection does not apply to Catalyst 6500/6000 series switches running Cisco IOS software 12.2 or earlier.

Table A-5 Device Communication Page (continued)

Element	Description
Connect to device using	<p>Select the Security Manager credentials option to be used to access the device from the list:</p> <ul style="list-style-type: none"> • 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 added to the inventory, regardless of the credentials configured for each device in the Device Credentials page. The login credentials are discarded when you exit the Security Manager client or the idle session timeout period is exceeded. • Security Manager Device Credentials—Security Manager contacts the device using the credentials that you specified in the Device Credentials page when you added the device to the inventory or Device Properties page after you added the device to Security Manager. This is the default. Selecting this option is the same as the behavior that existed in Security Manager 3.0.1 and earlier to establish communication with the device.
SSL Certificate Parameters	
IPS Device Authentication Certificates	<ul style="list-style-type: none"> • Select Retrieve while adding devices to enable Security Manager to automatically obtain certificates from IPS devices while you add one or more devices from the network or DCR. Security Manager calculates the IPS device certificate thumbprints and stores the calculated thumbprints in the certificate data store. For information and procedures see Adding Devices to the Security Manager Inventory, page 5-30. • Select Manually add certificates to prevent Security Manager from automatically accepting certificates from the Add Device From Network or the Add Device From DCR wizards (see Adding Devices to the Security Manager Inventory, page 5-30). You must add the device thumbprint manually before adding the IPS devices by clicking Add Certificate or from Device Properties pages to be successful. See Adding Certificates for IPS Devices, Cisco IOS Devices, and PIX/ASA/FWSM Devices, page 2-73. • Select Do not use certificate authentication to prevent automatic certificate validation for IPS devices using SSL.

Table A-5 Device Communication Page (continued)

Element	Description
IOS Device Authentication Certificates	<ul style="list-style-type: none"> • Select Retrieve while adding devices to enable Security Manager to automatically obtain certificates from Cisco IOS devices while you add one or more devices from the network or DCR. Security Manager calculates the device certificate thumbprints and stores the calculated thumbprints in the certificate data store. For information and procedures see Adding Devices to the Security Manager Inventory, page 5-30. • Select Manually add certificates to prevent Security Manager from automatically accepting certificates from the Add Device From Network or the Add Device From DCR wizards (see Adding Devices to the Security Manager Inventory, page 5-30). You must add the device thumbprint manually before adding the IOS devices by clicking Add Certificate or from Device Properties pages to be successful. See Adding Certificates for IPS Devices, Cisco IOS Devices, and PIX/ASA/FWSM Devices, page 2-73. • Select Do not use certificate authentication to prevent automatic certificate validation for IOS devices using SSL.
PIX/ASA/FWSM Device Authentication Certificates	<ul style="list-style-type: none"> • Select Retrieve while adding devices to enable Security Manager to automatically obtain certificates from firewall devices while you add one or more devices from the network or DCR. Security Manager calculates the device certificate thumbprints and stores the calculated thumbprints in the certificate data store. For information and procedures see Adding Devices to the Security Manager Inventory, page 5-30. • Select Manually add certificates to prevent Security Manager from automatically accepting certificates from the Add Device From Network or the Add Device From DCR wizards (see Adding Devices to the Security Manager Inventory, page 5-30). You must add the device thumbprint manually before adding the firewall devices by clicking Add Certificate or from Device Properties pages to be successful. See Adding Certificates for IPS Devices, Cisco IOS Devices, and PIX/ASA/FWSM Devices, page 2-73. • Select Do not use certificate authentication to prevent automatic certificate validation for firewall devices using SSL.

Table A-5 Device Communication Page (continued)

Element	Description
Accept Device SSL Certificate after Rollback	Select to obtain the certificate installed on a firewall device, FWSM, ASA, or Cisco IOS router when you roll back the configuration on the device. Note that this is true only for devices that use SSL as their transport protocol.
Add certificate button	Opens the Add Certificate Dialog Box . See Add Certificate Dialog Box, page A-14 .
HTTPS Port Number	<p>Enter the 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.</p> <p>In addition to providing access to the device via the Cisco web browser user interface, HTTPS port number is used by device management applications, such as the Cisco Router and Security Device Manager (SDM), and monitoring tools, such as IPS Event Viewer (IEV), to communicate with the device.</p> <p>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.</p>
Overwrite SSH Keys	<ul style="list-style-type: none"> • Select to allow Security Manager to apply changes in the device's SSH keys when they are updated directly on the device. • Deselect this check box with caution, and only if a greater level of security is necessary. Security manager does not communicate with the device if keys are changed on the device.
Save button	Saves and applies changes.

Add Certificate Dialog Box

With Security Manager, you can 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 the procedure, see [Adding Certificates for IPS Devices, Cisco IOS Devices, and PIX/ASA/FWSM Devices, page 2-73](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Device Communication**. Click **Add Certificate...**

Field Reference

Table A-6 *Add Certificate Dialog Box*

Element	Description
Host Name or IP Address	Hostname or IP address of the device from which you are retrieving the certificate.
Certificate Thumbprint	The string of hexadecimal digits that is unique to each device certificate.
OK button	Initiates device contact and adding of certificate thumbprint.

Device Groups Page

Use the Device Groups page to create group types (the highest level of the hierarchy) and groups, to delete groups, and to modify group names. For more information, see [Working with Device Groups, page 2-75](#).

Navigation Path

Select **Tools > Security Manager Administration > Device Groups**.

Related Topics

- [Understanding Device Grouping, page 5-57](#)
- [Working With Device Groups, page 5-59](#)

Field Reference

Table A-7 Device Groups Page

Element	Description
Add Type button	Creates a new group type.
Add(+) button	Creates a group or subgroup.
Save button	Saves your changes and closes the page.
Reset button	Restores all fields to their previous values.

Device OS Management Page

Security Manager 3.1 integrates several key features from Resource Manager Essentials (RME). You can use software management to analyze individual device operating system versions (also known as image versions) and to generate image analysis reports. This allows you to import and distribute operating system images to groups of devices. You can also schedule operating system upgrade jobs to ensure up-to-date versions and to minimize errors. For more information, and for detailed procedures, see [Working With Device OS Management, page 20-6](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Device OS Management**.

Related Topics

- [Resource Manager Essentials Documentation](#)
- [Working With Device OS Management, page 20-6](#)

Field Reference

Table A-8 Device OS Management

Element	Description
RME server address	IP address of RME server.
Connect using https	When selected indicates you are connecting to RME server using SSL.

Table A-8 **Device OS Management (continued)**

Element	Description
Save button	Saves your changes to the Security Manager database.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Discovery Page

From the Discovery page you can define how long to keep a record of discovery and device-import tasks. Any tasks older than the number of days you specify will be deleted. You can also determine whether to substitute any matching named objects that are already defined in Security Manager for any inline values found in the CLI, and whether to roll back all policies if an error is encountered during policy discovery. For the procedure see [Defining Discovery Settings, page 2-76](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Discovery**.

Related Topics

- [Frequently Asked Questions about Policy Discovery, page 6-13](#)
- [Understanding the Policy Object Manager Window, page 8-5](#)

Field Reference

Table A-9 Discovery Page

Element	Description
Prepend Device Name when Generating Security Context Names	<p>Selecting this check box prepends device names (that is, the device display names) when generating security context names. This turns off the Security Manager default naming method.</p> <p>Note By selecting this option, you disable Security Manager’s method for ensuring unique names. Instead, Security Manager will append a number to any duplicate name it encounters. (So, for example, the name “mydevice” when encountered a second time would be rendered as “mydevice_01”.)</p>
Purge discovery tasks older than (days)	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	When selected substitutes any named policy objects, such as IP addresses already defined in Security Manager for inline values in the CLI. For more information on policy objects, see Managing Objects, page 8-1 .
Allow Device Override for Discovered Policy Objects	For certain types of objects, selecting this check box enables you to override the parent object values at the device level. For more information see, Overriding Global Objects for Individual Devices, page 8-196 .
On error, rollback discovery for entire device	When selected, rolls back all discovered policies if even one error is encountered for a single policy. 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 6-7 .
Auto-Expand object-groups with prefixes.	For more information, see Expanding Object Groups During Discovery, page 12-49 .
Save button	Saves your changes to the Security Manager database.
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 and download updates
- Configure an IPS update server
- Configure automatic update settings

Navigation Path

Select **Tools > Security Manager Administration**, then click **IPS Updates**.

Related Topics

- [Establishing the IPS Update Server, page 2-78](#)
- [Administering IPS Updates, page 2-79](#)
- [Automating IPS Updates, page 2-80](#)



Caution

If you did not set Category CLI commands on your IOS IPS device to select a subset of IPS signatures that the device will attempt to compile, Security Manager will push CLI commands to enable the IOS IPS Basic category to prevent the device resources from being overloaded. These CLI commands are not managed by Security Manager after they are deployed. You can change these manually on the device to select another set of signatures to compile.

Field Reference

Table A-10 IPS Updates Page

Element	Description
Update Status area	<p>The Update Status area of the IPS Updates page lists the following items:</p> <ul style="list-style-type: none"> • Most recent signature and sensor update available on Cisco.com or local HTTP server • Most recent signature and sensor update downloaded to Security Manager • Most recent signature and sensor update deployed to any device in Security Manager • Time that last check of Cisco.com was performed • Time that last update was downloaded to Security Manager • Time that last update was deployed to any of the devices
Check for Updates	When clicked, opens a new window to check sensors for updates. Clicking Start then initiates the checking process.
Download Latest Updates button	When clicked, downloads the most recent sensor update package and the most recent signature update package to the Security Manager server if those packages have not already been downloaded.
Update Server area	<p>The Update Server area of the IPS Updates page contains the settings used to access Cisco.com or the local server that contains the update packages. The area lists the following items:</p> <ul style="list-style-type: none"> • Get Updates From • Update Server • User Name • Proxy Server
Edit Settings	Opens the Edit Update Server Settings dialog box. For more information, see Establishing the IPS Update Server, page 2-78
Auto Update Settings	Contains the settings specific to automatic updates. For more information, see Automating IPS Updates, page 2-80

Table A-10 IPS Updates Page (continued)

Element	Description
Auto Update Mode	<p>Establishes whether, and to what extent, automatic updates are performed. Contains the following options:</p> <ul style="list-style-type: none"> • Download, Apply, and Deploy Updates • Disable Auto Update • Check for Updates • Download Updates • Download and Apply Updates <p>By default, auto update is disabled. The other options are a combination of one or more of the following options:</p> <ul style="list-style-type: none"> • Check for Updates: CSM server contacts Cisco.com or Local HTTP Server to check if update available and send email if email notification configured. • Download Updates: CSM server downloads latest updates from Cisco.com or Local HTTP Server, and send email notification if configured. • Apply Updates: Modifies device configuration on CSM server based on the downloaded update package(s). • Deploy Updates: Send applicable update package(s) to device(s) if device(s) has Auto Update turned on.
Check for Updates At	<p>Determines when Cisco.com or the local server will be checked for updates. Time is entered in <i>hh:mm:ss</i> format. After you enabled it, a job will be scheduled and will happen daily at this time. If the selected “Auto Update Mode” is “Download, Apply, and Deploy Updates”, then the scheduled job will Check for Updates first followed by Download, Apply and Deploy Updates.</p>

Table A-10 IPS Updates Page (continued)

Element	Description
Notify Email	<p>Defines the email address to which notifications of automatic updates are sent. Only one email address can be entered. A notification is sent when an update meets one of the following conditions:</p> <ul style="list-style-type: none"> • Is available for download • Has been downloaded • Has been downloaded and applied • Has been downloaded, applied, and deployed. <p>The notification contains the status of the operation; for example, “<i>An update was successfully deployed to 12 of 12 devices.</i>”</p>
Deploy Updates	<p>Contains the following options:</p> <ul style="list-style-type: none"> • When applied • At the time specified <p>If “When applied” is selected, the Time field is disabled. The update is deployed as soon as it is downloaded . If “At the time specified” is selected, the Time field is enabled. The update is deployed at the time entered. If the download is not completed when the specified deployment time is reached, then the deployment occurs as soon as the download is completed. By default, this field is set to “When applied.” It is always disabled in non-workflow mode. It means if the “Download, Apply, and Deploy Updates” is chosen, then deploy to real devices always happens right after new packages are downloaded and applied.</p>
Time	<p>Indicates at what time the downloaded update should be deployed to devices. If the download is not completed when the specified time is reached, the deployment occurs as soon as the download is complete. This field is unavailable when "When Downloaded" is selected under Deploy Updates. Time is entered in <i>hh:mm:ss</i> format.</p>

Table A-10 *IPS Updates Page (continued)*

Element	Description
Apply Update To	A table which is used to define the auto update properties of the devices. The context menu and the edit button both open the Modify Signature Update Policies dialog box. The left-hand side of the table and the “Type” dropdown list provide a quick way for turning on Auto Update settings for devices based on Local Signatures Policies and Shared Signatures Policies; and the right hand side panel “Devices to be Auto Updated:” lists device(s) with Auto Update turned on.
Type	Allows you to switch between a list of “Local Signatures Policies” and a list of “Shared Signatures Policies.” Signatures are used as a convenient way to select, group, and turn on/off a device’s Auto Update setting. When “Shared Signatures Policies” is selected, the shared signature inheritance tree is shown. Each shared signature policy may have one or more devices assigned to it. If assigned devices have different Auto Update settings, the checkboxes next to the policy will be partial selected (grayish checked box).

Edit Update Server Settings Dialog Box

Use the upper portion of the Edit Update Server Settings dialog box to configure or edit the configuration of the server for use with IPS updates performed using auto update. In the lower half of this dialog box, you can configure or edit the configuration of a proxy server.

Navigation Path

Select **Tools > Security Manager Administration**, then click **IPS Updates** and **Edit Settings**.

Table A-11 *Edit Update Server Settings Dialog Box*

Element	Description
<i>(Upper Section: Server Settings)</i>	
Update From	Select from the list whether to get update from Cisco.com or from a local server. The local server is an HTTP server that you need to set up if you decide to use it.
IP Address/ Host Name	Hostname or IP address of the IPS update web server.

Table A-11 Edit Update Server Settings Dialog Box

Element	Description
Web Server Port	The port number that your local server listens on. The default value is 80.
User Name	The user name that Security Manager uses when connecting to your local server. If your local server does not need authentication, then leave this field blank.
Password	The password that Security Manager uses when connecting to your local server. If your local server does not need authentication, then leave this field blank.
Confirm	Re-enter the password. This action verifies that this password matches the one entered in the previous field.
Path to Update Files	The path to the IPS update files location on your local server. For example, if update files can be accessed at <code>http://local-server-ip:port/update_files_path/</code> , then type in <code>update_files_path</code> in this text field.
Connect Using HTTPS	When selected, indicates you are connecting to the IPS web using SSL.
(Lower Section: Proxy Server)	
Enable Proxy Server	When selected, indicates that a proxy server is needed to connect to Cisco.com or to your local server.
IP Address/ Host Name	Host name or IP address of the proxy server.
Web Server Port	The port number that the proxy server listens on. The default value is 80.
User Name	The user name that Security Manager uses when connecting to the proxy server. If the proxy server does not need authentication, then leave this field blank.
Password	The password that Security Manager uses when connecting to the proxy server. If the proxy server does not need authentication, then leave this field blank.
Confirm	Re-enter the password. This action verifies that this password matches the one entered in the previous field.

Modify Signature Update Policies Dialog Box

Use the Modify Signature Update Policies dialog box to configure auto update options for a device or group of devices in the Apply Update To table. You can access the Modify Signature Update Policies dialog box from the shortcut menu and the Edit button.

Licensing Page

The Licensing Page allows you to manage licenses for both Security Manager and IPS devices. The following tabs are available on the Licensing Page:

- [CSM Tab, page A-26](#)
- [IPS Tab, page A-27](#)

CSM Tab

From the CSM tab on the Licensing page you can view a record of installed Security Manager licenses and install new Security Manager licenses from Cisco.com or from a server to which a new Security Manager license has been sent.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Licensing** and the **CSM** tab.

Field Reference

Table A-12 *Licensing Page > CSM Tab*

Element	Description
License Information	Displays all relevant information about the license registered with the product: Edition, License Type, Expiration, Number of Licensed Devices, Number of Devices in Use, and Percentage device count used.
Install License	Displays a record of installed licenses and installation dates.
Install a License button	Enables you to obtain license file from Cisco.com or hard drive.

IPS Tab

From the IPS tab on the Licensing page you can view a record of installed IPS device licenses, update IPS device licenses from Cisco.com or from local license files, or redeploy licenses. The IPS license list shows not only current licenses, but also unlicensed devices, devices with expired licenses, and devices with invalid licenses.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Licensing** and the **IPS** tab.

Related Topics

- [Updating Licenses via CCO Dialog Box, page A-28](#)
- [Redeploying Licenses Dialog Box, page A-29](#)
- [Updating Licenses from File Dialog Box, page A-30](#)

Field Reference

Table A-13 *Licensing Page > IPS Tab*

Element	Description
IPS License Table	License summary displaying all relevant information about the license registered with the IPS device: Type, Device, Serial Number, Status, and Expiration date. The IPS license list shows not only current licenses, but also unlicensed devices, devices with expired licenses, and devices with invalid licenses.
Update Selected from CCO	Click to update the license file for the selected device(s) by connecting to CCO. The updated file is automatically applied.
Update from License File	Click to update the license file for the selected device(s) by navigating to a stored license file. The updated file is automatically applied.
Redeploy Selected License	Click this button when you have obtained an updated license file that was not applied to the device successfully during the automatic update.

Table A-13 *Licensing Page > IPS Tab (continued)*

Element	Description
Download and apply licenses automatically	Sets the system to automatically download and apply IPS licenses. To enable this feature, select the Download and apply licenses automatically check box and then specify how frequently Security Manager should check for new licenses using the Check list: <ul style="list-style-type: none"> • Daily: Once a day at midnight • Weekly: Once a week at midnight on Sunday • Monthly: Once a month at midnight on the first day of the month.
Refresh	Click to refresh the data in the IPS license table.

Updating Licenses via CCO Dialog Box

When you click **Update Selected via CCO. . .**, the Updating Licenses via CCO dialog box displays the list of IPS devices that you selected and for which you can update the license. Only supported devices are displayed.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Licensing** and the **IPS** tab. Next, select an IPS device in the table, then click **Update Selected via CCO**. Click **OK**.

Field Reference

Table A-14 *Updating Licenses via CCO Dialog Box*

Element	Description
Device List	A list of IPS devices for which you can update the license through communication with Cisco.com.

License Update Status Details Dialog Box

The License Update Status Details dialog box displays all relevant information about the license registered with the IPS device and the details of its update.

Field Reference

Table A-15 License Update Status Details Dialog Box

Element	Description
License Update Status Details	<p>Displays all relevant details about the status of the license update for the IPS device(s) that was (were) selected for update:</p> <ul style="list-style-type: none"> • Summary listing of Status, Devices to be updated (number of devices), Devices updated successfully (number of devices), Devices updated with errors (number of devices), and a heading that shows who ordered the update and when. • Tabular listing of Type, Device, Status, and Summary • Tabular listing of Messages and their Severity • Text listing of Description and Actions taken
Abort	Stops the update
Close	Closes the License Update Status Details

Redeploying Licenses Dialog Box

Use the Redeploying Licenses dialog box to see and confirm a list of IPS devices for which you are redeploying licenses.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Licensing** and the **IPS** tab. Select an IPS device in the table, and then click **Redeploy Selected License**.



Note

You must deploy the license file to the sensor before you can select the Redeploy button.

Field Reference

Table A-16 *Redeploying Licenses Dialog Box*

Element	Description
Device List	A list of IPS devices for which you are redeploying licenses.

Updating Licenses from File Dialog Box

Use the Updating Licenses from File dialog box to update the license for a particular IPS device when you have a license file stored locally or on your network.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Licensing** and the **IPS** tab. Finally, select an IPS device in the table and then click **Update from License File. . .**

Field Reference

Table A-17 *Update from License File Dialog Box*

Element	Description
License File	Name of local file (obtained by browsing) that contains the license needed to update a particular IPS device.
Browse	Opens the Choose The License Files dialog box, from which you can navigate to a particular license file from which to update.

Logs Page

When state changes occur in Security Manager, an event is generated and an audit entry is created in the audit log. You can display the aggregated results of the audit entries by defining the parameters in the Audit Report page. The System Administration Logs page allows you to determine how long to keep log files archived. For the procedure, see [Archiving Log Files, page 2-88](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Logs**.

Related Topics

- [Audit Report Page, page Q-8](#)
- [Understanding Audit Reports, page 20-7](#)

Field Reference**Table A-18** **Logs Page**

Element	Description
Keep Audit Log For (days)	The number of days to save audit report entries before deleting them. This field is used with the Purge Audit Log after (entries) field. Entries are deleted based on the number of days or entries, whichever maximum is reached first.
Purge Now button	Immediately purges entries older than the number of days specified in the Keep Audit Log For field.
Purge Audit Log after (entries)	The maximum number of audit report entries to save. This field is used with the Keep Audit Log For (days) field. Entries are deleted based on the number of days or entries, whichever maximum is reached first.
Keep Operation Log For (days)	The number of days that Security Manager keeps operation logs before deleting them. These logs are used for debugging purposes.
Log Level	Specifies the level of information, according to severity, that you would like collected in the operation logs. Valid choices are Severe, Warning, and Info. Each level collects different amounts of data. For example, the Info level yields the most data, and the Severe level collects the least. Note If you select the Info level (greatest amount of data), system performance might be slower than expected.
Save button	Saves your changes to the Security Manager database.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Policy Management Page

Customizing policy management settings on a Cisco IOS router makes it possible, for example, to use Security Manager to manage DHCP and NAT policies on Cisco IOS routers while leaving routing protocol policies, such as EIGRP and RIP, unmanaged. These settings, which can be modified only by a user with administrative permissions, apply globally in Security Manager.

Unmanaged policies are removed from both Device view and Policy view. Any unmanaged policies, local or shared, are removed from the Security Manager database.

You cannot unmanage a policy type if you have configured and assigned policies of that type in Security Manager. You must first remove the assignments and then unassign the policy type. If the configurations defined by those policies have already been deployed, these configurations are left in place on the devices, but the policies are no longer stored in the database or accessible from the Security Manager interface. For the procedure, see [Defining Policy Management Settings, page 2-89](#).

Navigation Path


Select **Tools > Security Manager Administration**, then click **Policy Management**.

Related Topics

- [Advanced Policy Features, page 6-49](#)
- [Managing Policies, page 6-1](#)
- [Managing Routers, page 14-1](#)
- [Managing Shared Policies in Policy View, page 6-40](#)
- [Understanding Policies, page 6-1](#)

Field Reference

Table A-19 Policy Management Page

Element	Description
Policies to Manage	<p>Displays the router platform policies that Security Manager manages, organized by category (NAT, Router Interfaces, and Router Platform). By default, all policies are selected. Deselected router platform policies are not managed. Deselecting the check box for a group of policies deselects all policies in that group.</p> <p> Note Unmanaged policies are removed from the Policy selectors in Device view and Policy view.</p>
Save button	Saves your changes to the Security Manager database.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Policy Objects Page

Use the Policy page to define these policy object settings:

- The warning behavior of Security Manager when identical objects are found.
- The default source ports for service objects.

For the procedure, see [Defining Policy Object Settings, page 2-91](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Policy Objects**.

Related Topics

- [Managing Objects, page 8-1](#)

Field Reference

Table A-20 Policy Objects Page

Element	Description
When Redundant Objects Detected (Conflict Detection)	<p>Defines 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:</p> <ul style="list-style-type: none"> • 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. <p>For more information, see Guidelines for Managing Objects, page 8-4.</p>
Default Source Ports	<p>Specifies the port range value that is used as the default source port range for service objects.</p> <p>You can choose one of the following:</p> <ul style="list-style-type: none"> • Use all ports—Includes all ports from 1 to 65535. • Use secure ports—Includes all ports from 1024 to 65535. <p>Note If you change the default source ports (Use all 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.</p> <p>For more information on objects, see Understanding Port List Objects, page 8-149.</p>
Save button	Saves your changes to the Security Manager database.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Server Security Page

Common Services provides the administrative functions that control a user's access in Security Manager. Security Manager provides access to these functions through the Server Security page. The buttons found in the Server Security page are actually a series of buttons that open Commons Services functions.

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 [Setting Up User Permissions, page 2-3](#). For the procedure, see [Working with Server Security, page 2-92](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Server Security**.

Field Reference

Table A-21 *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.

Table A-21 **Server Security Page (continued)**

Element	Description
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.
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.

Status Page

From the Status page you can enable deployment and Monitoring Center for Performance to send status updates to Security Manager. You can also access the Add and Edit Status Providers dialog boxes in order to set up a connection for these status providers. You can use the Inventory Status window from the Tools menu to view the events reported by status providers. For more information, and a procedure to configure status providers, see [Working with Status Providers, page 2-94](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Status**.

Related Topics

- [Add Status Provider Dialog Box, page A-37](#)
- [Edit Status Provider Dialog Box, page A-39](#)
- [Inventory Status Window, page Q-6](#)
- [Understanding Inventory Status, page 20-6](#)

Field Reference

Table A-22 Status Page

Element	Description
Connect Devices Status	
Deployment	When selected, displays details about deployment jobs for devices to the Status tab of the Inventory Status window. Deselect only if you do not want Deployment to appear as a column in the Inventory Status table. Selected is the default mode.
Providers table	
Provider	Monitoring Center for Performance (Performance Monitor) is the only external status provider available for monitoring in this release. If more than one instance is available on different servers, enter a short name or server name to distinguish one location from another. Each name you enter here appears as a separate column in the Inventory Status table.
Short name	Nickname, if any, for provider name above.
Status	Pull-down menu allowing you to select Enabled or Disabled . Specifies whether to enable or disable the display of status reported by the external status provider. The default is Enabled.
Add provider button(+)	Click to display the Add Status Provider dialog box to configure a new status provider.
Edit provider button	Click to display the Edit Status Provider dialog box to edit the status provider settings.
Trash button	Click to discard status provider name and contact information.
Save button	Saves your changes to the Security Manager database.
Reset button	Resets changes to the previously applied values.

Add Status Provider Dialog Box

Use the Add Status Provider dialog box to add Performance Monitor server contact information, so that Security Manager can check Performance Monitor event status, and report back, by creating an entry in the Inventory Status table in the Tools menu.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Status**. Click the Add button(+) to open the Add Status Provider dialog box. For a detailed procedure see [Working with Status Providers, page 2-94](#).

Related Topics

- [Edit Status Provider Dialog Box, page A-39](#)
- [Inventory Status Window, page Q-6](#)
- [Status Page, page A-36](#)
- [Understanding Inventory Status, page 20-6](#)

Field Reference

Table A-23 *Add Status Provider Dialog Box*


Element	Description
Provider name	The name of the service provider, for example, Performance Monitor. You can enter up to 128 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ : . and space.
Server	The DNS host and domain names for Performance Monitor. You can enter up to 128 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ : . and space. The domain name resolution requires that you configure at least one DNS name server on Security Manager. You can configure one or more DNS name servers. Routable domain names are fully qualified domain names (FQDN).
	 <hr/> <p>Note This field does accept IP addresses.</p>
Short Name	Short name, if any, for provider name above. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ : . and space.
Port	The port number that Security Manager uses to communicate with Performance Monitor. The default is 443.
Poll Cycle	The number of minutes the firewall device will wait between polling Performance Monitor for new information. The default is 600 seconds (5 minutes). Minimum time is 60 seconds.

Table A-23 Add Status Provider Dialog Box (continued)

Element	Description
Username	The username for logging in to Performance Monitor. Maximum length is 70 characters.
Password	The password for logging in to Performance Monitor. In the Confirm field, enter the password again. Maximum length is 70 characters.
URN	The uniform resource name for Performance Monitor. URN is the name that identifies the resource on the Internet. URN is part of a URL, for example, /status/StatusServlet. The full URL could be: https://:<server ip>:443/status/StatusServlet where: <ul style="list-style-type: none"> • <server ip> is the IP address of Performance Monitor. • 443 is the port number of Performance Monitor. • /status/StatusServlet is the URN of the Performance Monitor.
Status	Select Enabled from the pull-down menu to specify whether Security Manager needs to poll Performance Monitor for event details and display in the Inventory Status window. Alternatively, choose Disabled for Security Manager to stop polling Performance Monitor.
OK	Saves status provider information.

Edit Status Provider Dialog Box

Use the Edit Status Provider dialog box to revise Performance Monitor contact information you have entered using the Add Status Provider dialog box.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Status**. Click the Edit button to open the Edit Status Provider dialog box. For a detailed procedure see [Working with Status Providers, page 2-94](#).

Related Topics

- [Add Status Provider Dialog Box, page A-37](#)
- [Inventory Status Window, page Q-6](#)

- [Status Page, page A-36](#)
- [Understanding Inventory Status, page 20-6](#)

Field Reference

Table A-24 **Edit Status Provider Dialog Box**


Element	Description
Provider name	The name of the service provider, for example, Performance Monitor. You can enter up to 128 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ : . and space.
Server	The DNS host and domain names for Performance Monitor. You can enter up to 128 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ : . and space. The domain name resolution requires that you configure at least one DNS name server on Security Manager. You can configure one or more DNS name servers. Routable domain names are fully qualified domain names (FQDN).  <p>Note This field does accept IP addresses.</p>
Short Name	Short name, if any, for provider name above. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ : . and space.
Port	The port number that Security Manager uses to communicate with Performance Monitor. The default is 443.
Poll Cycle	The number of minutes the firewall device will wait between polling Performance Monitor for new information. The default is 600 seconds (5 minutes). Minimum time is 60 seconds.
Username	The username for logging in to Performance Monitor. Maximum length is 70 characters.
Password	The password for logging in to Performance Monitor. In the Confirm field, enter the password again. Maximum length is 70 characters.

Table A-24 Edit Status Provider Dialog Box (continued)

Element	Description
URN	The uniform resource name for Performance Monitor. URN is the name that identifies the resource on the Internet. URN is part of a URL, for example, /status/StatusServlet. The full URL could be: https://:<server ip>:443/status/StatusServlet where: <ul style="list-style-type: none"> • <server ip> is the IP address of Performance Monitor. • 443 is the port number of Performance Monitor. • /status/StatusServlet is the URN of the Performance Monitor.
Status	Select Enabled from the pull-down menu to specify whether Security Manager needs to poll Performance Monitor for event details and display in the Inventory Status window. Alternatively, choose Disabled for Security Manager to stop polling Performance Monitor.
OK	Saves status provider information.

Take Over User Session Page

A user with administrative privileges can take over the work of another user from the Take Over User session page in non-Workflow mode. This feature 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. For the procedure, see [Taking Over Another User's Work, page 2-96](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Take Over User Session**.

Related Topics

- [Activities and Multiple Users, page 7-5](#)
- [Understanding Activities, page 7-2](#)
- [Understanding Activity States, page 7-5](#)

Field Reference

Table A-25 Take Over User Session Page

Element	Description
User	The usernames of the persons who's session you might take over.
Session State	Displays the state of the activity. See Understanding Activity States, page 7-5 for a list of valid states.
Take over session button	Transfers changes made by the selected user to the currently logged in user. Any changes that have not already been committed are discarded. Note If the selected user is logged in at the time changes are taken over, the user receives a warning message, loses the changes in progress, and then is logged out.

Token Management Page

Security Manager uses FTP to deploy the configuration file to the Token Management System (TMS) server, from which it can be downloaded and encrypted onto an eToken. Security Manager uses the server settings and passwords you provide to connect to the designated TMS server. For the procedure, see [Defining TMS \(Token Management System\) Settings, page 2-97](#).


Note

To use TMS with Cisco IOS routers, you must specify TMS as the transport protocol in the device properties. (This is set by going to Device properties > DCS settings > Transport protocols. See [Working with Device Policies, page 5-54](#).) You must also configure the TMS server as an FTP server, otherwise deployment will fail.

Navigation Path

Select **Tools > Security Manager Administration**, then click **Token Management**.


Related Topics

- [Device Communication Page, page A-10](#)
- [Preparing the Devices for Security Manager to Manage, page 5-2](#)

- [Understanding Deployment Methods, page 18-11](#)

Field Reference

Table A-26 **Token Management Page**

Element	Description
Server Name or IP Address	The hostname or IP address for the TMS server.
Username	Enter the username Security Manager uses to sign on to the TMS server.
Password	Enter the password Security Manager uses to sign on to the TMS server.
Confirm Password	Re-enter the password. This action verifies that this password matches the one entered in the previous field.
Directory in the TMS for Config Files	Enter the directory on the TMS server where deployed configuration files will be downloaded. The “.” character is the default FTP location on the TMS server.
Public Key File Location	<p>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.</p> <p> 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.</p>
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

VPN Policy Defaults Page

The VPN Policy Defaults page has 8 tabs, see [Table A-27](#). The tab you choose depends on the policy type or parameter for which you want to configure the policy defaults. For the procedure to configure VPN policy defaults, see [Configuring VPN Policy Defaults, page 2-98](#).

**Note**

To use this page to set a default VPN policy, you must have previously defined an applicable shared VPN policy.

Navigation Path

Select **Tools > Security Manager Administration**, then click **VPN Policy Defaults**.

Related Topics

- [Configuring VPN Policy Defaults, page 2-98](#)
- [Understanding VPN Default Policies, page 9-12](#)

Field Reference

Table A-27 VPN Policy Defaults Page

Element	Description
Tabs	<p>The VPN Policy Default page in the Security Manager Administration section presents eight tabbed areas. Six of these tabs are for the following VPN technologies:</p> <ul style="list-style-type: none"> • DMVPN • Large Scale DMVPN • Easy VPN • IPsec/GRE • GRE Dynamic IP • Regular IPsec <p>The other two tabs on this page cover default settings for S2S (site-to-site) Endpoints and Remote Access.</p>
DMVPN tab	<p>Lists the six policy types for the DMVPN (Dynamic Multipoint VPN) VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • GRE (DMVPN) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings

Table A-27 VPN Policy Defaults Page (continued)

Element	Description
Large Scale DMVPN tab	<p>Lists the six policy types for the Large Scale DMVPN VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • GRE (Large Scale) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings
Easy VPN tab	<p>Lists the seven policy types for the Easy VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • Client Connection Characteristics • Easy VPN IPsec Proposal • IKE Proposal • PIX7.0/ASA Tunnel Group Policy • Public Key Infrastructure • User Group Policy • VPN Global Settings
IPsec/GRE tab	<p>Lists the six policy types for the IPsec/GRE VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • GRE (GRE Method) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings

Table A-27 VPN Policy Defaults Page (continued)

Element	Description
GRE Dynamic IP tab	Lists the six policy types for the IPsec/GRE VPN technology, and shows the name of the current default policy for each policy type. The types include the following: <ul style="list-style-type: none"> • GRE (Dynamic IP) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings
Regular IPsec tab	Lists the five policy types for regular IPsec VPN technology, and shows the name of the current default policy for each policy type. The types include the following: <ul style="list-style-type: none"> • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings
S2S Endpoints tab	Presents drop-down lists for Internal and External endpoints, each of which you can configure to: <ul style="list-style-type: none"> • All Interfaces • Internal • External
(Policy Type Drop Down List)	Lists the policies that are available to be set as the default policy for each policy type. Until you have created new, shared, VPN policies, only Factory Default is listed.
View Content	Opens the detailed specification page for each VPN policy.
Save button	Saves and applies changes.

Table A-27 VPN Policy Defaults Page (continued)

Element	Description
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets all policy values to Security Manager (factory) defaults.

Workflow Page

Security Manager workflow mode has two main modes:

- Workflow mode (with and without a approvers)
- Non-Workflow mode (default)

The workflow mode you choose depends on your organizational structure and the level of control you wish to have over changes to the network. For the procedure to enable or disable Workflow mode, see [Selecting a Workflow Mode, page 2-56](#).

Navigation Path

Select **Tools > Security Manager Administration**, then click **Workflow**.

Related Topics

- [Managing Activities, page 7-1](#)
- [Managing Deployment, page 18-1](#)

Field Reference



Table A-28 Workflow Page

Element	Description
Workflow Control	
Enable Workflow	Select to enable Workflow mode. When Workflow mode is enabled, you can select whether to have an approver for activities and jobs. See the fields below. For information on the differences between workflow modes, see Working in Workflow Mode, page 2-56 .

Table A-28 Workflow Page (continued)

Element	Description
Require Activity Approval	Automatically selected when you select Enable Workflow. Deselect to disable activity approval. If the check box is selected, an approver is required. A deselected check box means no approver is necessary. For more information about the differences between working with and without an approver, see Activity Approval, page 7-3 .
Require Deployment Approval	Automatically selected when you select Enable Workflow. Deselect to disable deployment job approval. If the check box is selected, an approver is required. A deselected check box means no approver is necessary. For more information about the differences between working with and without an approver, see Understanding Deployment, page 18-1 .
Default Approvers	
Sender Email	Enter the default email address for the person submitting the activity. A standard entry in the Sender field prevents email from not being delivered if the sender does not have the required permission set. For more information, see Submitting an Activity for Approval, page 7-14 .
Activity Approval Email	Enter the default email address for the person responsible for approving activities. Only one approver email can be entered. If necessary, you can replace the default email address with a different one when submitting an activity to an approver. For more information, see Submitting an Activity for Approval, page 7-14 .
Job Approval Email	Enter the default email address for the person responsible for approving deployment jobs. Only one approver email can be entered. If necessary, you can replace the default email address with a different one when submitting an activity to an approver. For more information, please see Submitting Deployment Jobs, page 18-55 .

Table A-28 Workflow Page (continued)

Element	Description
Workflow History	
Keep Activity for (days)	<p>Do one of the following:</p> <ul style="list-style-type: none"> Enter the number of days that activity information is kept in the Activity table. Valid values are 1-180 days. The default is 30 days. <p> Note To keep information longer than the maximum number of days, you need to perform a backup. For more information, see Backup and Restore, page 20-25.</p> <ul style="list-style-type: none"> Click Purge Now to delete all activities older than the number of days specified in the Keep Activity for (days) field.
Keep Job for (days)	<p>Do one of the following:</p> <ul style="list-style-type: none"> Enter the number of days that job deployment information is kept in the Deployment table. Valid values are 1-180 days. The default is 30 days. <p> Note To keep information longer than the maximum number of days, you need to perform a backup. For more information, see Backup and Restore, page 20-25.</p> <ul style="list-style-type: none"> Click Purge Now to delete all jobs greater than the number of days specified in the Keep Job for (days) field.
Save button	Saves your changes to the Security Manager database.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.