



# CHAPTER 1

## Getting Started with Security Manager

---

The following topics describe Cisco Security Manager, how to get started with the application, and how to complete its configuration.

- [Product Overview, page 1-1](#)
- [Using Security Manager - Overview, page 1-7](#)
- [Logging In to and Exiting Security Manager, page 1-12](#)
- [Using the JumpStart, page 1-15](#)
- [Completing the Initial Security Manager Configuration, page 1-15](#)

## Product Overview

Cisco Security Manager (Security Manager) enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of firewall, IPS, and VPN (site-to-site, remote access, and SSL) services across:

- IOS routers.
- PIX and ASA security appliances.
- Catalyst 6500/7600 services modules:
  - FWSM
  - VPNSM

- VPN SPA
- IDSM
- IPS appliances.
- IPS modules:
  - AIP-SSM for ASA security appliances
  - NM-CIDS for Cisco IOS routers
  - AIM-IPS for Cisco IOS routers

**Note**

---

For a complete list of devices and OS versions supported by Security Manager, please refer to [Supported Devices and Software Versions for Cisco Security Manager](#) on Cisco.com.

---

Security Manager also supports provisioning of many platform-specific settings, for example, interfaces, routing, identity, QoS, logging, and so on.

Security Manager efficiently manages a wide range of networks, from small networks consisting of a few devices to large networks with thousands of devices. Scalability is achieved through a rich feature set of shareable objects and policies and device grouping capabilities.

Security Manager supports multiple configuration views optimized around different task flows and use cases.

The following topics provide an overview of Security Manager:

- [Primary Benefits of Cisco Security Manager, page 1-3](#)
- [Security Manager Feature Sets, page 1-5](#)

## Primary Benefits of Cisco Security Manager

Table 1-1 lists the primary benefits of working with Security Manager.

**Table 1-1** Primary Benefits of Security Manager

Benefit	Description
Scalable network management	Centrally administer security policies and device settings for either small networks or large scale networks consisting of thousands of devices. Define policies and settings once and then optionally assign them to individual devices, groups of devices or all the devices in the enterprise.
Provisioning of multiple security technologies across different platforms	Manage VPN, firewall, and IPS technologies on routers, security appliances, Catalyst devices and service modules, and IPS devices.
Provisioning of platform-specific settings and policies	Manage platform-specific settings on specific device types. For example: routing, 802.1x, EzSDD, and Network Admission Control on routers, and device access security, DHCP, AAA, and multicast on firewall devices.
VPN wizard	Quickly and easily configure site-to-site, hub-and-spoke and full-mesh VPNs across different VPN device types.
Multiple management views	Device, policy, and map views enable you to manage your security in the environment that best suits your needs.
Reusable policy objects	Create reusable objects to represent network addresses, device settings, VPN parameters, and so on, then use them instead of manually entering values.
Device grouping capabilities	Create device groups to represent your organizational structure. Manage all devices in the groups concurrently.

**Table 1-1 Primary Benefits of Security Manager (Continued)**

Policy inheritance	Centrally specify which policies are mandatory and enforced lower in the organization. New devices automatically acquire mandatory policies.
Role-based administration	Enable appropriate access controls for different operators.
Workflow	Optionally allow division of responsibility and workload between network operators and security operators and provide a change management approval and tracking mechanism.
Single, consistent user interface for managing common firewall features	Single rule table for all platforms (router, PIX, ASA, and FWSM).
Intelligent analysis of firewall policies	The conflict detection feature analyzes and reports rules that overlap or conflict with other rules. The ACL hit count feature checks in real-time whether specific rules are being hit or triggered by packets.
Sophisticated rule table editing	In-line editing, ability to cut, copy, and paste rules and to change their order in the rule table.
Discover firewall policies from device	Policies that exist on the device can be imported into Security Manager for future management.
Flexible deployment options	Support for deployment of configurations directly to a device or to a configuration file. You can also use Auto-Update Server (AUS), CNS Configuration Engine, or Token Management Server (TMS) for deployment.
Rollback	Ability to roll back to a previous configuration if necessary.
FlexConfig (template manager)	Intelligent CLI configlet editor to manage features available on a device but not natively supported by Security Manager.

# Security Manager Feature Sets

Security Manager provides the following primary feature sets:

- **Firewall Services**

Configuration and management of firewall policies across multiple platforms, including IOS routers, PIX/ASA devices, and Catalyst Firewall Service Modules (FWSM). Features include:

- Access control rules—Permit or deny traffic on interfaces through the use of Access Control Lists.
- Inspection rules—Filter TCP and UDP packets based on application-layer protocol session information.
- AAA/Authentication Proxy rules—Filter traffic based on authentication and authorization for users who log into the network or access the Internet through HTTP, HTTPS, FTP, or Telnet sessions.
- Web filtering rules—Use URL filtering software, such as Websense, to deny access to specific web sites.
- Transparent firewall rules—Enable you to add a transparent firewall device or security appliance to an existing network without having to reconfigure statically defined devices.

For more information, see [Chapter 13, “Managing Firewall Services”](#).

- **Site-to-Site VPN**

Setup and configuration of IPsec site-to-site VPNs. Multiple device types can participate in a single VPN, including IOS routers, PIX/ASA devices, and Catalyst VPN Service Modules. Supported VPN topologies are:

- Point to point
- Hub and spoke
- Full mesh

Supported IPsec technologies are:

- Pure IPsec
- GRE
- GRE Dynamic IP
- DMVPN

- EzVPN

For more information, see [Chapter 10, “Managing Site-to-Site VPNs”](#).

- **Remote Access VPN**

Setup and configuration of IPsec VPNs between servers and mobile remote PCs running Cisco VPN client software. Security Manager supports the EzVPN server feature which allows IOS routers, firewall devices, and Catalyst 6500/7600 devices to act as VPN head-end devices. Security policies defined at the head-end are pushed to the remote VPN device so that minimal configuration is required by the end user.

See [Chapter 11, “Managing Remote Access VPNs”](#) for more information.

- **Intrusion Prevention System (IPS) Management**

Management and configuration of Cisco IPS sensors (appliances, switch modules, and network modules) and IOS IPS devices (Cisco IOS routers with IPS-enabled images and Cisco Integrated Services Routers).

For more information, see [Chapter 18, “Managing IPS Devices”](#) and [Chapter 14, “Managing IPS Services”](#).

- **Features Specific to Firewall Devices (PIX/ASA/FWSM)**

Configuration of advanced platform-specific features and settings on PIX/ASA devices and Catalyst Firewall Service Modules. These features provide added value when managing security profiles and include:

- Device administration settings
- Security
- Routing
- Multicast
- Logging
- NAT
- Bridging
- Failover
- Security contexts

See [Chapter 16, “Managing Firewall Devices”](#) for more information.

- **Features Specific to IOS Routers**

Configuration of advanced platform-specific features and settings on IOS routers. These features provide added value when managing security profiles and include:

- Routing
- NAT
- 802.1x
- NAC
- QoS
- Dialer interfaces
- Secure device provisioning

See [Chapter 15, “Managing Routers”](#) for more information.

- **Features Specific to Catalyst 6500/7600 Devices and Catalyst Switches**

Configuration, discovery, and deployment of VLAN, network connectivity, and service module features and settings on Catalyst 6500/7600 devices and on other Catalyst switches.

See [Chapter 17, “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers”](#) for more information.

- **FlexConfig Template Manager**

An intelligent CLI configlet editor that enables you to provision features that are available on the device but not natively supported by Security Manager. It enables you to manually specify a set of CLI commands and to deploy them to devices using Security Manager’s provisioning mechanisms. These commands can be either prepended or appended to the commands generated by Security Manager to provision security policies.

See [Chapter 20, “Managing FlexConfigs”](#) for more information.

## Using Security Manager - Overview

These topics provide an overview of the different views in which you can work in Security Manager, the basic task flow for defining and deploying policies to devices, and some basic concepts:

- [Configuration Views, page 1-8](#)

- [Task Flow for Configuring Security Policies, page 1-9](#)
- [Policy Overview, page 1-10](#)
- [Workflow Overview, page 1-11](#)

## Configuration Views

Security manager provides three views in which you can manage devices and policies: Device view, Map view and Policy view. You can switch between these views according to your needs.

### Device View

Device view enables you to add devices to the Security Manager inventory and to centrally manage device policies, properties, interfaces, and so on.

This is a device-centric view in which you can see all devices that you are managing and you can select specific devices to view their properties and define their settings and policies.

In Device View, you can define security policies locally on specific devices. You can then share these policies to make them globally available to be assigned to other devices.

For more information, see [Understanding the Device View, page 6-2](#).

### Policy View

Policy view enables you to create and manage reusable policies that can be shared among multiple devices.

This is a policy-centric view in which you can see all the policy types supported by Security Manager. You can select a specific policy type and create, view, or modify shared policies of that type. You can also see the devices to which each shared policy is assigned and change the assignments as required.

For more information, see [Managing Shared Policies in Policy View, page 7-39](#).

### Map View

Map view enables you to create customized, visual topology maps of your network, within which you can view connections between your devices and easily configure VPNs and access control settings.

For more information, see [Chapter 4, “Using Map View”](#).

# Task Flow for Configuring Security Policies

The basic user task flow for configuring security policies on devices involves adding devices to the Security Manager inventory, defining the policies, and then deploying them to the devices. The following briefly describes the steps in a typical user task flow:

---

**Step 1 Prepare devices for management.**

Before you can add a device to the Security Manager device inventory and manage it, you must configure some minimal settings on the device to enable Security Manager to contact it. For more information, see [Chapter 5, “Preparing Devices for Management”](#).

**Step 2 Add devices to the Security Manager device inventory.**

To manage a device with Security Manager, you must first add it to the Security Manager inventory. Security Manager provides multiple methods to add devices: from the network (live devices), from an inventory file exported from CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS), or from a device configuration file. You can also add a device that does not yet exist in the network but which will be deployed in the future, by creating it in Security Manager.

When you add a device, you can also discover its interfaces and certain policies that were already configured on the device. Discovery brings the information into the Security Manager database for continued management with Security Manager in the future.

For more information, see [Chapter 6, “Managing the Device Inventory”](#).

**Step 3 Define security policies.**

After you have added your devices, you can define the security policies you require. You can use Device view to define policies on specific devices. You can use Policy view to create and manage reusable policies that can be shared by any number of devices. When you make a change to a shared policy, the change is applied to all devices to which that policy is assigned.

To simplify and speed up policy definition, you can use policy objects, which are named, reusable representations of specific values. You can define an object once and then reference it in multiple policies instead of having to define the values individually in each policy.



---

**Note** If you are using Workflow mode, you must create an activity before you start defining policies. For more information, see [Workflow Overview](#), page 1-11.

---

For more information, see these topics:

- [Chapter 7, “Managing Policies”](#)
- [Chapter 9, “Managing Objects”](#)

**Step 4 Submit and deploy your policy definitions.**

Policy definition is done within your private view. Your definitions are not committed to the database and cannot be seen by other Security Manager users until you submit them. When you submit your policy definitions, the system validates their integrity. Errors or warnings are displayed to inform you of any problems that need to be addressed before the policies can be deployed to the devices.

Security Manager generates CLI commands according to your policy definitions and enables you to quickly and easily deploy them to your devices. You can deploy directly to live devices in the network (including dynamically addressed devices) through a secure connection, or to files that can be transferred to your devices at any time.

In non-Workflow mode, submitting and deploying your changes can be done in a single action. In Workflow mode, you first submit your activity and then you create a deployment job to deploy your changes.

For more information, see [Chapter 19, “Managing Deployment”](#).

---

## Policy Overview

A policy is a set of rules or parameters that define a particular aspect of network configuration. In Security Manager, you define policies that specify the security functionality you want on your devices. Security Manager translates your policies into CLI commands that can be deployed to the relevant devices.

Security Manager enables you to configure local policies and shared policies. Local policies are confined to the device on which they are configured. Shared policies are named, reusable policies that can be assigned to multiple devices at once. Any changes you make to a shared policy are reflected on all devices to which that policy is assigned, so you do not have to make the change on each device.

For more detailed information, see [Understanding Policies, page 7-1](#).

### **Policy Assignment**

In Security Manager, the application of a policy to a device is called “assignment.” A local policy is automatically assigned to the device on which it is configured. A shared policy can be assigned to multiple devices.

### **Policy Discovery**

Policy discovery enables you to bring policies and settings that already exist on your devices into Security Manager. Policy discovery can be done when you add your device to the Security Manager inventory, or you can initiate policy discovery manually at any time.

### **Policy Objects**

Objects are reusable components that can be referenced by name by multiple policies. An object is a named representation of a set of values. For example, you can define a network object called MyNetwork that contains a set of IP addresses in your network. Whenever you configure a policy requiring these addresses, you can simply refer to the MyNetwork network object rather than manually entering the addresses each time. Furthermore, you can make changes to policy objects in a central location and these changes will be reflected in all the policies that reference those objects.

For more information, see [Chapter 9, “Managing Objects”](#).

## **Workflow Overview**

Security Manager provides two modes of operation that scale to different organizational working environments: Workflow mode and non-Workflow mode.

### Workflow Mode

Workflow mode is for organizations that have division of responsibility between users who define security policies and those who administer security policies. It imposes a formal change-tracking and management system by requiring all policy configuration to be done within the context of an activity. An activity is essentially a private view of the Security Manager database. Changes made within the activity are only committed to the database and made public after the activity has been submitted and then approved by a user with the appropriate permissions. At this stage, the changes can be deployed to the network by creating a deployment job to define the devices to which configurations will be deployed and the deployment method to be used.

### Non-Workflow Mode (Default)

This is the default mode of operation in which there is no need to create activities and jobs. When you log in, Security Manager creates an activity for you. You can define and save your policies, and then submit and deploy them in one step.

For more information, see [Selecting a Workflow Mode, page 1-19](#).

## Logging In to and Exiting Security Manager

Security Manager has two interfaces:

- Cisco Security Management Suite home page—Use this interface to install the Security Manager client and to manage the server. You can also access other CiscoWorks applications you installed, such as Resource Manager Essentials (RME).
- Security Manager client—Use this interface to perform most Security Manager tasks.

These topics describe how to log in to and exit these interfaces:

- [Logging In to the Cisco Security Management Suite Server, page 1-13](#)
- [Logging In to and Exiting the Security Manager Client, page 1-14](#)

## Logging In to the Cisco Security Management Suite Server

Use the Cisco Security Management Suite home page, and CiscoWorks Common Services, to install the Security Manager client and to manage the server. You can also access other CiscoWorks applications you installed, such as RME.

- 
- Step 1** In your web browser, open one of these URLs, where *SecManServer* is the name of the computer where Security Manager is installed. Click **Yes** on any Security Alert windows.
- If you are not using SSL, open `http://SecManServer:1741`
  - If you are using SSL, open `https://SecManServer:443`
- The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser. For information on configuring the browser to run Security Manager, see [Installation Guide for Cisco Security Manager](#).
- Step 2** Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username **admin** and the password defined during product installation.
- Step 3** On the Cisco Security Management Suite home page, you can access at least the following features. Other features might be available depending on how you installed the product.
- Cisco Security Manager Client Installer—Click this item to install the Security Manager client. The client is the main interface for using the product.
  - Server Administration—Click this item to open the CiscoWorks Common Services Server page. CiscoWorks Common Services is the foundation software that manages the server. Use it to configure and manage back-end server features such as server maintenance and troubleshooting, local user definition, and so on.
  - CiscoWorks link (in the upper right of the page)—Click this link to open the CiscoWorks Common Services home page.
- Step 4** To exit the application, click **Logout** in the upper right corner of the screen. If you have both the home page and the Security Manager client open at the same time, exiting the browser connection does not exit the Security Manager client.
-

## Logging In to and Exiting the Security Manager Client

Use the Security Manager client to perform most Security Manager tasks.

### Before You Begin

Install the client on your computer. To install the client, log into the Security Manager server as described in [Logging In to the Cisco Security Management Suite Server, page 1-13](#), and then click **Cisco Security Manager Client Installer** and follow the instructions in the installation wizard.

---

**Step 1** Select **Start > All Programs > Cisco Security Manager Client > Cisco Security Manager Client** to start the client.



#### Tip

If the client was installed on the workstation, but it does not appear in your Start menu, it probably was installed by another user. To make Security Manager Client visible in the Start menu for every user of the client station, copy the Cisco Security Manager Client folder from Documents and Settings\

---

**Step 2** In the Security Manager login window, select the server to which you want to log in, and enter your Security Manager username and password. Click **Login**.

The client logs in to the server and opens the client interface.



#### Tip

The client automatically closes if it is idle for 120 minutes. To change the idle timeout, select **Tools > Security Manager Administration**, select **Customize Desktop** from the table of contents, and enter the desired timeout period. You can also disable the feature so that the client does not close automatically.

---

**Step 3** To exit Security Manager, select **File > Exit**.

---

# Using the JumpStart

The JumpStart is an introduction to Security Manager. It describes and illustrates the major concepts of using the product.

The JumpStart opens automatically when you first launch Security Manager. To get to the JumpStart while you are working with Security Manager, select **Help > JumpStart** from the main menu.

The JumpStart contains the following navigation features:

- A table of contents, which is always visible in the upper right corner. Click an entry to open its page.
- Links in the page enable you to drill down to more detailed information in the JumpStart or to relevant information in the online help.

## Completing the Initial Security Manager Configuration

After you install Security Manager, there are several configuration steps you might want to perform to complete the installation. Although most of the features you initially configure have default settings, you should familiarize yourself with the features and decide if the default settings are the best settings for your organization.

The following list explains the features you might want to initially configure, with pointers to topics that provide more detailed information where appropriate. You can configure these features in any order, or delay configuring those that you do not yet need to use.

- Configure an SMTP server and default e-mail addresses. Security Manager can send e-mail notifications for several actions that occur in the system. For example, you can get an e-mail when your deployment job finishes reconfiguring network devices. For e-mail notifications to work, you must configure an SMTP server.

For information on configuring an SMTP server and setting the default e-mail addresses, see [Configuring an SMTP Server and Default Addresses for E-Mail Notifications](#), page 1-18

- Create user accounts. Users must log into Security Manager to use the product. However, if a user logs in with an account another user is already using, the first user is automatically disconnected. Thus, each user should have a unique account. You can create accounts local to the Security Manager server, or you can use your ACS system to manage user authentication. For more information, see [Chapter 2, “Managing User Accounts”](#)
- Configure default deployment settings. When users deploy configurations to devices, they can select how the configurations should be deployed and how Security Manager should handle anomalies. However, you can select system-default settings that make it easier for users to follow your organization’s recommendations. To set deployment defaults, select **Tools > Security Manager Administration**, and then select **Deployment** from the table of contents to open the Deployment settings page (see [Deployment Page, page A-9](#)).

The following deployment settings are of particular interest:

- **Default Deployment Method**—Whether configuration deployments should be written directly to the device or to a transport server, or if configuration files should be written to a specified directory on the Security Manager server. The default is to deploy configurations directly to the device or transport server, if one is configured for the device. However, if you have your own methods for deploying configuration files, you might want to select File as the default deployment method. For more information on deployment methods, see [Understanding Deployment Methods, page 19-11](#)
  - **When Out-of-Band Changes Detected**—How to respond when Security Manager detects that configuration changes were made on the device through the CLI rather than through Security Manager. The default is to issue a warning and proceed with the deployment, overwriting the changes that were made through the CLI. However, you can change this behavior to simply skip the check for changes (which means Security Manager overwrites the changes but does not warn you), or to cancel the deployment, thus leaving the device in its current state.
  - **Allow Download on Error**—Whether to allow deployment to continue if minor configuration errors are found. The default is to not allow deployment when minor errors are found.
- Select a workflow mode. The default mode is non-Workflow mode. In non-Workflow mode, users have more freedom to create and deploy configurations. However, if your organization requires a more

transaction-oriented approach to network management, where separate individuals perform policy creation, approval, and deployment, you can enable Workflow mode to enforce your procedures. If you are using Workflow mode, ensure that you configure user permissions appropriately when you define user accounts to enforce your required division of labor. For information on the types of workflow you can use, and how to change the mode, see [Selecting a Workflow Mode, page 1-19](#)

- Configure default device communication settings. Security Manager uses the most commonly used methods for accessing devices based on the type of device. For example, Security Manager uses SSH by default when contacting Catalyst switches. If the default protocols work for the majority of your devices, you do not need to change them. For devices that should use a non-default protocol, you can change the protocol in the device properties for the specific devices. However, if you typically use a protocol that is not the Security Manager default (for example, if you use a token management server (TMS) for your routers), you should change the default setting. To change the default communication settings, select **Tools > Security Manager Administration**, and select **Device Communication** from the table of contents. In the Device Connection Settings group, select the most appropriate protocols for each type of device. You can also change the default connection time out and retry settings. For more information about device communication settings, see [Device Communication Page, page A-14](#)
- Configure a Resource Management Essentials (RME) server. Security Manager comes packaged with RME, which you can use to manage the operating systems on your devices. There are a number of shortcut commands to RME from the Tools > Device OS Management menu. To enable these shortcuts, you must configure Security Manager with the location of your RME server. Select **Tools > Security Manager Administration** and select **Device OS Management** from the table of contents. Enter the IP address or DNS name of the RME server. If you installed RME to require SSL connections, select **Connect Using HTTPS**.
- Configure Cisco Performance Monitor servers. If you use Performance Monitor to monitor your devices, you can identify the servers to Security Manager. Users can then view monitoring messages when they view inventory status by selecting **Tools > Inventory Status**. For information on registering Performance Monitor servers with Security Manager, see [Configuring Status Providers, page 1-24](#).

- Configure Cisco Security Monitoring, Analysis and Response System (CS-MARS) servers. If you use CS-MARS for monitoring your network, you can identify the servers to Security Manager and then access CS-MARS information from within Security Manager. For information on registering CS-MARS servers with Security Manager, see [Configuring CS-MARS Servers, page 1-25](#).
- Select the types of router policies you will manage with Security Manager. When you manage FWSM, ASA, PIX, and IPS devices in Security Manager, you automatically manage the entire configuration for these devices. However, with routers, you can select which types of policies are managed by Security Manager. You can manage other parts of the router configuration using other tools (including the router's CLI). By default, all security-related router policies are managed. To change which router policies are managed, select **Tools > Security Manager Administration > Policy Management**. For more information about changing these settings, see [Policy Management Page, page A-40](#). For information about the affects of changing these settings, see [Customizing Policy Management for Routers, page 7-47](#).

## Configuring an SMTP Server and Default Addresses for E-Mail Notifications

Security Manager can send e-mail notifications for several types of events such as deployment job completion, activity approval, or ACL rule expiration. To enable e-mail notifications, you must configure an SMTP server that Security Manager can use for sending the e-mails. Then, you can configure e-mail addresses and notification settings on these settings pages (select **Tools > Security Manager Administration** and select the page from the table of contents):

- Workflow page—For default e-mail addresses and notification settings for deployment jobs and activities. Users can override the defaults when managing deployment jobs and activities.
- Rules Expiration page—For default e-mail addresses and notification settings for ACL rule expiration. Rules expire only if you configure them with expiration dates.
- IPS Updates page—For the e-mail address that should be notified of IPS update availability.

- **Server Security page**—When you configure local user accounts (click **Local User Setup**), specify the user's e-mail address. This address is used as the default target for some notifications such as deployment job completion.

---

**Step 1** Access CiscoWorks Common Services on the Security Manager server:

- If you are currently using the Security Manager client, the easiest way to do this is to select **Tools > Security Manager Administration**, select **Server Security** from the table of contents, and click any button on that page (for example, **Local User Setup**).
- You can use your web browser to log into the home page on the Security Manager server (<https://servername/CSCONm/servlet/login/login.jsp>) and click **Server Administration**.

**Step 2** Click **Server > Admin**, and select **System Preferences** from the table of contents.

**Step 3** On the System Preferences page, enter the host name or IP address of an SMTP server that Security Manager can use. The SMTP server cannot require user authentication for sending e-mail messages.

Also, enter an e-mail address that CiscoWorks can use for sending e-mails. This does not have to be the same e-mail address that you configure for Security Manager to use when sending notifications.

**Step 4** Click **Apply** to save your changes.

---

## Selecting a Workflow Mode

Security Manager has two main workflow modes:

- Workflow mode (with or without approvers).
- Non-Workflow mode (the 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. The following topics help you understand the different workflow modes and how to configure the desired mode:

- [Working in Workflow Mode, page 1-20](#)
- [Working in Non-Workflow Mode, page 1-21](#)

- [Comparing the Two Workflow Modes, page 1-21](#)
- [Changing Workflow Modes, page 1-23](#)

## Working in Workflow Mode

Workflow mode is an advanced mode of operation that imposes a formal change-tracking and change-management system. Workflow mode is suitable for organizations in which there is division of responsibility among security and network operators for defining policies and deploying those policies to devices. For example, a security operator might be responsible for defining security policies on devices, another security operator might be responsible for approving the policy definitions, and a network operator might be responsible for deploying the resulting configurations to a device. This separation of responsibility helps maintain the integrity of deployed device configurations.

You can use Workflow mode with or without an approver. When using Workflow mode with an approver, device management and policy configuration changes performed by one user are reviewed and approved by another user before being deployed to the relevant devices. When using Workflow mode without an approver, device and policy configuration changes can be created and approved by a single user, thus simplifying the change process.

In Workflow mode:

- A user must create an *activity* before defining or changing policy configurations. An activity is essentially a proposal to make configuration changes. The changes made within the activity are applied only after the activity is approved by a user with the appropriate permissions. An activity can either be submitted to another user for review and approval (Workflow mode with an activity approver), or it can be approved by the current user (Workflow mode without an activity approver). For detailed information about the process of creating, submitting, and approving activities, see [Chapter 8, “Managing Activities”](#).
- After the activity is approved, the configuration changes need to be deployed to the relevant devices. To do this, a user must create a *deployment job*. A deployment job defines the devices to which configurations will be deployed, and the deployment method to be used. A deployment job can either be submitted to another user for review and approval (Workflow mode with a deployment job approver), or it can be approved by the current user

(Workflow mode without a job approver). Deployment preferences can be configured with or without job approval. For more information, see [Chapter 19, “Managing Deployment”](#)

## Working in Non-Workflow Mode

Some organizations have no division of responsibility between users when defining and administering their VPN and firewall policies. These organizations can work in non-Workflow mode, which is the default mode of operation. When using non-Workflow mode, there is no need to create activities and jobs. When you log in, Security Manager creates an activity for you. This activity is transparent to the user and does not need to be managed in any way. In addition, when you save and deploy configuration changes, Security Manager creates a job for you as well. Like activities, jobs are transparent and do not need to be managed.

When using non-Workflow mode, multiple users with the same username and password cannot be logged into Security Manager at the same time. If another user logs in with the same username and password while you are working, your session will be terminated and you will have to log in again.

## Comparing the Two Workflow Modes

[Table 1-2](#) highlights the differences between the two workflow modes.

**Table 1-2 Comparison Between Workflow Mode and Non-Workflow Mode**

Question	Non-Workflow Mode	Workflow Mode
What is the default mode for Security Manager?	Default	Not default
How do I know which mode is currently selected?	In Tools > Security Manager Administration > Workflow, the Enable Workflow check box is <i>not</i> selected.	In Tools > Security Manager Administration > Workflow, the Enable Workflow check box <i>is</i> selected.
Must I create activities to make configuration changes?	No. Security Manager automatically creates an activity when you log in.	Yes.

**Table 1-2 Comparison Between Workflow Mode and Non-Workflow Mode (Continued)**

Must I create jobs to deploy configurations to devices?	No. Security Manager creates a deployment job for you when you deploy configuration changes.	Yes.
How do I deploy my configuration changes to the devices?	Do one of the following: <ul style="list-style-type: none"> <li>• Click the <b>Submit and Deploy Changes</b> button in the Main toolbar.</li> <li>• Select <b>File &gt; Submit and Deploy</b>.</li> <li>• Select <b>Tools &gt; Deployment Manager</b> and click <b>Deploy</b> on the Deployment Jobs tab.</li> </ul>	Select <b>Tools &gt; Deployment Manager</b> and create a deployment job.
At what stage are the CLI commands for my configuration changes generated?	When initiating deployment.	When creating a deployment job.
How do I delete my current changes?	Select <b>File &gt; Discard</b> , or if you have already started deploying devices, abort the deployment by selecting the job in the Deployment Manager and clicking <b>Abort</b> .	Select the job in the Deployment Manager and click <b>Discard</b> . If the job has already been deployed, you can abort the job by selecting <b>Abort</b> .
Can multiple users log into Security Manager at the same time?	Yes, but only if each one has a different username. If a user with the same username logs into Security Manager, the first user is automatically logged out.	Yes. Each user can open a different activity and make configuration changes.
What if another user is configuring the devices I want to configure?	You will receive a message indicating that the devices are locked. See <a href="#">Activities and Locking, page 8-4</a> .	You will receive a message indicating that the devices are locked. See <a href="#">Activities and Locking, page 8-4</a> .

## Changing Workflow Modes

You can change the workflow mode that Security Manager enforces if you have the appropriate administrator permissions. Changing the workflow mode has significant effects on users. Before making a change, be sure to understand the following:

- When you change the workflow mode, the change will take effect for all Security Manager users working from the same server.
- Before you can change from Workflow mode to non-Workflow mode, all activities in editable states (Edit, Edit Open, Submit, or Submit Open) must be approved or discarded, and all generated jobs must be deployed, rejected, discarded, or aborted so that the locks on the devices can be released. You do not have to do anything to jobs that are in the failed state.
- If you change from Workflow mode to non-Workflow mode and then restore an earlier version of the database, Security Manager automatically changes to Workflow mode if the restored database has any activities in an editable state (Edit, Edit Open, Submit, or Submit Open). Approve or delete the editable activities, and then turn Workflow mode off again.
- Both Workflow and non-Workflow modes use activities. However, Security Manager hides and automatically manages activities when in non-Workflow mode. Therefore, when changing from non-Workflow mode to Workflow mode, the current hidden activity is then exposed and placed in the Edit\_Open state.

### Related Topics

- [Working in Workflow Mode, page 1-20](#)
- [Working in Non-Workflow Mode, page 1-21](#)
- [Comparing the Two Workflow Modes, page 1-21](#)
- [Chapter 8, “Managing Activities”](#)
- [Chapter 19, “Managing Deployment”](#)

- 
- Step 1** Click **Tools > Security Manager Administration** and select **Workflow** from the table of contents to open the Workflow page (see [Workflow Page, page A-56](#)).
- Step 2** Configure the workflow mode settings in the Workflow Control group. If you select Enable Workflow (to use Workflow mode), you can also select these options:

- **Require Activity Approval**—To enforce explicit approval of activities before policy changes are committed to the database.
  - **Require Deployment Approval**—To enforce explicit approval of deployment jobs before they can be run.
- Step 3** Configure the e-mail notification settings. These are the default e-mail addresses for the e-mail sender (that is, Security Manager), the approvers, and another person or e-mail alias who should be notified when deployment jobs are complete. You also have the options to include the job deployer when sending notifications of job status, and to require that e-mail notifications are sent for deployment job status changes.
- Step 4** Click **Save** to save and apply changes.
- 

## Configuring Status Providers

Users can view status on the devices they can configure by selecting **Tools > Inventory Status**. The status information available depends on the type of status providers you configure.

By default, Security Manager provides status on deployment jobs that affect a device.

In addition to deployment, you can provide status that is obtained from Cisco Performance Monitor, if you use that application (which comes bundled in the Cisco Security Management Suite). As a status provider, Performance Monitor collects the status of events, such as VPN tunnels, device connectivity, and CPU usage threshold, and reports them to Security Manager.

To enable Security Manager to collect status information from your Performance Monitor servers, you must register them with Security Manager. You can add up to five servers. This procedure explains how to register the Performance Monitor servers as status providers.

### Related Topics

- [Viewing Inventory Status, page 6-30](#)
- [Inventory Status Window, page C-49](#)

- 
- Step 1** Click **Tools > Security Manager Administration** and select **Status** from the table of contents to open the Status page (see [Status Page, page A-47](#)).
- Step 2** Click the **Add** button to add a Performance Monitor server. The Add Status Provider dialog box opens (for a detailed explanation of the fields, see [Add or Edit Status Provider Dialog Box, page A-48](#)).
- Step 3** In the Add Status Provider dialog box, the key fields are:
- Provider name, short name—These are the names that will be displayed in Security Manager. They do not need to match anything configured on the device.
  - Server—The IP address or fully-qualified host name of the Performance Monitor server.
  - Username, password, confirm password—A user account that can log into the server.
- You can change the other fields if they are not correct for your setup. Change the polling period if you want it to be more or less frequent.
- Click **OK** when finished, and the provider is added to the provider list.
- Step 4** Click **Save** on the Status page to save your changes.



---

**Tip** You can selectively disable or enable Performance Monitor servers on this page by changing the setting in the Status column. This allows you to temporarily discontinue polling a server for status without deleting its registration.

---

## Configuring CS-MARS Servers

Cisco Security Monitoring, Analysis and Response System (CS-MARS) is a separate application that monitors devices and collects syslog and event information. If you use Security Manager to configure firewall access rules and IPS signatures, you can configure CS-MARS to collect information related to those rules. By registering your CS-MARS servers with Security Manager, users can directly view syslogs and events related to the specific rules on a device when

viewing the device rules in Security Manager. This connection makes it easy for users to identify and analyze the results of Security Manager rules without having to perform an independent query in CS-MARS.

To enable this connection, you must register your CS-MARS servers with Security Manager, and also register the Security Manager server with the CS-MARS servers. Then, when users try to view events for a device, Security Manager automatically identifies the CS-MARS server that is collecting events for the device. If more than one CS-MARS server is collecting events for a device, the user can select which server to use. You can also specify the correct CS-MARS server to use in the device properties for each device.

You must independently configure CS-MARS to collect status from the devices that you configure with Security Manager.

This procedure explains how to register the CS-MARS servers with Security Manager.

- 
- Step 1** Click **Tools > Security Manager Administration** and select **CS-MARS** from the table of contents to open the CS-MARS page (see [CS-MARS Page, page A-4](#)).
- Step 2** Click the **Add** button to add a CS-MARS server. The New CS-MARS Device dialog box opens (for a detailed explanation of the fields, see [New or Edit CS-MARS Device Dialog Box, page A-6](#)).
- Step 3** In the New CS-MARS Device dialog box, enter the IP address or fully-qualified DNS host name of the server, and a username and password for logging into the server.
- Click **Retrieve From Device** to get the server's authentication certificate, and click **Accept** when the certificate is presented to you.
- Click **OK** when finished, and the server is added to the CS-MARS device list.
- Step 4** In the **When Launching CS-MARS** field, select whether you want to prompt users to log into the CS-MARS server when they request event status, or if Security Manager should use the username and password the user used when logging into Security Manager.
- Step 5** Click **Save** on the CS-MARS page to save your changes.
-