Release Notes for Cisco Security Manager 4.22

First Published: 2020-11-10

Last Modified: 2021-01-25

Introduction

This document contains the following topics:

Note Use this document in conjunction with the documents identified in Communications, Services, and Additional Information. 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 4.22**—Cisco Security Manager enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of firewall, VPN, ASA security appliances, and several other services modules. (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.

Note From version 4.21 onwards, Cisco Security Manager terminates whole support, including support for any bug fixes or enhancements, for all Aggregation Service Routers, Integrated Service Routers, Embedded Service Routers, and any device operating on Cisco IOS software, including the following devices:

- Cisco Catalyst 6500 and 7600 Series Firewall Services Modules (EOL8184)
- Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (EOL8843)
- Cisco Intrusion Prevention System: IPS 4200, 4300, and 4500 Series Sensors (EOL9916)
- Cisco SR 500 Series Secure Routers (EOL7687 , EOL7657)
- PIX Firewalls (EOL)
- Cisco IOS devices

- **Auto Update Server 4.22**—The Auto Update Server (AUS) is a tool for upgrading ASA software images, Adaptive Security Device Manager (ASDM) images, 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 4.22, we recommend that you read this entire document. In addition, it is critical that you read the Important Notes, on page 8, the Installation Notes, on page 4, and the *Installation Guide for Cisco Security Manager 4.22* before installing Cisco Security Manager 4.22.

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 4.22*.

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	4.22
Auto Update Server	4.22

Application	Support Releases
CiscoWorks Common Services	4.2.2
Related Applications	
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	6.0.7, 6.1.1
Cisco Configuration Engine	3.5, 3.5(1)

Note Beginning with version 4.21, Cisco Security Manager supports only TACACS+ authentication via Cisco Identity Services Engine (ISE), because ACS has reached its end of life.

What's New

Cisco Security Manager 4.22 Service Pack 1

This release includes bug fixes. Refer Resolved Caveats, on page 13 for more information.

Cisco Security Manager 4.22

This release includes the following new features and enhancements:

Support for ASA 9.15 (1) version

- **Support for AnyConnect Web Security WSO**— For using Web Security AnyConnect Profile type, Cisco Security Manager earlier allowed uploading only WSP files. From Cisco Security Manager 4.22, you can directly upload WSO files by selecting the new **Web Security WSO** AnyConnect Profile type.
- **Support for Host Scan 4.6 and higher versions**—Beginning with version 4.22, Cisco Security Manager supports Host Scan versions 4.6 and above. In addition, support for new Anti-Malware (am) and Personal Firewall (pfw) through Host Scan has been added, whereas support for existing Anti-Virus (av), Anti-Spyware (as), and Firewall (fw) has been removed. Refer Important Notes, on page 8 for more information.
- **ASDM Banner Enhancement**—Cisco Security Manager lets you configure banners to specify Session (exec), Login, and Message-of-the-Day (motd). Beginning with version 4.22, Security Manager supports the new **ASDM Banner** that can be configured along with the existing banners.
- **Deprecation of IKEv1 ciphers**—Beginning with version 4.22, Cisco Security Manager terminates support for MD5 hash algorithm, and DES and 3DES encryption algorithms, for IKEv1 as they are no longer secure against modern threats.
- **Deprecation of IKEv2 ciphers**—From version 4.22 onwards, Cisco Security Manager terminates support for MD5 integrity algorithm and MD5 PRF algorithm. In addition, DES, 3DES, and NULL encryption algorithms for IKEv2 are no longer supported, because these algorithms are considered less secure.
- **Deprecation of IPsec ciphers**—Beginning with version 4.22, Cisco Security Manager does not support the following IPsec ciphers that are less secure:

  - DES and 3DES ESP encryption algorithms for IKEv1
  - MD5 ESP hash algorithm for IKEv1 and IKEv2
  - DES, 3DES, AES-GMAC, AES-GMAC-192, and AES-GMAC-256 for IKEv2

- **Deprecation of DH groups 2 and 24**—Cisco Security Manager supports numerous DH group algorithms in various policies. DH groups determine the strength of the key used in the key exchange process. However, from Cisco Security Manager 4.22 onwards, DH groups 2 and 24, considered to be less secure, are no longer supported for IKEv2, for ASA 9.15(1) or higher devices.
- **Deprecation of DH group 2**—Beginning with version 4.22, Cisco Security Manager does not support DH group 2 for IKEv1, for ASA 9.15(1) and higher devices.
- **Transcipt Purging Enhancement**—Beginning with version 4.22, Cisco Security Manager purges the deployment transcript files older than the number of days specified, from the **<NMSROOT>\MDC\tomcat\vms\athena\transcript** folder also. This helps eradicate stale entries getting piled up.
- **Snapshot Purging Enhancement**—From Cisco Security Manager 4.22 onwards, **Snapshot Purge Settings** is introduced under **Deployment Page**. Note that for purging, Security Manager considers only the debugging files that got created after the **Capture Discovery/Deployment Debugging Snapshots to File** checkbox in the **Debug Options** page is enabled.

Installation Notes

Please refer to the *Installation Guide for Cisco Security Manager 4.22* for specific installation instructions and for important information about client and server requirements. Before installing Cisco Security Manager 4.22, it is critical that you read the notes listed in this section and the Important Notes, on page 8.

- 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 2016 Standard— 64-bit

  - Microsoft Windows Server 2016 Datacenter—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 operating systems for the client machine are the following:
  - Microsoft Windows 7
  - Microsoft Windows 8.1 Enterprise Edition—64-bit and 32-bit
  - Microsoft Windows 10 —64-bit and 32-bit
  - Microsoft Windows Server 2016 Standard— 64-bit
  - Microsoft Windows Server 2016 Datacenter— 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 4.22 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 4.22 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 4.22* 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.

- Inline upgrades are not supported for Cisco Security Manager 4.12 SP2. If you are upgrading from 4.12SP2 to 4.13 or 4.14, follow the remote upgrade procedure and refer to the steps given in "Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2" section of the *Installation Guide for Cisco Security Manager 4.22* to resolve the database migration issues.

Note This exception is not applicable if you are upgrading from Cisco Security Manager 4.12.

- 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 4.12, 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 1 Download and Installation Instructions

To download and install Security Manager 4.22 Service Pack 1, follow these steps:

Note You must install the Cisco Security Manager 4.22 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
MDC\athena\config\CSM.properties
MDC\athena\config\DCS.properties
```

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

Important When configuring values in Security Manager property files, ensure you modify only the required values in the file. Copying the whole content from an already-existing property file and appending it to a new property file creates duplicate entries in the same file and might result in deployment failures.

Procedure

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 4.22** in the rightmost column.

Step 4 Click Security Manager (CSM) Software and then click **4.22sp1** under **Latest**.

Step 5 Download the file CSM4.22.0Service_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 CSM4.22.0Service_Pack1.exe file that you previously downloaded.

Step 9 In the **Install Cisco Security Manager 4.22 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].

Installing Client Patch on Re-installed CSM 4.22 SP1 Machine

If you are installing the CSM 4.22 SP1 for the first time, the client patch is also installed automatically. However, if you are re-installing CSM 4.22 SP1, you must manually install client patch on the machine:

1. After CSM 4.22 SP1 is re-installed successfully, go to CSM installed directory {NMSROOT}/MDC/tomcat/VMS/desktop.
2. Double-click the CSMClient4.22.0Patch1.exe file and follow the procedure to install the client patch.
3. If you have multiple clients in separate machines, copy the CSMClient4.22.0Patch1.exe file to that machine and install the CSM 4.22 SP1 client patch on it.

Important Notes

The following notes apply to the Security Manager 4.22 release:

- You can upgrade from Host Scan version 4.3 to any higher versions. However, when directly upgrading from Host Scan 4.3 to 4.6 or higher versions, as the attributes Anti-Virus (AV), Anti-Spyware (AS), and Firewall (FW) are not supported, there are certain manual actions required for all the devices. Follow the steps below for each device:
  - Create a backup of **dap.xml, data.xml**, and **data-record.txt files** in the HostScan_Migration_Backup directory on Adaptive Security Appliance.
  - Navigate to **RAVPN** > **Dynamic Access Policy** > **Enable Hostscan** and select the intended Host Scan package from the list of packages.
  - Now, navigate to any policy and come back to Dynamic Access Policy. This ensures all the attributes are loaded properly.
  - Manually delete the Anti-Virus (AV), Anti-Spyware (AS), and Firewall (FW) attributes and LUA scripts, if any.
  - Create a Dynamic Access Policy using the new attributes Anti-Malware (AM) and Personal Firewall (PFW).
  - Deploy the changes into the device.

For more information, refer *User Guide for Cisco Security Manager 4.22*.

- The following patches are required to run the critical Cisco Security Manager services on the Microsoft Windows Server 2012 R2. Failing to install the patches will bring down the services. Ensure that you have these patches installed on your server, else install the patches in the following order:

  1. KB2919442
  2. Run the clearcompressionflag.exe

  

  Note The clearcompressionflag.exe file is part of the cumulative set of security updates. This tool prepares the computer for the Windows Updates in the background. The executable file can be downloaded from the Microsoft site: https://support.microsoft.com/en-in/kb/2919355.

  3. KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, and KB2934018
  4. KB2999226

You can also install these patches after installing the Cisco Security Manager to bring up the critical services. To register the services with the windows services, you must run the "RegisterApache.bat" script which is located in "<CSMInstalledDirectory>\CSCOpx\bin", and then restart the server.

- For remote access VPN in multi-context ASA devices running the software version 9.6(2) or later, the device modifies the storage-url configured with flash:/ directory into disk0:/. Since the device modifies the configuration, Security Manager negates the device configuration and pushes the configuration into the device again. This is a limitation of Security Manager version 4.12.
- 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.
- Cisco Security Manager was using OpenSSL for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. Beginning with version 4.13, Cisco Security Manager replaced OpenSSL version 1.0.2 with Cisco SSL version 6.x. Cisco SSL enables FIPS compliance over full FIPS Validation which results in fast and cost-effective connectivity. The Common Criteria mode in Cisco SSL allows easier compliance. Cisco SSL is feature-forward when compared to OpenSSL. The product Security Baseline (PSB) requirements for CiscoSSL ensures important security aspects such as credential and key management, cryptography standards, anti-spoofing capabilities, integrity and tamper protection, and session, data, and stream management and administration are taken care of. In version 4.17, the SSL 1.0.2N is being used.
- 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.
  - 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.

Note From version 4.21 onwards, Cisco Security Manager does not support IOS routers.

- 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 supported in Security Manager version 4.8 and higher:
  - — SSL
  - — EIGRP

Therefore these policies are managed by default in a fresh 4.8 version, or higher, 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.

- You can also create the Unified ACL object on-the-fly in certain Remote Access VPN policies, such as the Dynamic Access Policy. However, when you create the Unified ACL object on-the-fly, Cisco Security

Manager displays an error message. You must add again the created ACL in the Selector window and save the policy.

- If PKI specification is chosen for IKEv2 authentication in Site to Site VPN, created using S2S manager and if a trustpoint is chosen for PKI specification. Then the corresponding Trustpoint should be selected in: Remote Access VPN > Public Key Infrastructure also.
- 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 the User Guide for Cisco Security Manager 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 4.22* 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.

- The Rollback feature is not supported with ASA clusters. Hence, do not attempt to rollback ASA cluster configurations.
- Device and Credential Repository (DCR) functionality within Common Services is not supported in Security Manager 4.8 and later versions.
- 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.
- Up to version 4.20, Security Manager used SQL Anywhere version 12.x as the database. Beginning with version 4.21, Security Manager uses Sybase SQL Anywhere version 17.0.10.5855.
- Do not run SQL queries against the database.
- If an online help page displays blank in your browser view, refresh the browser.
- 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.
- From Cisco Security Manager 4.4, 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.
- To be PCI compliant, in Cisco Security Manager 4.15 and 4.16, TLS 1.0 and TLS 1.1 were disabled respectively. Hence from 4.16, Cisco Security Manager was using only TLS 1.2 version. However, the ISE 1.3 server and its lower versions does not support TLS 1.2. This impacts the legacy ISE settings with Cisco Security Manager from release 4.15. This incompatibility prevents integration of ISE server with Cisco Security Manager. If you are required to integrate ISE 1.3 and lower versions with Cisco Security Manager successfully, refer “Resolving errors while integrating ISE server with Cisco Security Manager” section in User Guide for Cisco Security Manager 4.19.
- Beginning with version 4.19, Cisco Security Manager does not support the device SSL Certificates using DES algorithms. If the device SSL uses DES algorithms, Security Manager throws up an error when you try to add the device. This happens because the JRE, by default, disables the DES algorithms due to security vulnerability.

- From version 4.21 onwards, Cisco Security Manager terminates whole support, including support for any bug fixes or enhancements, for all Aggregation Service Routers, Integrated Service Routers, Embedded Service Routers, and any device operating on Cisco IOS software.
- Beginning with version 4.21, Cisco Security Manager supports cross-launch of ASDM for ASA 9.14(1) and earlier devices. However, to avail this feature, ensure the CLI **http server basic-auth-client Java** is configured manually in ASA.

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

The following link provides details on the open bugs on this release and releases prior to this release:

- Open Caveats—Release 4.22 Service Pack 1
- Open Caveats—Releases Prior to 4.22
- Open Caveats—Releases 4.22 (Severity 3 or higher)
- Open Caveats—Releases 4.22 (Severity 4 or higher)

4.23 open caveats

- Open Caveats—Release Prior to 4.23Open Caveats—Releases Prior to 4.22
- Open Caveats—Release 4.23Open Caveats—Releases 4.22 (Severity 3 or higher)
- Open Caveats—Release 4.23Open Caveats—Releases 4.22 (Severity 4 or higher)

Resolved Caveats

- Resolved caveats—Release 4.22 Service Pack 1
- Resolved caveats—Release 4.22

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

- Resolved Caveats—Release 4.23 Resolved caveats—Release 4.22

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

Where to Go Next

Note The links in the following table pertain to Cisco Security Manager version 4.21 and earlier.

If you want to:	Do this:
Install Security Manager server or client software.	See Installation Guide for Cisco Security Manager.
Understand the basics.	See the interactive JumpStart guide that opens automatically when you start Security Manager.
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.
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.
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 7 of Installation Guide for Cisco Security Manager. • 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.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

This document is to be used in conjunction with the documents listed in the Communications, Services, and Additional Information section.