Release Notes for Cisco Security Manager 4.10

Originally Published: December 23, 2015

This document contains the following topics:

Introduction

Note Use this document in conjunction with the documents identified in Obtaining Documentation and Submitting a Service Request, page 14. The online versions of the user documentation are also occasionally updated after the initial release. As a result, the information contained in the Cisco Security Manager end-user guides on Cisco.com supersedes any information contained in the context-sensitive help included with the product.

This document contains release note information for the following:

- **Cisco Security Manager 4.10**—Cisco Security Manager enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of firewall, VPN, and IPS services across IOS routers, PIX and ASA security appliances, IPS sensors and modules, Catalyst 6500 and 7600 Series ASA Services Modules (ASA-SM), and several other services modules for Catalyst switches and some routers. (You can find complete device support information

under Cisco Security Manager Compatibility Information 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 device grouping capabilities and objects and policies that can be shared.

- **Auto Update Server 4.10**—The Auto Update Server (AUS) is a tool for upgrading PIX security appliance software images, ASA software images, PIX Device Manager (PDM) images, Adaptive Security Device Manager (ASDM) images, and PIX security appliance and ASA configuration files. Security appliances with dynamic IP addresses that use the auto update feature connect to AUS periodically to upgrade device configuration files and to pass device and status information.

Note Before using Cisco Security Manager 4.10, we recommend that you read this entire document. In addition, it is critical that you read the Important Notes, page 10, the Installation Notes, page 5, and the *Installation Guide for Cisco Security Manager 4.10* before installing Cisco Security Manager 4.10.

Supported Component Versions and Related Software

The Cisco Security Management Suite of applications includes several component applications plus a group of related applications that you can use in conjunction with them. The following table lists the components and related applications, and the versions of those applications that you can use together for this release of the suite. For a description of these applications, see the *Installation Guide for Cisco Security Manager 4.10*.

Note For information on the supported software and hardware that you can manage with Cisco Security Manager, see the *Supported Devices and Software Versions for Cisco Security Manager* online document under Cisco Security Manager Compatibility Information on Cisco.com.

Table 1 Supported Versions for Components and Related Applications

Application	Support Releases
Component Applications	
Cisco Security Manager	4.10
Auto Update Server	4.10
CiscoWorks Common Services	4.2.2
Related Applications	
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	6.0.7, 6.1.1

Table 1 Supported Versions for Components and Related Applications (Continued)

Application	Support Releases
Cisco Secure Access Control Server (ACS) for Windows **Notes** • Cisco Secure ACS Solution Engine 4.1(4) is also supported. • Cisco Secure ACS 5.x is supported for authentication. • You can use other versions of Cisco Secure ACS if you configure them as non-ACS TACACS+ servers. A non-ACS configuration does not provide the granular control possible when you configure the server in ACS mode.	4.2(0), 5.x
Cisco Configuration Engine	3.5, 3.5(1)

What's New

Cisco Security Manager 4.10 SP2

In addition to the resolved caveats, this release provides support for the SNMP Host Group and User List feature. You can now add and edit the host group entries for SNMP users. You can also add a user list containing multiple SNMP users.

Cisco Security Manager 4.10

In addition to resolved caveats, this release includes the following new features and enhancements:

- High-availability on VMware based solutions

You can now install Security Manager in a VMware based High Availability (HA) or Disaster Recovery (DR) environment. Security Manager 4.10 supports the following scenarios:

  - Host-based Failover (Local HA)—In this configuration Security Manager is installed on a virtual machine on an ESXi host within a VMware cluster. In the event of a hardware failure on the existing ESXi host, the host-based failover configuration automatically starts up the same virtual machine (VM) on another host within the VMware cluster.
  - Fault Tolerance—In the VMware Fault Tolerance configuration, when a hardware failure is detected on a host, a second VM is created on a different host and Security Manager starts running on the second VM without an interruption of service. VMware Fault Tolerance enables a new level of guest redundancy. VMware Fault Tolerance implies that two copies of the VM are maintained, each on separate hosts. This feature can be enabled by turning on Fault Tolerance on the VM on which Security Manager has been installed.
  - Disaster Recovery—Security Manager uses the VMware vCenter Site Recovery Manager tool with VMware vSphere Replication for disaster recovery and management. Site Recovery Manager integrates natively with VMware vSphere Replication and supports a broad set of high-performance array-based replication products to reliably copy virtual machines across sites according to business requirements. Site Recovery Manager is an extension to VMware vCenter Server that delivers a disaster recovery solution that helps to plan, test, and run the recovery of virtual machines. Site Recovery Manager can discover and manage replicated datastores, and automate migration of inventory between vCenter Server instances.

Support for ASA 9.5(2) version

- Support for Remote Access VPN in multiple context mode—In the Device View > Remote Access VPN tree, only specific supported policies are displayed for ASA 9.5(2) devices in multiple context mode for the following:
  - Configuration Wizard
  - Connection Profiles
  - Group Policies
  - Global Settings
  - Certificate to Connection Profiles—Policies and Rules
  - SSL VPN—Access and Other Settings
- Support for Carrier Grade NAT in Clustering Devices—Beginning with version 4.10, Security Manager supports Carrier Grade NAT in ASA clustering devices.
- Support for SAML 2.0—Security Manager now enables you to configure Security Assertion Markup Language (SAML) 2.0 based Single Sign-On and Single-Logout for ASA VPN. Single Sign-on Server configuration is no longer supported from ASA version 9.5(2). This has been replaced by SAML Identity Provider.
- Support for 5516 clustering—Security Manager 4.10 supports clustering with ASA 5516 devices.
- Support for Automatic Import of Trust Pool settings—Security Manager now supports automatic import of the Trustpool certificate bundle. The user can specify a URL, which the ASA uses to download and import the bundle. This feature offers users flexibility to schedule and download the the certificate bundle, as per their convenience.
- Support for SCTP Inspection—Security Manager 4.10 supports SCTP inspection on the ASA.You can use the SCTP protocol and port specifications in service objects, access control lists (ACLs) and access rules and inspect SCTP traffic.
- Support for Diameter Inspection—Security Manager 4.10 supports inspect of Diameter traffic, on the ASA.
- Support for DCERPC Inspection improvements—DCERPC Inspection on Security Manager can now filter on DCERPC message universally unique identifiers (UUIDs) to reset or log particular message types. There is a new DCERPC inspection class map for UUID filtering.
- Support for LISP Inspection for inter site flow mobility— The Cisco Locator/ID Separation Protocol (LISP) architecture separates the device architecture from its location into two different numbering spaces, making server migration transparent to clients. Security Manager 4.10 supports LISP inspection on the ASA. The ASA can inspect LISP traffic for location changes and then use this information for seamless clustering operation; the ASA cluster members inspect LISP traffic passing between the first hop router and egress tunnel router (ETR) or ingress tunnel router (ITR), and then change the flow owner to be at the new site.
- PIM BSR Support for multicast routing— Security Manager 4.10 supports PIM Bootstrap Router for multicast routing on the ASA. Until Security Manager 4.10, the ASA supported configuring static rendezvous points (RPs) to route multicast traffic for different groups. Starting from CSM 4.10, the ASA ow supports dynamic RP selection using PIM BSR to support mobility of RPs.
- Private VLAN Support— Currently CSM supports a primary VLAN ID that is used to carry downstream traffic from the router(s) to the host ports.Starting from Security Manager 4.10, you can configure the ASA to map secondary VLANs to a primary VLAN.
- Event Export Enhancement— Currently CSM supports 20000 or 40000 events based on the users' page size. Starting from Security Manager 4.10, the user can export upto 100000 events to event viewer.

- Logging for ASA Standby— Security Manager 4.10 will be able to receive logs from standby ASAs.
- Alerting for Critical Processes— Security Manager 4.10 has the ability to generate email notifications when critical CSM processes go down or are not running.
- ICMPv6 Support— Security Manager 4.10 supports IPv6 addresses for the ICMP policy.

Support for ASA 9.5(1) version

- IPv6 Support for VLAN Mapping—The VLAN mapping feature on the ASA allows for traffic from VPN connections to be directed to a specified VLAN interface. Beginning with Security Manager version 4.10 and ASA 9.5(1), you can assign IPv6 addresses to remote users.

Support for New Device Types

You can now manage the following new device types in Security Manager:

- Support for Cisco Firepower 9000 Series appliances has been added in Security Manager version 4.10. The following devices are supported:
  - FPR9K-SM-24
  - FPR9K-SM-36
- Support for Cisco 1783 Industrial Security Appliance has been added in Security Manager version 4.10.

Other Enhancements in Cisco Security Manager 4.10

- Support for IPv6 values in remote access VPN policies—Security manager now supports IPv6 entries for Unified access Control Lists and Web Type Access Control Lists.
- Support for IPv6 entries in Packet Tracer—Security Manager now supports IPv6 values for the Source and Destination host addresses for the Packet Tracer utility.

Installation Notes

Please refer to the *Installation Guide for Cisco Security Manager 4.10* for specific installation instructions and for important information about client and server requirements. Before installing Cisco Security Manager 4.10, it is critical that you read the notes listed in this section and the Important Notes, page 10.

- The “Licensing” chapter in the installation guide enables you to determine which license you need. (The license you need depends upon whether you are performing a new installation or upgrading from one of several previous versions.) It also describes the various licenses available, such as standard, professional, and evaluation.
- The STD-TO-PRO upgrade converts an ST25 license to a PRO50 license and will result in support for 50 devices. If additional devices need to be supported, you need to buy the necessary incremental licenses.
- Beginning with Version 4.7 of Security Manager, a temporary license for the API is available from Cisco.
- Beginning with Version 4.7 of Security Manager, you can apply incremental licenses to the evaluation version of the Security Manager license.
- Do not modify casuser (the default service account) or directory permissions that are established during the installation of the product. Doing so can lead to problems with your being able to do the following:

  - Logging in to the web server
  - Logging in to the client
  - Performing successful backups of all databases
- Supported operating systems for the server machine are the following:
  - Microsoft Windows Server 2012 R2 Standard—64-bit
  - Microsoft Windows Server 2012 Standard—64-bit
  - Microsoft Windows Server 2012 R2 Datacenter—64-bit
  - Microsoft Windows Server 2012 Datacenter—64-bit
- Supported operating systems for the client machine are the following:
  - Microsoft Windows 7 SP1 Enterprise—64-bit and 32-bit
  - Microsoft Windows 8.1 Enterprise Edition—64-bit and 32-bit
  - Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit
  - Microsoft Windows Server 2012 R2 Standard—64-bit
  - Microsoft Windows Server 2012 Standard—64-bit
  - Microsoft Windows Server 2012 R2 Datacenter—64-bit
  - Microsoft Windows Server 2012 Datacenter—64-bit
- Supported browsers are the following for both the server machine and the client machine:
  - Internet Explorer 8.x, 9.x, 10.x, or 11.x, but only in Compatibility View
  - Firefox 15.0.1 and above supported and recommended
- You can install Security Manager server software directly, or you can upgrade the software on a server where Security Manager is installed. The *Installation Guide for Cisco Security Manager 4.10* explains which previous Security Manager releases are supported for upgrade and provides important information regarding server requirements, server configuration, and post-installation tasks.
- Before you can successfully upgrade to Security Manager 4.10 from a prior version of Security Manager, you must make sure that the Security Manager database does not contain any pending data, in other words, data that has not been committed to the database. If the Security Manager database contains pending data, you must commit or discard all uncommitted changes, then back up your database before you perform the upgrade. The *Installation Guide for Cisco Security Manager 4.10* contains complete instructions on the steps required for preparing the database for upgrade.
- We do not support installation of Security Manager on a server that is running any other web server or database server (for example, IIS or MS-SQL). Doing so might cause unexpected problems that may prevent you from logging into or using Cisco Security Manager.
- Be aware of the following important points before you upgrade:
  - Ensure that all applications that you are upgrading are currently functioning correctly, and that you can create valid backups (that is, the backup process completes without error). If an application is not functioning correctly before an upgrade, the upgrade process might not result in a correctly functioning application.

Note It has come to Cisco's attention that some users make undocumented and unsupported modifications to the system so that the backup process does not back up all installed CiscoWorks applications. The upgrade process documented in the installation guide assumes that you have not subverted the intended functioning of the system. If you are creating backups that back up less than all of the data, you are responsible for ensuring you have all backup data that you require before performing an update. We strongly suggest that you undo these unsupported modifications. Otherwise, you should probably not attempt to do an inline upgrade, where you install the product on the same server as the older version; instead, install the updated applications on a new, clean server and restore your database backups.

- If you log in to a Security Manager server that is running a higher version than your client, a notification will be displayed and you will have the option of downloading the matching client version.
- Beginning with Security Manager 4.4, AUS and the Security Manager client are installed in parallel to improve installation time.
- CiscoWorks Common Services 4.2.2 is installed automatically when you install Security Manager or AUS.
- An error message will pop up if there is any database migration error; this will be at a point where installation can be taken forward without stopping.
- It is recommended to do disk defragmentation for every 50 GB increase in the disk size for optimal performance.

Caution Frequent defragmentation will also contribute to bad sectors, eventually leading to disk failure.

- Beginning with Version 4.4, Security Manager includes a Windows Firewall configuration script in the server installer. This script automates the process of opening and closing the ports necessary for Windows Firewall to work correctly and securely; its purpose is to harden your Security Manager server.

Service Pack 2 Download and Installation Instructions

To download and install Security Manager 4.10 service pack 2, follow these steps:

Note You must install the Cisco Security Manager 4.10 FCS build on your server before you can apply this service pack.

Caution Before installing this service pack, please back up the following files:

MDC\ips\etc\sensorupdate.properties
MDC\eventing\config\communication.properties

If you have previously modified these files, you will need to reconfigure them after installing the service pack.

Step 1 Go to http://www.cisco.com/go/csmanager, and then click **Download Software for this Product** under the Support heading on the right side of the screen.

Step 2 Enter your user name and password to log in to Cisco.com.

Step 3 Click **Security Manager 4.10** in the rightmost column.

Step 4 Click **Security Manager (CSM) Software** and then click **4.10sp2** under **Latest**.

Step 5 Download the file CSM4.10.0Service_Pack2.exe.

Step 6 To install the service pack, close all open applications, including the Cisco Security Manager Client.

Step 7 If Cisco Security Agent is installed on your server, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 8 Run the CSM4.10.0Service_Pack2.exe file that you previously downloaded.

Step 9 In the Install Cisco Security Manager 4.10 Service Pack 2 dialog box, click **Next** and then click **Install** in the next screen.

Step 10 After the updated files have been installed, click **Finish** to complete the installation.

Step 11 On each client machine that is used to connect to the Security Manager server, you must perform the following steps to apply the service pack before you can connect to the server using that client:

a. If Cisco Security Agent is installed on the client, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

b. Launch the Security Manager client.

You will be prompted to “Download Service Pack”.

c. Download the service pack and then launch the downloaded file to apply the service pack.

Step 12 (Optional) Go to the client installation directory and clear the cache, for example, <Client Install Directory>/cache.

Step 13 (Optional) Configure SSL Certificates or self-signed certificates for Open SSL:

a. Stop the CSM Daemon service [net stop crmdmgtd]

b. If you have your own SSL certificates configured, you can reconfigure the certificates as per the steps outlined in the link below:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/user/guide/admin/admin/appendixcli.html#wp1016314

c. For self-signed certificates, from the command prompt navigate to the <CSCOpx>\MDC\Apache directory, and then execute the gencert.bat file.
(where <CSCOpx> is your installation directory)

d. Start the CSM Daemon service [net start crmdmgtd]

Service Pack 1 Download and Installation Instructions

To download and install Security Manager 4.10 service pack 1, follow these steps:

Note You must install the Cisco Security Manager 4.10 FCS build on your server before you can apply this service pack.

Caution Before installing this service pack, please back up the following files:

MDC\ips\etc\sensorupdate.properties
MDC\eventing\config\communication.properties

If you have previously modified these files, you will need to reconfigure them after installing the service pack.

Step 1 Go to http://www.cisco.com/go/csmanager, and then click **Download Software for this Product** under the Support heading on the right side of the screen.

Step 2 Enter your user name and password to log in to Cisco.com.

Step 3 Click **Security Manager 4.10** in the rightmost column.

Step 4 Click **Security Manager (CSM) Software** and then click **4.10sp1** under **Latest**.

Step 5 Download the file CSM4.10.0Service_Pack1.exe.

Step 6 To install the service pack, close all open applications, including the Cisco Security Manager Client.

Step 7 If Cisco Security Agent is installed on your server, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 8 Run the CSM4.10.0Service_Pack1.exe file that you previously downloaded.

Step 9 In the Install Cisco Security Manager 4.10 Service Pack 1 dialog box, click **Next** and then click **Install** in the next screen.

Step 10 After the updated files have been installed, click **Finish** to complete the installation.

Step 11 On each client machine that is used to connect to the Security Manager server, you must perform the following steps to apply the service pack before you can connect to the server using that client:

a. If Cisco Security Agent is installed on the client, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

b. Launch the Security Manager client.

You will be prompted to “Download Service Pack”.

c. Download the service pack and then launch the downloaded file to apply the service pack.

Step 12 (Optional) Go to the client installation directory and clear the cache, for example, <Client Install Directory>/cache.

Step 13 (Optional) Configure SSL Certificates or self-signed certificates for Open SSL:

a. Stop the CSM Daemon service [net stop crmdmgtd]

b. If you have your own SSL certificates configured, you can reconfigure the certificates as per the steps outlined in the link below:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/user/guide/admin/admin/appendixcli.html#wp1016314

c. For self-signed certificates, from the command prompt navigate to the <CSCOpx>\MDC\Apache directory, and then execute the gencert.bat file.
(where <CSCOpx> is your installation directory)

d. Start the CSM Daemon service [net start crmdmgtd]

Important Notes

The following notes apply to the Security Manager 4.10 release:

- In Policy Object Manager > Access Control List > Unified ACL, if you right-click the ACL which is used in any of the device configuration and select “Find Usage”, the Find Usage option does not show the list of devices that are configured with the Unified Access List.
- Beginning with version 4.9, Security Manager does not support the Secure Sockets Layer version 3.0 (SSLv3) security protocol.
- Security Manager sends only the delta configuration to the Configuration Engine, where the particular device retrieves it. The full configuration is not pushed to the device. Therefore, the following behaviors are encountered for OSPF, VLAN, and failover for devices.
  - OSPF for IOS routers—Security Manager supports OSPF policy for routers running the IOS Software version 12.2 and later. However, Security Manager does not support OSPF policy for Catalyst devices. Therefore when you configure the OSPF policy in a Catalyst device and perform the discovery in Security Manager, the latter removes the ‘no passive-interface <*interface number*>’ command from the full configuration. Therefore you will see a difference in the Security Manager-generated configuration and the configuration on the device.
  - VLAN—Security Manager supports discovery of VLAN command in IOS devices but does not support dynamic behavior of the VLAN command. If there are user driven changes in VLAN policy, Security Manager generates the command in delta and full configuration. In other words, in normal preview or deployment, Security Manager does not generate VLAN command in full configuration. Therefore you will see a difference in the Security Manager-generated configuration and the configuration on the device.
  - Failover policy for firewall devices, such as ASA and FWSM, and IOS devices—Security Manager does not support dynamic behavior of failover devices. That is, the primary unit in HA has ‘failover lan unit primary’ command and secondary unit has ‘failover lan unit secondary’ command. When there is a switchover, Security Manager tries to compare with the ‘failover lan unit primary’ and generates the delta configuration. This leads to a failure in deployment.

    Note Security Manager does not support ‘dynamic’ CLI commands. If the syntax of a CLI command is modified, for example, the ‘primary’ keyword is changed to ‘secondary’; it will not be supported by Security Manager.

- The following ASA policies are newly supported in Security Manager 4.8:
  - SSL
  - EIGRP

Therefore these policies are managed by default in a fresh 4.8 installation. However, if you are upgrading Security Manager from version 4.7 to 4.8, or from version 4.7 to 4.9, by default the said policies will be unmanaged for both inline and remotely upgraded servers.

If you are upgrading from Security Manager 4.7 to 4.9, in addition to the SSL and EIGRP ASA policies, the following ASA policies will also be unmanaged:

- Route-Map
- CLI Prompt
- Virtual Access
- AAA Exec Authorization

If you have a device that uses commands that were unsupported in previous versions of Security Manager, these commands are not automatically populated into Security Manager as part of the upgrade to this version of Security Manager. If you deploy back to the device, these commands are removed from the device because they are not part of the target policies configured in Security Manager. We recommend that you set the correct values for the newly added attributes in Security Manager so that the next deployment will correctly provision these commands. You can also rediscover the platform settings from the device; however, you will need to take necessary steps to save and restore any shared Security Manager policies that are assigned to the device.

Note If a route-map is configured on the ASA and the same route-map is used in OSPF policy, after upgrading to Security Manager 4.9 from Security Manager 4.7, the OSPF page will show a red-banner. To overcome this issue, you must rediscover the ASA.

- If you upgrade an ASA managed by Security Manager to release 8.3(x) or higher from 8.2(x) or lower, you must rediscover the NAT policies using the NAT Rediscovery option (right-click on the device, select Discover Policies on Device(s), and then select NAT Policies as the only policy type to discover). This option will update the Security Manager configuration so that it matches the device configuration while preserving any existing shared policies, inheritance, flex-configs, and so on.

  When upgrading an ASA device from 8.4.x to 9.0.1, the device policies will be converted to the unified format. You can rediscover the unified NAT rules using the NAT Rediscovery option or you can convert the existing NAT policies to unified NAT policies with the help of the rule converter in Security Manager. For more information, see http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-6/user/guide/CSMUserGuide/porules.html#pgfId-161507 or the “Converting IPv4 Rules to Unified Rules” topic in the online help.

  You can also use the rule converter for the other firewall rules like access rules, AAA rules, and inspection rules if you want to manage these policies in unified firewall rules format.
- If you upgrade a device that you are already managing in Security Manager from 8.x to 9.0(1) or higher, you must rediscover the device inventory so that Security Manager starts interpreting the device as a 9.x device and then you must rediscover the policies on the device to ensure that Security Manager looks for and discovers the appropriate policy types. Alternatively, you can delete the device from Security Manager and then add the device again.
- If you perform one of the following upgrades to a device that you are already managing in Security Manager:

  —from 7.x to 8.x

  —from any lower version to 8.3(1) or higher

—from 8.3(x) to 8.4(2) or higher

you must rediscover the device in Security Manager. This is required due to significant policy changes between the two releases.

For detailed information on these scenarios, refer to the section titled "Validating a Proposed Image Update on a Device" in the *User Guide for Cisco Security Manager 4.10* at the following URL:

http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html

- ASA 8.3 ACLs use the real IP address of a device, rather than the translated (NAT) address. During upgrade, rules are converted to use the real IP address. All other device types, and older ASA versions, used the NAT address in ACLs.
- The device memory requirements for ASA 8.3 are higher than for older ASA releases. Ensure that the device meets the minimum memory requirement, as explained in the ASA documentation, before upgrade. Security Manager blocks deployment to devices that do not meet the minimum requirement.
- For ASA devices in cluster mode, Security Manager treats the entire cluster as a single node and manages the cluster using the main cluster IP address. The main cluster IP address is a fixed address for the cluster that always belongs to the current master unit. If the master node changes, the SNMP engine ID for the cluster also changes. In such a case, Security Manager will regenerate the CLI for all SNMP Server Users that are configured with a Clear Text password. Security Manager will not regenerate the CLI for users that are configured using an Encrypted password.

  You can use the Get SNMP Engine ID button on the SNMP page to retrieve the engine ID from the device currently functioning as the cluster master unit.
- You cannot use Security Manager to manage an IOS or ASA 8.3+ device if you enable password encryption using the **password encryption aes** command. You must turn off password encryption before you can add the device to the Security Manager inventory.
- Device and Credential Repository (DCR) functionality within Common Services is not supported in Security Manager 4.8.
- LACP configuration is not supported for the IPS 4500 device series.
- A Cisco Services for IPS service license is required for the installation of signature updates on IPS 5.x+ appliances, Catalyst and ASA service modules, and router network modules.
- Do not connect to the database directly, because doing so can cause performance reductions and unexpected system behavior.
- Do not run SQL queries against the database.
- If an online help page displays blank in your browser view, refresh the browser.
- Security Manager 4.9 only supports Cisco Secure ACS 5.x for authentication. ACS 4.1(3), 4.1(4), or 4.2(0) is required for authentication and authorization.
- If you do not manage IPS devices, consider taking the following performance tuning step. In *$NMSROOT*\MDC\ips\etc\sensorupdate.properties, change the value of packageMonitorInterval from its initial default value of 30,000 milliseconds to a less-frequent value of 600,000 milliseconds. Taking this step will improve performance somewhat. [*$NMSROOT* is the full pathname of the Common Services installation directory (the default is C:\Program Files (x86)\CSCOpx).]
- The IPS packages included with Security Manager do not include the package files that are required for updating IPS devices. You must download IPS packages from Cisco.com or your local update server before you can apply any updates. The downloaded versions include all required package files and replace the partial files that are included in the Security Manager initial installation.

- The “License Management” link on the CiscoWorks Common Services home page has been removed.
- CsmReportServer and CsmHPMServer are now supported with 64-bit JRE.
- The “rsh” service has been changed to manual start mode. You can start it manually if you need it.

Caveats

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats

All open bugs severity 3 and higher for version 4.10 are included in the following search:

- Open caveats—Release 4.10
- Open caveats—Releases prior to 4.10

Resolved Caveats

All resolved caveats for each version are included in the following searches:

- Resolved caveats—Release 4.10 Service Pack 2
- Resolved caveats—Release 4.10 Service Pack 1
- Resolved caveats—Release 4.10
- Resolved caveats—Releases prior to 4.9

  For the list of caveats resolved in releases prior to this one, see the following documents:

  http://www.cisco.com/c/en/us/support/security/security-manager/products-release-notes-list.html

Where to Go Next

If you want to:	Do this:
Install Security Manager server or client software.	See *Installation Guide for Cisco Security Manager 4.10*.
Understand the basics.	See the interactive JumpStart guide that opens automatically when you start Security Manager.

If you want to:	Do this:
Get up and running with the product quickly.	See "Getting Started with Security Manager" in the online help, or see Chapter 1 of User Guide for Cisco Security Manager 4.10.
Complete the product configuration.	See "Completing the Initial Security Manager Configuration" in the online help, or see Chapter 1 of User Guide for Cisco Security Manager 4.10.
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 7 of *Installation Guide for Cisco Security Manager 4.10*. • Setting Up User Permissions • Integrating Security Manager with Cisco Secure ACS
Bootstrap your devices.	See "Preparing Devices for Management" in the online help, or see Chapter 2 of User Guide for Cisco Security Manager 4.10.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation and Submitting a Service Request" section.