Overview

This chapter contains the following sections:

Introduction to Component Applications

The Security Manager installer enables you to install certain applications and, when you do, requires that you install certain other applications. This section describes those applications and their interdependencies:

Common Services

Common Services 4.2.2 is bundled by default with Security Manager 4.9.

Common Services provides the framework for data storage, login, user role definitions, access privileges, security protocols, and navigation. It also provides the framework for installation, data management, event and message handling, and job and process management. Common Services supplies essential server-side components to Security Manager that include the following:

- SSL libraries
- An embedded SQL database
- The Apache webserver
- The Tomcat servlet engine
- The CiscoWorks home page
- Backup and restore functions

Note Device and Credential Repository (DCR) functionality within Common Services is not supported in Security Manager 4.9. The Groups tab is also removed from the Common Services page in Security Manager 4.9.

Security Manager

Cisco Security Manager is an enterprise-class management application designed to configure firewall, VPN, and intrusion prevention system (IPS) security services on Cisco network and security devices. Cisco Security Manager can be used in networks of all sizes—from small networks to large networks consisting of thousands of devices—by using policy-based management techniques. Cisco Security Manager works in conjunction with the Cisco Security Monitoring, Analysis, and Response System (MARS). Used together, these two products provide a comprehensive security management solution that addresses configuration management, security monitoring, analysis, and mitigation.

Note For more information about Security Manager, visit http://www.cisco.com/go/csmanager. For more information about Cisco Security MARS, visit http://www.cisco.com/go/mars.

To use Security Manager, you must install server *and* client software.

Security Manager offers the following features and capabilities:

- Service-level and device-level provisioning of VPN, firewall, and intrusion prevention systems from one desktop
- Device configuration rollback
- Network visualization in the form of topology maps
- Workflow mode
- Predefined and user-defined FlexConfig service templates
- Integrated inventory, credentials, grouping, and shared policy objects
- Convenient cross-launch access to related applications:
  - When you install the server software, you also install read-only versions of the following device managers: Adaptive Security Device Manager (ASDM), PIX Device Manager (PDM), Security Device Manager (SDM), and IPS Device Manager (IDM)
  - When you install the server software, you also install a cross-launch point to (but not actual installation of) Cisco Prime Security Manager.
  - You can add ASA and PIX devices from Security Manager to Auto Update Server (AUS).
- Integrated monitoring of events generated by ASA and IPS devices. You can selectively monitor, view, and examine events from ASA and IPS devices by using the Event Viewer feature.

Auto Update Server

If you choose to install AUS, you can install it on the same server where you install Security Manager or on a different server, such as a server in your DMZ. AUS and Security Manager can share device inventory information and other data. AUS uses a browser-based user interface and requires Common Services.

AUS enables you to upgrade device configuration files and software images on PIX Security Appliance (PIX) and Adaptive Security Appliance (ASA) devices that use the auto update feature. AUS supports a pull model of configuration that you can use for device configuration, configuration updates, device OS updates, and periodic configuration verification. In addition, supported devices that use dynamic IP addresses in combination with the Auto Update feature can use AUS to upgrade their configuration files and pass device and status information.

AUS increases the scalability of your remote security networks, reduces the costs involved in maintaining a remote security network, and enables you to manage dynamically addressed remote firewalls.

For more information about AUS you can refer to the AUS documentation located at the Security Manager site: http://www.cisco.com/go/csmanager.

Introduction to Related Applications

Other applications are available from Cisco that integrate with Security Manager to provide additional features and benefits:

- **Cisco Security Monitoring Analysis and Response System (MARS)**—Security Manager supports cross linkages between policies and events with MARS for firewall and IPS. Using the Security Manager client you highlight specific firewall rules or IPS signatures and request to see the events related to those rules or signatures. Using MARS you can select firewall or IPS events and request to see the matching rule or signature in Security Manager. These policy-event cross-linkages are especially useful for network connectivity troubleshooting, identifying unused rules, and signature tuning activities. The policy-event cross-linkage feature is explained in detail in the *User Guide for Cisco Security Manager*. For more information about MARS you can visit http://www.cisco.com/go/mars.
- **Cisco Secure Access Control System (ACS)**—You can optionally configure Security Manager to use ACS for authentication and authorization of Security Manager users. ACS supports defining custom user profiles for fine-grained role based authorization control and ability to restrict users to specific sets of devices. For details on configuring Security Manager and ACS integration, see Integrating Security Manager with Cisco Secure ACS, page 8-12. For more information about ACS, visit http://www.cisco.com/go/acs.
- **Cisco Configuration Engine**—Security Manager supports the use of the Cisco Configuration Engine as a mechanism for deploying device configurations. Security Manager deploys the delta configuration file to the Cisco Configuration Engine, where it is stored for later retrieval from the device. Devices such as Cisco IOS routers, PIX Firewalls, and ASA devices that use a Dynamic Host Configuration Protocol (DHCP) server, contact the Cisco Configuration Engine for configuration (and image) updates. You can also use Security Manager with Configuration Engine to manage devices that have static IP addresses. When using static IP addresses, you can discover the device from the network and then deploy configurations through Configuration Engine. For information about the Configuration Engine releases you can use with Security Manager, see the release notes for this version of the product at http://www.cisco.com/c/en/us/support/security/security-manager/products-release-notes-list.html. For more information about the Configuration Engine, visit http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-engine/index.html.

Effect of Enabling Event Management

If you enable Event Management on your Security Manager server, you cannot use that server for the following services:

- Syslog on CiscoWorks Common Services

During the installation or upgrade of Security Manager, the Common Services syslog service port is changed from 514 to 49514. Later, if Security Manager is uninstalled, the port is not reverted to 514. Additional information regarding ports is available in Table 3-1 on page 3-2 and in Table A-1 on page A-2.

If the amount of RAM available to the operating system is insufficient, Event Viewer is disabled (see details in Table 3-3 on page 3-5); however, the Common Services syslog service port is still changed.