



CHAPTER 1

Getting to Know Security Manager

The following topics describe Cisco Security Manager and best practices to getting started quickly and efficiently:

- [What's New in Cisco Security Manager 3.1, page 1-1](#)
- [Product Overview, page 1-4](#)
- [Using Security Manager - Overview, page 1-10](#)
- [Getting Started Checklist, page 1-15](#)
- [Using the JumpStart, page 1-16](#)

What's New in Cisco Security Manager 3.1

- Upgrade from Security Manager 3.0 and 3.0.1.
- Integrated IPS features. While Security Manager 3.0 allowed you to cross-launch the IPS Management Center to access IPS functionality, Security Manager 3.1 provides fully integrated IPS features.
- Native, integrated Catalyst 6500/7600 and VACL management.
- Ability to discover site-to-site and remote access VPNs.
- Ability to discover IOS router configurations.
- High availability.
- Embedded, read-only access to SDM, ASDM, IDM, and IEV for monitoring of individual devices.

- Enhanced reporting features, including device-centric policy report and inventory report.
- Device, interface, and VPN up/down status reported in inventory report.
- Detailed activity report for firewall and IDS devices.
- Ability to configure SSL VPN on IOS and ASA 7.1/7.2 devices.
- Cross-launch of RME SWIM for OS management.
- Ability to use Security Manager user login credentials to connect to devices.
- Ability to use Telnet as a transport protocol to communicate with IOS and Catalyst 6500/7600 devices.
- Enhanced device certificate retrieval support including bulk retrieval through CLIs.
- Support for the following additional features on IOS devices:
 - SSL VPN
 - Additional Easy VPN features
 - Line access
 - SSH configuration
 - Local time
 - Comprehensive AAA support
 - HTTP server
 - PPP
 - DSL/ATM
 - DNS
 - NFP
 - Bridging (wireless)
 - QoS TAC enhancements
 - Authentication proxy enhancements
 - Additional interface settings, such as IP redirect, IP reply, virtual reassembly, and others.
 - Additional firewall features, such as support for IM blocking, java list, DOS settings, and voice service inspection.

- Additional IPsec VPN features, such as large-scale DMVPN, AIM III
- Support for the following additional features on FWSM 3.1:
 - More than one pair of layer 2 interfaces
 - SNMPv2c
 - Skinny video
 - Asymmetric routing
 - FTP authentication challenge
 - Destination NAT for multicast
 - 4K global statements
- Support for the following features on ASA 7.2 devices:
 - Easy VPN HW client parity with PIX 501/506/VPN3002
 - Dual ISP support
 - PPPoE
 - Home/Business VLAN support
 - Enhanced auto-update support
 - Dynamic DNS
 - HA - sub-second failover
 - Virtualization - resource manager
 - Extended usage of DNS domain names
 - Generic input rate limiting
 - MPF-based regular expression classification map
 - N2H2 HTTPS/FTP filtering support
- Support for the following features on FWSM 3.2:
 - L2 NAT/PAT
 - TACACS+ command enhancements
 - Xlate table bypass
 - H323 GUP support
 - Cut through proxy enhancements
 - RTSP PAT

- Support for AIM III (IPsec/SSL VPN)
- Support for IPS 5.1/6.0 and IOS IPS in IOS 12.4(11)Tx
- Support for the following features on IPS 6.0 devices:
 - Virtual sensors
 - Anomaly detection
 - Passive OS fingerprinting
 - Simplified custom signature creation
 - Signature update wizard, preview and tuning of new signatures
 - IPS signature update license management
 - External product interface (linkage of IPS sensor with CSA MC)

Product Overview

Cisco Security Manager (Security Manager) version 3.1 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 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 3.1* 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 through 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 3.1, page 1-5](#)
- [Security Manager Feature Sets, page 1-7](#)

Primary Benefits of Cisco Security Manager 3.1

[Table 1-1](#) lists the primary benefits of working with Security Manager.

Table 1-1 Primary Benefits of Security Manager 3.1

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.

Table 1-1 Primary Benefits of Security Manager 3.1 (continued)

Benefit	Description
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.
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).

Table 1-1 Primary Benefits of Security Manager 3.1 (continued)

Benefit	Description
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 configuration file. 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 websites.
- 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 [Managing Firewall Services, page 12-1](#).

- **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 [Managing Site-to-Site VPNs, page 9-1](#).

- **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 [Managing Remote Access VPNs, page 10-1](#) 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 [Managing IPS Devices](#) and [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 [Managing Firewall Devices, page 15-1](#) 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 [Managing Routers, page 14-1](#) for more information.

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

The embedded CiscoView Device Manager (CVDM) for Catalyst 6500/7600 devices enables the configuration of basic VLAN and network connectivity from within the Security Manager user interface and infrastructure.

See [Chapter 16, “Managing Catalyst Devices”](#) 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 [Managing FlexConfigs, page 19-1](#) 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 taskflow for defining and deploying policies to devices, and some basic concepts:

- [Configuration Views, page 1-10](#)
- [Getting Started Checklist, page 1-15](#)
- [Policy Overview, page 1-13](#)
- [Workflow Overview, page 1-14](#)

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 5-24](#).

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 6-40](#).

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 [Using Map View, page 4-1](#).

User Taskflow

The basic user taskflow 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 taskflow:

Step 1 **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 quickly and easily add devices: from the network (live devices), from the device credential repository (DCR), or from a device configuration file. You can also add a device that does not yet exist in the network but 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 [Managing Devices, page 5-1](#).

Step 2 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 the Workflow mode, you must create an activity before you start defining policies. For more information, see [Workflow Overview, page 1-14](#).

For more information, see [Managing Policies, page 6-1](#) and [Managing Objects, page 8-1](#).

Step 3 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) via 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 is 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 [Managing Deployment, page 18-1](#).

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 6-1](#).

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

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 2-56](#).

Getting Started Checklist

The [Checklist for Getting Started with Cisco Security Manager](#) lists the tasks that typically need to be performed to get up and running with Security Manager. It assumes that you have already installed Security Manager on your server. If you have not yet installed the product, please refer to *Installation Guide of Cisco Security Manager 3.1* for detailed information.



Note

While we recommend performing the steps in the checklist sequentially, some steps might not be relevant to you, depending on your role in the organization.

Table 1-2 **Checklist for Getting Started with Cisco Security Manager**

✓	Task
Step 1	<p>Install the client application on your workstation.</p> <p>Use Cisco Security Manager Suite homepage to install the Security Manager client and to manage the server. You can also access other CiscoWorks applications you installed, such as RME.</p> <p>See Logging In to and Exiting the Security Manager Client, page 3-3.</p>
Step 2	<p>Define application-wide settings that will determine the behavior of certain aspects of the application.</p> <p>There are a few application-wide settings we recommend defining before you begin working with Security Manager, such as the default deployment method (to device or file), the workflow mode, and so on. These settings are located in Tools > Security Manager Administration.</p> <p>See Define These Settings First, page 2-2.</p>
Step 3	<p>Understand how to get to context-sensitive help.</p> <p>Context-sensitive help is available throughout the product. Click the help button on any page or access the entire help system from the Help menu.</p>

✓	Task
Step 4	<p>Familiarize yourself with basics of Security Manager.</p> <p>Understanding the concepts upon which Security Manager is based will help you to get up and running quickly with the product. We recommend you read the section that provides an overview of using Security Manager and that you take a look at the JumpStart that opens when you first open the application.</p> <p>See Using Security Manager - Overview, page 1-10 and Using the JumpStart, page 1-16.</p>
Step 5	<p>Bootstrap your devices so that they can be managed by Security Manager.</p> <p>Before you can manage devices in Security Manager, you must prepare the devices by making sure they are configured with the protocols Security Manager needs to communicate with them, for example, SSH and SSL.</p> <p>See Preparing the Devices for Security Manager to Manage, page 5-2.</p>
Step 6	<p>Add devices to Security Manager inventory.</p> <p>Before you can configure devices, you must add them to the inventory.</p> <p>See Adding Catalyst 6500/7600 Devices from the Network, page 5-33.</p> <p>After adding the devices, you can define your security policies and deploy them to the devices.</p>

Using the JumpStart

The JumpStart is an interactive 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 the 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.