Release Notes for Cisco Security Manager 4.13

Originally Published: February 16, 2017

This document contains the following topics:

Introduction

Note Use this document in conjunction with the documents identified in Communications, Services, and Additional Information, page 12. 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 4.13**—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 4.13**—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 4.13, we recommend that you read this entire document. In addition, it is critical that you read the Important Notes, page 7, the Installation Notes, page 5, and the *Installation Guide for Cisco Security Manager 4.13* before installing Cisco Security Manager 4.13.

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 4.13*.

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	4.13
Auto Update Server	4.13
CiscoWorks Common Services	4.2.2
Related Applications	
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	6.0.7, 6.1.1
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 4.13

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

Support for ASA 9.7(1) version

- **MTP3 User Adaptation (M3UA) inspection Phase 2 Support** — With Cisco Security Manager 4.12, you could inspect M3UA traffic and also apply actions based on point code, service indicator, and message class and type. Starting from Cisco Security Manager 4.13, the M3UA policy-map supports additional CLI for Timeout session, Message tags and ASP state validations parameters.
- **Integrated Routing and Bridging Support** — Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. A bridge group is a group of interfaces that the ASA bridges instead of routes. The ASA is not a true bridge in that the ASA continues to act as a firewall: access control between interfaces is controlled, and all of the usual firewall checks are in place. Previously, you could only configure bridge groups in transparent firewall mode, where you cannot route between bridge groups. This feature lets you configure bridge groups in routed firewall mode, and to route between bridge groups and between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group. Integrated Routing and Bridging provides an alternative to using an external Layer 2 switch if you have extra interfaces on the ASA to assign to the bridge group. In routed mode, the BVI can be a named interface and can participate separately from member interfaces in some features, such as access rules and DHCP server. Cisco Security Manager 4.13 provides Bridge group interface support for the routed mode and for the policies that use the BVI interfaces and BVI member interfaces.
- **SAML2.0 based SSO for Clientless Remote Access VPN Phase 2 Support** — Starting with Cisco Security Manager 4.13, SAML 2.0 supports two new options - the Enable Internal Flag and the Enable Force Re-authentication option.
  When enabled, the Internal Flag identifies the Identity Provider in a private network and the SAML Identity Provider can only be accessed through a WebVPN connection.
  When the Force Re-authentication option is enabled, the Identity Provider must authenticate the presenter directly rather than rely on a previous security context.
- **CMPv2 Support** — To be positioned as a security gateway device in wireless LTE networks, the ASA now supports certain management functions using the Certificate Management Protocol (CMPv2). Correspondingly the Public Key Infrastructure (PKI) Policy has been enhanced in Cisco Security Manager 4.13.
- **VM Attributes** — Starting from Cisco Security Manger 4.13, you can define network objects to filter traffic according to attributes associated with one or more Virtual Machines (VMs) in an VMware ESXi environment managed by VMware vCenter. You can define access control lists (ACLs) to assign policies to traffic from groups of VMs sharing one or more attributes.
- **Security Gateway Dynamic RRI Support** — Dynamic Reverse Route Injection occurs upon the successful establishment of IPsec Security Associations (SA's) when dynamic is specified for a crypto map. Routes are added based on the negotiated selector information. The routes will be deleted after the IPsec SA's are deleted. Starting from Cisco Security Manager 4.13, dynamic RRI is supported on IKEv2 based static crypto maps only.
- **IPv6 Support:**
  - IPv6 Address Support — Starting with Cisco Security Manager 4.13, AAA Server Host Configuration supports IPv6 addresses. Additionally the Syslog server supports IPv6 addresses alongside IPv4 addresses. Ci 4.13 supports IPv6 configurations for the HTTP, Telnet, SSH policies for ASA 8.2(3) version and above.

  - IPv6 Trace Route Support — The trace route command now accepts IPv6 addresses.
  - Cisco Security Manager 4.13 supports IPv6 configurations for the HTTP, Telnet, SSH policies from ASA 8.2.3 version and above.
- **Clientless SSL VPN Customization** — With Cisco Security Manager 4.13, you can customize the user prompt in the SSL VPN dialog. All web interfaces will now display details of the current session, including the user name used to login, and user privileges which are currently assigned. This will help the user be aware of the current user session and will improve user security.
- **Bidirectional Forwarding Detection (BFD) support for Active/Standby failover health monitoring on the Firepower 9300 and 4100** — You can enable Bidirectional Forwarding Detection (BFD) for the failover health check between two units of an Active/Standby pair on the Firepower 9300 and 4100. Using BFD for the health check is more reliable than the default health check method and uses less CPU.
- **Director-Localization** — Director localization is used to minimize the RTT latency and the delays in performance lookup messages. You can enable this option to make the flow owner and director to be in the same DC site, so that the flow owner lookup is done in local DC site, and the traffic is contended within the same site.
- **Multiple Certificate Authentication Support** — The Cisco Security Manager supports ASA 9.7.1 feature of multiple certificate authentication for VPN connectivity. The client can authenticate remote VPN users with two client certificates. The two client certificate could be a combination of one user certificate and one machine certificate, or two user certificates. Two machine certificate authentication is not supported for security considerations. The multiple certificate authentication works for both SSL VPN and IPsec VPN.
- **VRF Support to Trustpool** — Beginning with Cisco Security Manager 4.13, source interface option is provided that ASA can use to identify the destination URL. This feature is not supported for ASA versions lower to 9.7.1. If the interface configured is management-only, the destination URL is routed through management VRF. For non-management interface, the URL is routed through data VRF. If interface is not specified, both the routing table of the management and data VRF are polled to identify the route to reach the URL.
- **Tunnel Interface** — Beginning with Cisco Security Manager 4.13, route based VPN method for the Site-to-Site VPN is supported. Towards this requirement, you can define tunnel interface for the VPN and its associated IPSec policy. VTI is supported only for Regular IPsec with Hub and Spoke, and Point to Point VPN topologies. VTI is not supported for other topologies like Full Mesh Topology, Extranet VPN Topology and RAVPN Policies.
- **Flow Control** — Cisco Security Manager 4.13 supports SCTP in traffic flow. Thus, while configuring traffic flow object, option to specify SCTP protocol and to specify a destination port number or range of numbers to use for matching traffic is introduced.
- **IGP Timeout Policy** — Prior to ASA 9.7.1, ASA had 70 seconds as a OSPF convergence time. In ASA 9.7.1 the convergence time was made as user configurable. In CSM 4.13 existing timeout page is enhanced to support the OSPF convergence time. The IGP Timeout CLI is introduced for setting the OSPF convergence time.

Support for ASA 9.6(2) version

- **Bridge group interface support** — Beginning with Cisco Security Manager 4.13, a Bridge Group now supports 64 interfaces.

Other Enhancements in Cisco Security Manager 4.13

- **31 Bit Subnet Mask** — In earlier versions, Cisco Security Manager allowed usage of 255.255.255.253 as subnet mask for a point to point interface. Beginning from version 4.13, Cisco Security Manager allows 255.255.255.254.

- **Remote Access VPN Configuration Wizard Changes** — Starting with Cisco Security Manager 4.13, the Configuration Wizard now includes the following features- The Global IPv6 Address Pool, Primary/Secondary IPv6 DNS Server and Spilt Tunneling.
- **Report Manager enhancement** — Starting with Cisco Security Manager 4.13, the VPN User Report includes Public IP and Assigned IP information.
- **Workflow mode Deployment jobs enhancement** — Starting with Cisco Security Manager 4.13, you can configure whether or not a submitter can approve his /her own deployment jobs.
- **Out Of Band Notifications** — Cisco Security Manager considers an out-of-band (OOB) change to be any change made to a device manually or outside of Security Manager control. Starting with Cisco Security Manager version 4.13, whenever (HPM) detects an OOB change, and syncs with the Configuration Manager, a separate email alert notification is sent (to configured recipients) for each device being monitored.
- **Support for TLS 1.2 protocol for Security Manager client and server communication** — From ASA 9.7.1, the Cisco Security Manager supports TLS1.2 new cipher suites— aes256-sha384 and aes128-sha256.
- **IPSec Profile Policy Object Introduced** — A new policy object called “IPSec Profile” is implemented in order to associate Crypto IPSec Profile to VTI Interfaces.
- **Restrict overriding the deployment default option** — Whenever a user tries to change the default Out Of Band Behavior option to any other option the change will be permitted based on the user authorization set in the 'Modify_Deploy_OOB' option set in the Role Based Access Control (RBAC) configuration, for the user.
- **Rollback operation is controlled by a separate Role Based Access Control** — By default only the System Administrator and the Network Administrator roles are permitted to perform the rollback operation.If required, a user can create a custom role and assign the Rollback task to that role.

Installation Notes

Please refer to the *Installation Guide for Cisco Security Manager 4.13* for specific installation instructions and for important information about client and server requirements. Before installing Cisco Security Manager 4.13, it is critical that you read the notes listed in this section and the Important Notes, page 7.

- 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 4.13* 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 4.13 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 4.13* 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.

Important Notes

The following notes apply to the Security Manager 4.13 release:

- 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:
  - **a.** KB2919442
  - **b.** 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.

c. KB2919355, KB2932046, KB2959977, KB2937592, KB2938439, and KB2934018

d. 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.
- 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.
  - The dynamic behavior of the failover devices such as ASA and IOS, is not supported in Cisco Security Manager. This is because, CSM does not identify the failover LAN unit as primary or secondary. However, after an HA switchover on ASA, the CSM continues to manage the secondary unit with active IP.
- 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.

- 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 4.13* 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 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.
- Do not run SQL queries against the database.
- If an online help page displays blank in your browser view, refresh the browser.
- Beginning with version 4.9, Security Manager 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.
- 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.

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 4.13 are included in the following search:

- Open caveats—Release 4.13
- Open caveats—Releases prior to 4.13

Resolved Caveats

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

- Resolved caveats—Release 4.13
- Resolved caveats—Releases prior to 4.13

  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 4.13*.
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 4.13*.
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 4.13.*

If you want to:	Do this:
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 7 of *Installation Guide for Cisco Security Manager 4.13*. • 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 4.13*.

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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.