Release Notes for Cisco Security Manager 4.7

Originally Published: August 21, 2014
Last Updated: May 30, 2016

Security Manager 4.7 is now available. Registered SMARTnet users can obtain release 4.7 from the Cisco support website by going to http://www.cisco.com/go/csmanager and clicking Download Software for this Product under Support.

This document contains the following topics:

- Introduction, page 1
- Supported Component Versions and Related Software, page 2
- What’s New, page 3
- Installation Notes, page 6
- Service Pack 1 Download and Installation Instructions, page 8
- Service Pack 2 Download and Installation Instructions, page 10
- Service Pack 3 Download and Installation Instructions, page 11
- Service Pack 4 Download and Installation Instructions, page 12
- Important Notes, page 14
- Caveats, page 18
- Where to Go Next, page 27
- Product Documentation, page 27
- Obtain Documentation and Submit a Service Request, page 27

Introduction

Note

Use this document in conjunction with the documents identified in Product Documentation, page 27. 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 4.7**—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](https://www.cisco.com) 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 4.7**—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.

Before using Cisco Security Manager 4.7, we recommend that you read this entire document. In addition, it is critical that you read the Important Notes, page 14, the Installation Notes, page 6, and the Installation Guide for Cisco Security Manager 4.7 before installing Cisco Security Manager 4.7.

This document lists the ID numbers and headlines for issues that may affect your operation of the product. This document also includes a list of resolved problems. If you accessed this document from Cisco.com, you can click any ID number, which takes you to the appropriate release note enclosure in the Cisco Bug Search Tool (BST). The release note enclosure contains symptoms, conditions, and workaround information.

## 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 4.7.

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>
<thead>
<tr>
<th>Table 1</th>
<th>Supported Versions for Components and Related Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td><strong>Support Releases</strong></td>
</tr>
<tr>
<td>Component Applications</td>
<td></td>
</tr>
<tr>
<td>Cisco Security Manager</td>
<td>4.7</td>
</tr>
<tr>
<td>Auto Update Server</td>
<td>4.7</td>
</tr>
</tbody>
</table>
What’s New

Cisco Security Manager 4.7 Service Pack 3
Security Manager 4.7 Service Pack 3 provides fixes for various problems. For more information, see Resolved Caveats—Release 4.7 Service Pack 3, page 23.

In addition to the resolved bugs listed below, this service pack also provides IPv6 support for Internet Control Message Protocol (ICMP) configuration and packet-tracer features.

Cisco Security Manager 4.7 Service Pack 2
Security Manager 4.7 Service Pack 2 provides fixes for various problems. For more information, see Resolved Caveats—Release 4.7 Service Pack 2, page 23.
This service pack also provides support for IPv6 address for failover-configured interfaces on devices running the ASA software version 8.2(2) or higher.

Cisco Security Manager 4.7 Service Pack 1
Security Manager 4.7 Service Pack 1 provides fixes for various problems. For more information, see Resolved Caveats—Release 4.7 Service Pack 1, page 23.

This service pack also provides support for the following:
- ASA software version 9.2(3)
- ISE version 1.3
- TLS version 1.2

Cisco Security Manager 4.7
In addition to resolved caveats, this release includes the following new features and enhancements:
- Support for additional devices (for detailed compatibility information, refer to Supported Devices and Software Versions for Cisco Security Manager 4.7):
  - ASA 9.1(5), ASA 9.2(1), ASA 9.2(2), and ASA 9.3(1)
What’s New

- Cisco Virtual Security Appliance (ASAv) on ASA 9.2(1)+
- IPS 7.3(2)

- Crosslaunch to FireSIGHT Management Center for ASAs with a FirePOWER module installed. The GUI element for single sign-on configuration now extends to FireSIGHT Management Center in addition to Prime Security Manager.

- Support for detection of ASA FirePOWER modules installed in ASA devices.

- A new OOB Re-sync Tool, available for the first time in Version 4.7 of Security Manager, helps you re-sync, or reconcile, out of band data. The OOB Re-sync Tool is an extension of the OOB Detection Tool available in Security Manager 4.6 and earlier versions and continued into 4.7. The OOB Re-sync Tool aims to automate the process of bringing OOB data on a device into your Security Manager installation while retaining the policy structures that you previously established.

- In Report Manager, the new “Connection Profile Report” has been added to the System Reports > VPN folder.

- Also in Report Manager, the Username filter now supports uppercase/lowercase character sensitivity, wildcard characters, and “NOT” operation.

- Light Diagnostics Support—Beginning with Version 4.7, Security Manager supports diagnostics in a new, light variant; this “Light Diagnostics” variant collects only basic information; as a result, the diagnostics file is smaller, and its generation is faster. The existing “General Diagnostics” variant is the same in Version 4.7 as it was in 4.6 and earlier versions.

- Device Filter for Shared Policy Assignment—In Version 4.7, Cisco Security Manager has added a new option to the available filtering choices in the Device Filter. This new option provides a filter for devices that have shared policies applied.

- In Health and Performance Monitor in 4.6 and earlier versions of Security Manager, e-mail notifications were sent to users when HPM alerts were generated for ASA, IPS, and VPN. This framework has been enhanced for Version 4.7 to send SNMP trap notifications also.


- Beginning with Version 4.7, all VPN functionalities provided by Security Manager are supported on virtualized Adaptive Security Appliance (virtualized ASA) devices.

- Crypto maps—Beginning with Version 4.7, Security Manager enables you to manually configure the crypto map name and crypto ACL name for each peer device in a VPN topology. This feature is supported only in Regular IPsec topologies.

- Support for ASA Version 9.2.1—Security Manager 4.7 enables you to exempt certain users of clientless SSL VPN and AnyConnect from running the Cisco Secure Desktop software in VPN tunnel groups.

- Support for ASA Version 9.3.1 custom policy attribute—Security Manager 4.7 provides the ability to configure custom attributes in dynamic access policy. AnyConnect custom attributes allow for a more expeditious delivery and deployment of new endpoint features by giving the ASA the ability to generically support the addition of new client controls without the need for an ASA software upgrade. Beginning with Version 4.7, Security Manager enables you to add custom attribute data to an existing custom attribute type.

- Support for AnyConnect Version 3.2—Security Manager Version 4.7 provides support for ISE posture in AnyConnect Version 3.2. You can use the ISE editor to configure the ISE profile.

- Security Manager Version 4.7 enables you to create smart tunnel network objects and define whether to tunnel all traffic or to allow or disallow traffic through specified networks.
• Security Manager Version 4.7 enables you to define a script to use in mapping the user name from the certificate. This mapping is used to specify the fields in a digital certificate from which the user name is extracted. You can either specify the script parameters or configure custom LUA scripts.

• Security Manager Version 4.7 addresses gaps in dynamic access policy to support the functionalities equivalent to those provided in the Adaptive Security Device Manager software and managed devices. The attributes that were enhanced in this version include AAA, LDAP, Device, File, Always-on VPN, and, Session Action attributes.

• Security Manager Version 4.7 addresses gaps in group policy including:
  – Allowing AnyConnect to automatically establish a VPN session as soon as the user logs on to the computer.
  – Allowing configuring the proxy settings of the end users’ browser as required, when connected to the corporate network, and by automatically reverting to the original configuration when disconnected.

• Support for the Border Gateway Protocol (BGP) on ASA 9.2(1)+. BGP is an inter autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

  For ASA 9.3(1)+, BGP is supported in L2 (EtherChannel Type) and L3 (Individual Interface Type) clustering modes.

• Support for the following ASA routing policy objects: route maps, policy lists, prefix lists, As paths, and community lists.

**Note**

For Security Manager 4.7, route map objects can only be used with BGP, OSPF, and OSPFv3 routing protocols.

• For ASA 9.2(1)+, OSPF now supports the Fast Hello Packets feature, resulting in a configuration that results in faster convergence in an OSPF network.

• For ASA 9.2(1)+, the valid range of values for OSPF interface intervals and virtual link intervals have been updated.

• For ASA 9.2(1)+, new OSPF timers were added; old ones were deprecated.

• For ASA 9.2(1)+, route filtering using ACL is now supported.

• For ASA 9.2(1)+, OSPF redistribution feature was added.

• Support for static null0 route configuration. A static null0 route is used to forward unwanted or undesirable traffic into a black hole.

• For ASA 9.3(1)+, support for Nonstop Forwarding was added for BGP, OSPFv2, and OSPFv3.

• Support for Embedded Event Manager (EEM) on ASA 9.2(1)+. The EEM feature enables you to debug problems and provides general purpose logging for troubleshooting. The EEM responds to events in the EEM system by performing actions. There are two components: events that the EEM triggers, and event manager applets that define actions. You may add multiple events to each event manager applet, which triggers it to invoke the actions that have been configured on it.

• Support for RADIUS Dynamic Authorization Change of Authorization (CoA) services for the AAA server groups on ASA 9.2(1)+.

• When using the RADIUS protocol on an ASA 9.2(1)+ device, you can enable the generation of RADIUS interim-accounting-update messages. Currently these messages are only generated when a VPN tunnel connection is added to a clientless VPN session. When this happens the accounting update is generated in order to inform the RADIUS server of the newly assigned IP address.
• When using the RADIUS protocol on an ASA 9.2(1)+ device, you can enable authorize-only mode for the RADIUS server group so that the common password configured for individual AAA servers is not required and does not need to be configured.
• For ASA devices running 9.1(5) or later, you can now configure up to 128 SNMP hosts.
• Added support for enabling authorization for exec shell access.
• Added support for automatic enabling of AAA authorization. Administrators who have sufficient authorization privileges may enter privileged EXEC mode by entering their authentication credentials once.
• Beginning with ASA 9.1(5), you can configure the rule engine to use a transactional model when implementing rule changes. With the transactional model, the ASA continues to use the old rules until the new rules are compiled and ready for use. Using the transactional model, performance should not drop during the rule compilation. You can enable the transactional model for access group rules, NAT rules, or both.
• Supports URL normalization for ASA 9.1(5)+. URL normalization is an additional security feature that includes path normalization, case normalization and scheme normalization. URLs specified in an ACE and portal address bar are normalized before comparison; for making decisions on webvpn traffic filtering.
• You can use the CLI Prompt page to customize the prompt used by ASA 7.2(1)+ devices during CLI sessions.
• Support for configuration of traffic redirection to a FirePOWER module installed in an ASA. Applicable only on ASA 55xx-X devices running version 9.2(1)+.
• Support for mount points. Mount points are used to make a Common Internet File System (CIFS) or a File Transfer Protocol (FTP) file system accessible to the security appliance.
• Support for configuring virtual HTTP servers and virtual Telnet servers.
• Some switches do not support dynamic port priority with LACP (active and standby links). Beginning with ASA 9.2(1), you can now disable dynamic port priority to provide better compatibility with spanned EtherChannels.
• For ASA 9.2(1)+, EtherChannels now support up to 16 active links.

**Installation Notes**

Please refer to the *Installation Guide for Cisco Security Manager 4.7* for specific installation instructions and for important information about client and server requirements. Before installing Cisco Security Manager 4.7, it is critical that you read the notes listed in this section and the Important Notes, page 14.

• 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. It is available at [http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/installation/guide/IG/licensing.html](http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/installation/guide/IG/licensing.html).
• 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

• The Installation Guide for Cisco Security Manager 4.7 provides important information regarding server requirements, server configuration, and post-installation tasks.

• The Installation Guide for Cisco Security Manager 4.7 also provides important information regarding operating system and browser support. The following few bullet points list the most important new support information in this area.

• Supported operating systems for the server machine are the following:
  - Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit
  - Microsoft Windows Server 2012 Standard—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 Standard—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, or 10.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 for this release of the product 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 4.7 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 for this release of the product 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.

\[\text{Note}\]

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.

\[\text{Caution}\]

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 service pack 1, follow these steps:

\[\text{Note}\]

You must install the Cisco Security Manager 4.7 FCS build on your server before you can apply this service pack.
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](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 4.7** in the rightmost column.

**Step 4**
Click **Security Manager (CSM) Software** and then click **4.7sp1** under **Latest**.

**Step 5**
Download the file `fcs-csm-470-sp1-win-k9.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 `fcs-csm-470-sp1-win-k9.exe` file that you previously downloaded.

**Step 9**
In the Install Cisco Security Manager 4.7 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:
  

- **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]
To download and install service pack 2, follow these steps:

**Note** You must install the Cisco Security Manager 4.7 FCS build on your server before you can apply this service pack.

**Caution** Before installing this service pack, you must 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.

**Note** While restoring database backups, do not restore a database backup from Security Manager version 4.7 or 4.7 SP1 build directly on a 4.7 SP2 installation. Instead, restore the database to the respective version from which the backup was taken and then install version 4.7 SP2.

**Step 1** Go to [http://www.cisco.com/go/csmmanager](http://www.cisco.com/go/csmmanager), 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 4.7** in the rightmost column.

**Step 4** Click **Security Manager (CSM) Software** and then click **4.7sp2** under **Latest**.

**Step 5** Download the file fcs-csm-470-sp2-win-k9.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 fcs-csm-470-sp2-win-k9.exe file that you previously downloaded.

**Step 9** In the Install Cisco Security Manager 4.7 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:


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 3 Download and Installation Instructions

To download and install service pack 3, follow these steps:

Note You must install the Cisco Security Manager 4.7 FCS build on your server before you can apply this service pack.

Caution Before installing this service pack, you must 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.

Note While restoring database backups, do not restore a database backup from Security Manager version 4.7 or 4.7 SP2 build directly on a 4.7 SP3 installation. Instead, restore the database to the respective version from which the backup was taken and then install version 4.7 SP3.

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 4.7 in the rightmost column.

Step 4 Click Security Manager (CSM) Software and then click 4.7sp3 under Latest.

Step 5 Download the file fcs-csm-470-sp3-win-k9.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 fcs-csm-470-sp3-win-k9.exe file that you previously downloaded.
Step 9  In the Install Cisco Security Manager 4.7 Service Pack 3 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:


   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 4 Download and Installation Instructions

To download and install service pack 4, follow these steps:

**Note**
You must install the Cisco Security Manager 4.7 FCS build on your server before you can apply this service pack.

**Caution**
Before installing this service pack, you must 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.

**Note**
While restoring database backups, do not restore a database backup from Security Manager version 4.7 or 4.7 SP3 build directly on a 4.7 SP4 installation. Instead, restore the database to the respective version from which the backup was taken and then install version 4.7 SP4.
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 4.7** in the rightmost column.

Step 4: Click **Security Manager (CSM) Software** and then click **4.7sp4** under **Latest**.

Step 5: Download the file `fcs-csm-470-sp4-win-k9.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 `fcs-csm-470-sp4-win-k9.exe` file that you previously downloaded.

Step 9: In the Install Cisco Security Manager 4.7 Service Pack 4 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:


   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

Security Manager 4.7 Service Pack 1

The following notes and fixes apply to the Security Manager 4.7 Service Pack 1 release:

- Due to import regulations in some countries, the Oracle implementation provides a default cryptographic jurisdiction policy file that limits the strength of cryptographic algorithms. If stronger algorithms need to be configured or are already configured on the device (for example, AES with 256-bit keys, DH group with 5,14,24), follow these steps:
  a. Download the unlimited strength cryptography policy .jar files from http://www.oracle.com/technetwork/ > Downloads > Java SE > Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 7. (Click the download button to download the files by accepting the license agreement.)
  b. Replace local_policy.jar and US_export_policy.jar on your Security Manager server in the folder CSCOpx\MDC\vms\jre\lib\security.
  c. Restart the Security Manager server.

- CSCuh52092 — This fix enables you to configure HTML and PDF reports and set the timeout to quit report generation after preset time. You can configure the following properties:
  - #generate_activity_report_timeout=10
  - #generate_activity_pdf_report=true
  - #generate_activity_html_report=false

  Follow these steps:
  a. From $NMSROOT\MDC\athena\config\ subdirectory, open csm.properties file in a text editor, such as Notepad. ($NMSROOT is the full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\CSCOpx]).
  b. Search for the above mentioned properties in the csm.properties file.
  c. Remove the # character at the beginning of the line of code to enable the specific property.
  d. Timeout (generate_activity_report_timeout) is common for PDF and HTML report generation. If enabled and set, report generation will stop after the set time and release all resources. Set the timeout in minutes depending upon the mean time of report generation. We recommend setting the timeout to 10 minutes.
  e. Enable either generate_activity_pdf_report or generate_activity_html_report and set it “true” based on your requirement. If both the properties are set to true, Security Manager will generate the report in PDF format.
  f. To disable a property, add the # character at the beginning of the line of code.
  g. Save and then close the csm.properties file.
  h. Restart the Cisco Security Manager Daemon Manager service from Start > Programs > Administrative Tools > Services.

- CSCup28957 — This fix enables you to exclude the list of operation rows in all applicable policies from the Activity Change report.
  - Excluded operations must be comma separated and if the value is empty or the line of code is commented, it will include all operations.
  - The excluded operations are Add, Delete, Modify, Move, ReOrder, Assign, UnAssign. You must not modify these operation names, they should be used as is.
By default the values of the operations are empty, if you wish to exclude a specific operation, follow these steps:

a. From SNMSROOT\MDC\athena\config\ subdirectory, open the csm.properties file in a text editor, such as Notepad. (SNMSROOT is the full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\CSCOpx])

b. Search for ActChangeReport.excludedOperations=

c. Add the required excluded operation as follows using any of the available options. For example:
   - ActChangeReport.excludedOperations=ReOrder
   - ActChangeReport.excludedOperations=Add,ReOrder
   - ActChangeReport.excludedOperations=Add,Modify,Move,ReOrder

d. Save and then close the csm.properties file.

e. Restart the Cisco Security Manager Daemon Manager service from Start > Programs > Administrative Tools > Services.

**Security Manager 4.7**

The following notes apply to the Security Manager 4.7 release:


- Security Manager does not support Internet Control Message Protocol (ICMP) for IPv6 addresses. It supports ICMP for IPv4 addresses only.

- 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.

- 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.

- 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](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.

- 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.

- If you are upgrading from Security Manager 4.6 to 4.7, the following are newly supported ASA policies in Security Manager 4.7:
  - 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 4.7 from Security Manager 4.6, the OSPF page will show a red-banner. To overcome this issue, you must rediscover the ASA.
Important Notes

- 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.

- Device and Credential Repository (DCR) functionality within Common Services is not supported in Security Manager 4.7.

- 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 4.7 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

This section describes the open and resolved caveats with respect to this release.

For your convenience in locating caveats using the Cisco Bug Search Tool (BST), the caveat titles listed in this section are drawn directly from the Bug Search Tool database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note

If you are a registered cisco.com user, you can access the Cisco Bug Search Tool on cisco.com at https://tools.cisco.com/bugsearch. For more information about the Bug Search Tool, visit the help page at http://www.cisco.com/web/applicat/cbsshelp/help.html.

To become a registered cisco.com user, go to the following website: http://tools.cisco.com/RPF/register/register.do

This section contains the following topics:

- Open Caveats—Release 4.7, page 18
- Resolved Caveats—Release 4.7 Service Pack 4, page 22
- Resolved Caveats—Release 4.7 Service Pack 3, page 23
- Resolved Caveats—Release 4.7 Service Pack 2, page 23
- Resolved Caveats—Release 4.7 Service Pack 1, page 23
- Resolved Caveats—Release 4.7, page 25
- Resolved Caveats—Releases Prior to 4.7, page 26

Open Caveats—Release 4.7

The following caveats affect this release and are part of Security Manager 4.7.

- Cisco IOS Router Devices Caveats
- Cisco IPS and IOS IPS Devices Caveats
- Client and Server Install Caveats
- Device Management, Discovery, and Deployment Caveats
- Event Viewer Caveats
- Firewall Services Caveats
- Health and Performance Monitor Caveats
- Image Management Caveats
- Miscellaneous Caveats
- Policy Management Caveats
- Report Manager Caveats
VPN Device and Configuration Support Caveats

In some instances, a known problem might apply to more than one area, for example, a PIX device might encounter a problem during deployment. If you are unable to locate a particular problem within a table, expand your search to include other tables. In the foregoing example, the known problem might be listed in either the Deployment table or the PIX/ASA/FWSM Configuration table.

Table 2 Cisco IOS Router Devices Caveats

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCth95357</td>
<td>XE: Deploy Fails when Memory Critical Notifications are Changed</td>
</tr>
<tr>
<td>CSCti15944</td>
<td>CLI: “dot1x pae authenticator” generated after deployment of 802.1x</td>
</tr>
<tr>
<td>CSCtg12795</td>
<td>Generic Router : AAA rules getting negated.</td>
</tr>
</tbody>
</table>

Table 3 Cisco IPS and IOS IPS Devices Caveats

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtk36259</td>
<td>MU-IPS Licensing page taking too long for Refresh / CCO Update operation</td>
</tr>
<tr>
<td>CSCug68487</td>
<td>CSM isn't closing all the HTTPS session as part of config deployment</td>
</tr>
<tr>
<td>CSCum79301</td>
<td>TP tunings are not applied when sig is tuned other than status fields</td>
</tr>
</tbody>
</table>

Table 4 Client and Server Install Caveats

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtq99125</td>
<td>Installation: Evaluation and Licensing options get enabled simultaneous</td>
</tr>
<tr>
<td>CSCtr71792</td>
<td>ETSGJ-CH:CSM Launch Icons Missing on XP JOS Client</td>
</tr>
<tr>
<td>CSCtr72248</td>
<td>ETSGJ-CH:Not able to proceed with install if going back to previous page</td>
</tr>
<tr>
<td>CSCuj65797</td>
<td>CSM 4.5 Security Tools page UI launching Issues on Win 7 32 bit client</td>
</tr>
</tbody>
</table>

Table 5 Device Management, Discovery, and Deployment Caveats

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCub81927</td>
<td>Scal Testing: DB error during deployment</td>
</tr>
<tr>
<td>CSCuc13848</td>
<td>Getting error while submitting a ticket for Validation.</td>
</tr>
<tr>
<td>CSCup91317</td>
<td>ASAv:Rediscovery fails after OOB image Upgrade</td>
</tr>
</tbody>
</table>

Table 6 Event Viewer Caveats

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtg57676</td>
<td>Internal error thrown when portlist is used in service object filter.</td>
</tr>
<tr>
<td>CSCtg57745</td>
<td>Filtering does not work when only protocol name is used in service obj.</td>
</tr>
</tbody>
</table>
### Table 6  Event Viewer Caveats (Continued)

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtg57839</td>
<td>Results not correct when network obj with non-contiguous mask is used.</td>
</tr>
<tr>
<td>CSCua81392</td>
<td>CSM 4.2 - Eventing directory does not get deleted</td>
</tr>
<tr>
<td>CSCuh16940</td>
<td>IPS subscription is not getting closed when unmonitoring the device</td>
</tr>
<tr>
<td>CSCuh38244</td>
<td>P2E: Events are not filtered properly if ACE has multiple services</td>
</tr>
<tr>
<td>CSCui01213</td>
<td>Changing “Time field” by highlighting the value is not inserting properly</td>
</tr>
</tbody>
</table>

### Table 7  Firewall Services Caveats

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtf32208</td>
<td>Deployment fails with ACE edit in ACL BB</td>
</tr>
<tr>
<td>CSCtg80500</td>
<td>Manual-NAT: need validation for “neq” operator in static NAT</td>
</tr>
<tr>
<td>CSCti08077</td>
<td>system context Config file discovery fails with ASA 5580 platform</td>
</tr>
<tr>
<td>CSCti10613</td>
<td>Int: ASA 5580/85 should support max 1034 int allocation to context</td>
</tr>
<tr>
<td>CSCto67515</td>
<td>ASA/ASASM Failover commands not negated</td>
</tr>
<tr>
<td>CSCto80002</td>
<td>UID: Deployment fails when domain is used in ACL and is deleted</td>
</tr>
<tr>
<td>CSCtuq04794</td>
<td>NAT: Deployment is failing for object NAT for Translate DNS rule</td>
</tr>
<tr>
<td>CSCtuq20997</td>
<td>NAT:Subnet Can not be used as mapped Source in Dynamic NAT policy</td>
</tr>
<tr>
<td>CSCtuq24069</td>
<td>UID: repeated ACL delta with ACL match protocol inspection</td>
</tr>
<tr>
<td>CSCtuq36739</td>
<td>NAT: Same Mapped address cannot be used to perform both NAT and PAT</td>
</tr>
<tr>
<td>CSCtuq63721</td>
<td>UID: order of AAA server negation/appending _1 on discovery should modify</td>
</tr>
<tr>
<td>CSCtuq82588</td>
<td>Discovery fails for device with scan safe AAA in CSM 4.1</td>
</tr>
<tr>
<td>CSCtr12016</td>
<td>ETSGJ-CH:Japanese User not displayed in Identity UserGroup UI</td>
</tr>
<tr>
<td>CSCtr12155</td>
<td>ETSGJ-CH:Japanese User Group shows Name as Square blocks in JOS Client</td>
</tr>
<tr>
<td>CSCtr25092</td>
<td>ETSGJ-CH:Pop-up for wrong bind in Identity needs to be revisited</td>
</tr>
<tr>
<td>CSCtr25195</td>
<td>ETSGJ-CH:Domain name with special characters are permitted</td>
</tr>
<tr>
<td>CSCtr30676</td>
<td>Deployment fails when http accounting banner from file is configured</td>
</tr>
<tr>
<td>CSCtr71998</td>
<td>ETSGJ-CH:Incremental pop-up for a wrong MAC in Cat6k ASA-SM Failover</td>
</tr>
<tr>
<td>CSCts25221</td>
<td>Edit ACL in Identity Policy-CSM generates incorrect order of cli</td>
</tr>
<tr>
<td>CSCtw48451</td>
<td>Override BB are not mapping with BBs used in import rules</td>
</tr>
<tr>
<td>CSCty77037</td>
<td>Remove unreferenced Object-Group option can cause deployment error</td>
</tr>
<tr>
<td>CSCud37752</td>
<td>ASA Image Downgrade From 9.0 to 8.4.4 Contain Xlate Rules in Preview</td>
</tr>
<tr>
<td>CSCuj99884</td>
<td>Global search does not display default inspection rule present in device</td>
</tr>
<tr>
<td>CSCuo15620</td>
<td>WebACL: URL Validation is not happening with the added ACL object</td>
</tr>
<tr>
<td>CSCup33218</td>
<td>[OOB]Avoid Rule Splitting during OOB Re-synch</td>
</tr>
<tr>
<td>CSCup76874</td>
<td>[OOB]Change In Section Structure After Re-Synch for Modified ACL</td>
</tr>
<tr>
<td>CSCup77926</td>
<td>Red banner Error in asa 921 post upgrade from csm 4.5</td>
</tr>
</tbody>
</table>
**Table 7  
Firewall Services Caveats (Continued)**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuq19631</td>
<td>Route Map edit is not working properly.</td>
</tr>
<tr>
<td>CSCuq23825</td>
<td>Prefix-list/As-Path modification and route-map delete not in one activity</td>
</tr>
</tbody>
</table>

**Table 8  
Health and Performance Monitor Caveats**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtt95667</td>
<td>FW: Certificates should be displayed as part of Non VPN Views</td>
</tr>
<tr>
<td>CSCtx48130</td>
<td>VPN: SitetoSite VPN tunnel details not proper with dynamic cryptomap 8.4</td>
</tr>
<tr>
<td>CSCue50284</td>
<td>Tunnel Alerts: Traps Not Processed if the Remote Subnet is a Host</td>
</tr>
<tr>
<td>CSCuo10773</td>
<td>Perf : HPM Client Lag Issue after leaving it idle for long time</td>
</tr>
</tbody>
</table>

**Table 9  
Image Management Caveats**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCup89988</td>
<td>ASAv: Image Upgrade Fails for Virtual ASA</td>
</tr>
<tr>
<td>CSCuq01829</td>
<td>ReloadWait: Image loading failing from IM with an active VPN tunnel</td>
</tr>
</tbody>
</table>

**Table 10  
Miscellaneous Caveats**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtq99617</td>
<td>CSM UI unresponsive for a long period in MU testing</td>
</tr>
<tr>
<td>CSCuh86712</td>
<td>Device state is not changed as rediscovering the changes</td>
</tr>
<tr>
<td>CSCui32627</td>
<td>Adding IP to cluster pool is not getting updated in logrelay filter</td>
</tr>
<tr>
<td>CSCui78433</td>
<td>Flickering issue : IP Intel and View Statistics refresh/other flows</td>
</tr>
<tr>
<td>CSCuj25254</td>
<td>Not able to crosslaunch frm CSM-PRSM if username starts with bold letter</td>
</tr>
<tr>
<td>CSCuj50087</td>
<td>Image is removing from the list after viewing the config file</td>
</tr>
<tr>
<td>CSCuj60513</td>
<td>Logrelay:Warning can be given when one user changes impacting other user</td>
</tr>
<tr>
<td>CSCui96498</td>
<td>Device Status view is not getting autorefreshed when in undock view</td>
</tr>
<tr>
<td>CSCui97177</td>
<td>Device filter is not working in OOB detection window</td>
</tr>
<tr>
<td>CSCun70866</td>
<td>Discrepancy in displaying Geoip Schedule download timings</td>
</tr>
<tr>
<td>CSCuo06326</td>
<td>Cross launch to DC with IPv6 address does not work with 2 browsers</td>
</tr>
<tr>
<td>CSCuo29366</td>
<td>Need proper validation error message with invalid data for BB</td>
</tr>
</tbody>
</table>

**Table 11  
Policy Management Caveats**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCud86519</td>
<td>CSM deployment error with an Object</td>
</tr>
<tr>
<td>CSCuh40492</td>
<td>Configuration differences in OOB detection not shown exactly</td>
</tr>
</tbody>
</table>
### Caveats

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.7 Service Pack 4.

### Table 11  
**Policy Management Caveats (Continued)**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCun24271</td>
<td>Mutual usage of PB in multiuser scenario showing exceptions in message</td>
</tr>
<tr>
<td>CSCup00905</td>
<td>Smart Tunnel Network List BB: Overriden Values Not Imported</td>
</tr>
</tbody>
</table>

### Table 12  
**Report Manager Caveats**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuo48915</td>
<td>VPN User rpt: Couldn’t do the column sorting based on login / logout time</td>
</tr>
<tr>
<td>CSCuq28564</td>
<td>Upgrade: Issue in showing pre upgrade data in VPN User report</td>
</tr>
</tbody>
</table>

### Table 13  
**VPN Device and Configuration Support Caveats**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCqu67354</td>
<td>preview fails, rule name (SSLVPN-&gt;othersett-&gt;content rewrite) having space</td>
</tr>
<tr>
<td>CSCtq86149</td>
<td>deployment fails: existing Virtual Template int with type serial - Ezvpn</td>
</tr>
<tr>
<td>CSCtr06681</td>
<td>preview fails: if SSO name is given with spaces</td>
</tr>
<tr>
<td>CSCtq28222</td>
<td>IPSec Proposal is not discovered, if DVTI/VRF is configured in ISR</td>
</tr>
<tr>
<td>CSCts30832</td>
<td>Preview failed due to FQDN acl BB used in group policy.</td>
</tr>
<tr>
<td>CSCub82270</td>
<td>CSM deletes the existing ACL when changing protected nw/Spk2Spk connecti</td>
</tr>
<tr>
<td>CSCub89125</td>
<td>PKI node under Remote Access VPN to be enabled</td>
</tr>
<tr>
<td>CSCud61707</td>
<td>PKI deployment failed with trustpoint not enrolled error for ASA 9.0</td>
</tr>
<tr>
<td>CSCum00081</td>
<td>Discovery issue for IKEv2 Auth policy when changed from PSK to PKI</td>
</tr>
<tr>
<td>CSCun33192</td>
<td>IOS SSL VPN: negation of ssl trustpoint cli</td>
</tr>
<tr>
<td>CSCun52538</td>
<td>existing IPsec proposals are deleted when anew tungrp is created via wiz</td>
</tr>
<tr>
<td>CSCup04598</td>
<td>Device has to be redeployed to change Crypto Map on Multi Topology</td>
</tr>
<tr>
<td>CSCup95990</td>
<td>Browser proxy: Incorrect cli when removing entry from the exception list</td>
</tr>
<tr>
<td>CSCuq25585</td>
<td>Activity Validation For Different Crypto Map Name of Multi Topology</td>
</tr>
</tbody>
</table>

### Resolved Caveats—Release 4.7 Service Pack 4

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.7 Service Pack 4.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuv33750</td>
<td>CSM fails to deploy with &quot;internal error&quot; when CSM user login credentials is selected</td>
</tr>
<tr>
<td>CSCux34671</td>
<td>Evaluation of vms for Java_December_2015</td>
</tr>
<tr>
<td>CSCuz52432</td>
<td>Evaluation of vms for OpenSSL May 2016</td>
</tr>
<tr>
<td>CSCuz85362</td>
<td>CSM 4.7 SP4 client installation issue on 32 bit server</td>
</tr>
</tbody>
</table>
Resolved Caveats—Release 4.7 Service Pack 3

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.7 Service Pack 3.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCut29478</td>
<td>CSM client memory leakage in javaw.exe process</td>
</tr>
<tr>
<td>CSCuv35928</td>
<td>CSM - Error &quot;Parent policy is locked&quot; when modifying inherited policies</td>
</tr>
<tr>
<td>CSCuv39677</td>
<td>Translated source shows &quot;,0&quot; value in Activity Report</td>
</tr>
<tr>
<td>CSCuu43022</td>
<td>CSM - Flex Config permissions with Terminal Services</td>
</tr>
<tr>
<td>CSCut87333</td>
<td>CSM 4.7cp2 ICMP does not support IPv6 Addresses</td>
</tr>
<tr>
<td>CSCut65297</td>
<td>CSM - unable to do packet-tracer with IPv6 addresses</td>
</tr>
<tr>
<td>CSCuu12847</td>
<td>CSM - ICMP IPv6 Support</td>
</tr>
<tr>
<td>CSCuu18236</td>
<td>CSM - ICMP IPv6 warning commands to line up with ASA</td>
</tr>
<tr>
<td>CSCuv26167</td>
<td>Evaluation of vms for OpenSSL July 2015 vulnerability</td>
</tr>
</tbody>
</table>

Resolved Caveats—Release 4.7 Service Pack 2

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.7 Service Pack 2.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCub97603</td>
<td>CSM should allow configuring a secondary IPv6 address on ASA interface</td>
</tr>
<tr>
<td>CSCur23742</td>
<td>CSM fails to deploy class-map when access-list is used</td>
</tr>
<tr>
<td>CSCut76507</td>
<td>CSM 4.8 CSM fails to deploy class-map when access-list is used</td>
</tr>
<tr>
<td>CSCut59655</td>
<td>Multi-context ASA discovery failing on 4.7</td>
</tr>
<tr>
<td>CSCus59205</td>
<td>CSM: IPS Licenses show &quot;Nonretrievable - Invalid username and password&quot;</td>
</tr>
<tr>
<td>CSCuq26685</td>
<td>Not able to edit a specific object-group in the CSM v 4.5</td>
</tr>
<tr>
<td>CSCut07447</td>
<td>CSM 4.7 CP2: CSM sending &quot;no speed nonegotiate&quot; for fiber interface</td>
</tr>
<tr>
<td>CSCus42723 (CSCut45947)</td>
<td>OpenSSL PSIRT</td>
</tr>
<tr>
<td>CSCut22499</td>
<td>Incorrect delta changes for CSM deployment to ASR</td>
</tr>
<tr>
<td>CSCut60126</td>
<td>Re-discovery fails on CSM after upgrade of ASA to 9.2(2)</td>
</tr>
<tr>
<td>CSCut03558</td>
<td>CSM 4.7: Preview configuration fails while parsing group-object</td>
</tr>
</tbody>
</table>

Resolved Caveats—Release 4.7 Service Pack 1

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.7 Service Pack 1.
<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCud11355</td>
<td>CSM Server needs to support TLS v1.2</td>
</tr>
<tr>
<td>CSCus82037</td>
<td>Support for &quot;http-only-cookie&quot; cli for ASA 9.2(3)</td>
</tr>
<tr>
<td>CSCur29069</td>
<td>Cisco Security Manager : evaluation of SSLv3 POODLE vulnerability</td>
</tr>
<tr>
<td>CSCus88379</td>
<td>CSM:- Import/Export perl script not working on non default HTTPS port</td>
</tr>
<tr>
<td>CSCus12592</td>
<td>CSM 4.7 support for ISE 1.3</td>
</tr>
<tr>
<td>CSCuq75832</td>
<td>CSM 4.7 Editing OSPF interfaces in device view</td>
</tr>
<tr>
<td>CSCup63069</td>
<td>CSM 4.6 Event Manager 'go to policy' fails for none Unified ACLs ASA 9.x</td>
</tr>
<tr>
<td>CSCuq30700</td>
<td>CSM pushing &quot;management-only&quot; on interfaces with a &quot;management&quot; alias</td>
</tr>
<tr>
<td>CSCup58780</td>
<td>CSM: Event Management/Viewer [PartitionPurgeRoutine] - Failed to delete</td>
</tr>
<tr>
<td>CSCup91495</td>
<td>CSM 4.6 HPM startup issue when VPN alerting is enabled</td>
</tr>
<tr>
<td>CSCuq01831</td>
<td>CSM: Event Viewer Error &quot;This operation cannot be performed&quot;</td>
</tr>
<tr>
<td>CSCul51205</td>
<td>Image Manager not using correct user credentials</td>
</tr>
<tr>
<td>CSCup91522</td>
<td>CSM 4.6 Additional Tunnels displayed when SNMP query to device fails</td>
</tr>
<tr>
<td>CSCuh52092</td>
<td>CSM 4.3SP1 : tomcat.exe spikes during change report generation</td>
</tr>
<tr>
<td>CSCup70309</td>
<td>CSM Inconsistency in shared policy access-rules.</td>
</tr>
<tr>
<td>CSCup28957</td>
<td>Ability to exclude line number changes from Activity Report</td>
</tr>
<tr>
<td>CSCur13055</td>
<td>CSM 4.7 removes ospf hello-interval and dead-interval settings</td>
</tr>
<tr>
<td>CSCup70029</td>
<td>CSM: Inspection Rule policy for Scansafe has no HTTPS</td>
</tr>
<tr>
<td>CSCup70098</td>
<td>CSM: Scansafe Inspection Rule policy have no changes in delta config</td>
</tr>
<tr>
<td>CSCuq64605</td>
<td>Event viewer shows incorrect event if sorts event</td>
</tr>
<tr>
<td>CSCup91482</td>
<td>ASA/FWSM:IPV6 ACL Removed on Discovery</td>
</tr>
<tr>
<td>CSCur08936</td>
<td>Unable to import policies in CSM 4.6</td>
</tr>
<tr>
<td>CSCul96691</td>
<td>Cmf Database engine service was disabled after a failed scheduled backup</td>
</tr>
<tr>
<td>CSCuq52900</td>
<td>CSM 4.6 SP1 Deploys wrong SNMPv3 password</td>
</tr>
<tr>
<td>CSCur54703</td>
<td>csm 4.7 and ospf redistribute static and metric-type 1</td>
</tr>
<tr>
<td>CSCup02863</td>
<td>CSM Preview config fails with &quot;network-object object null&quot; exception</td>
</tr>
<tr>
<td>CSCur82360</td>
<td>CSM: Unable to generate VPN reports after the upgrade</td>
</tr>
<tr>
<td>CSCur76940</td>
<td>Deployment report can't be generated in HTML format</td>
</tr>
<tr>
<td>CSCus14411</td>
<td>Validation error while applying interface role with override</td>
</tr>
<tr>
<td>CSCus19784</td>
<td>CSM deploys management-only under non-management interface</td>
</tr>
<tr>
<td>CSCur89878</td>
<td>CSM: ZBF deployment fails due to invalid access-group used in class-map.</td>
</tr>
<tr>
<td>CSCus43939</td>
<td>NoValueNetworkBBValidationLevel property throws error for unified rules</td>
</tr>
<tr>
<td>CSCuq56721</td>
<td>media-type does not exist in show run, causing CSM deployments to fail</td>
</tr>
<tr>
<td>CSCuq21511</td>
<td>Username From CertScript Policy View does not show the scripts properly</td>
</tr>
</tbody>
</table>
## Resolved Caveats—Release 4.7

The following customer found or previously release noted caveats have been resolved in this release.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCse93193</td>
<td>Add VPN-PKI enhancement for terminal enrollment</td>
</tr>
<tr>
<td>CSCsl42198</td>
<td>address-pool under ASA user-group is not supported + other enhancements</td>
</tr>
<tr>
<td>CSCsy95299</td>
<td>Banner motd first empty line can not be removed</td>
</tr>
<tr>
<td>CSTtb17772</td>
<td>CSM: ENH To detect changes and import just the changes.</td>
</tr>
<tr>
<td>CSTtb68104</td>
<td>ENH: Notify user when they modify a shared object in CSM</td>
</tr>
<tr>
<td>CSTtg54222</td>
<td>Eventing Restore: Restore failing or partially succeeding in some cases</td>
</tr>
<tr>
<td>CSCud93498</td>
<td>CSM 4.3-SSLVPN Missing the option to configure the parameters for SSO</td>
</tr>
<tr>
<td>CSCud93515</td>
<td>CSM 4.3 - VPN - ip/network missing for smart tunneled application config</td>
</tr>
<tr>
<td>CSCuh31093</td>
<td>ENH: CSM needs to be able to create &quot;username_from_cert.xml&quot; file</td>
</tr>
<tr>
<td>CSCuh53309</td>
<td>dmgtd.exe causes bluescreen on the CSM Server</td>
</tr>
<tr>
<td>CSCui60252</td>
<td>CSM 4.3 Misleading Information in Common Services</td>
</tr>
<tr>
<td>CSCui94177</td>
<td>CSM 4.4 does not support &quot;time-range&quot;</td>
</tr>
<tr>
<td>CSCuj59706</td>
<td>CSM 4.4 deploys IOS NTP configuration in worng command order</td>
</tr>
<tr>
<td>CSCuj65553</td>
<td>CSM 4.5 Installation Command Buttons appear garbled</td>
</tr>
<tr>
<td>CSCuj65593</td>
<td>CSM 4.5 Installation Button Appears Garbled</td>
</tr>
<tr>
<td>CSCui70104</td>
<td>CSM does not properly disable isakmp keepalives</td>
</tr>
<tr>
<td>CSCum03347</td>
<td>CSM: Deployment Validation Fails if ASA nameif Contains &quot;(&quot; or &quot;)&quot; Chars</td>
</tr>
<tr>
<td>CSCum61701</td>
<td>CSM 4.4 Activity and Ticket field cannot be altered independently</td>
</tr>
<tr>
<td>CSCum87972</td>
<td>Can't execute backup on CSM4.4SP1</td>
</tr>
<tr>
<td>CSCum91828</td>
<td>Security Notification:Event Archival-Event data deleted before archival</td>
</tr>
<tr>
<td>CSCum92428</td>
<td>CSM should handle NPE in ServiceSplitter.java</td>
</tr>
<tr>
<td>CSCun00643</td>
<td>CSM reports hitcounts not for all ACE in FWSM</td>
</tr>
<tr>
<td>CSCun04177</td>
<td>CSM 4.5 does not report hitcount for some ACE with obj-group on ASA</td>
</tr>
<tr>
<td>CSCun05594</td>
<td>HPM statuses not showing proper device states in Config Manager</td>
</tr>
<tr>
<td>CSCun06578</td>
<td>CSM Event Viewer hangs for several hours.</td>
</tr>
<tr>
<td>CSCun13807</td>
<td>CSM trying to negate unmanaged VPN config</td>
</tr>
<tr>
<td>CSCun14649</td>
<td>OSPFv3: Add Range and Virtual Link Table Empty on GUI</td>
</tr>
<tr>
<td>CSCun29381</td>
<td>CSM 4.5: Raw ACE table content does not match with the selected ACL</td>
</tr>
<tr>
<td>CSCun36357</td>
<td>CSM: Cannot login to Client App After Upgrading to 4.5+</td>
</tr>
<tr>
<td>CSCun48049</td>
<td>Support of dhcprelay server per interface on ASA</td>
</tr>
<tr>
<td>CSCun55888</td>
<td>CSM does not deploy changed Network object name in Shared policy</td>
</tr>
<tr>
<td>CSCun65303</td>
<td>CSM 4.5 - Warnings related to IOSMethodType when deploying on ASA</td>
</tr>
<tr>
<td>CSCun94866</td>
<td>Security Manager: CSM fails to find unused objects for all policy types.</td>
</tr>
<tr>
<td>CSCuo03654</td>
<td>CSM 4.5 Wrong src/dst address ACEs show up in &quot;Show HitCount Details&quot;</td>
</tr>
</tbody>
</table>
Resolved Caveats—Releases Prior to 4.7

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

Where to Go Next

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Security Manager server or client software.</td>
<td>See <em>Installation Guide for Cisco Security Manager 4.7</em>.</td>
</tr>
<tr>
<td>Understand the basics.</td>
<td>See the interactive JumpStart guide that opens automatically when you start Security Manager.</td>
</tr>
<tr>
<td>Get up and running with the product quickly.</td>
<td>See “Getting Started with Security Manager” in the online help, or see Chapter 1 of <em>User Guide for Cisco Security Manager 4.7</em>.</td>
</tr>
<tr>
<td>Complete the product configuration.</td>
<td>See “Completing the Initial Security Manager Configuration” in the online help, or see Chapter 1 of <em>User Guide for Cisco Security Manager 4.7</em>.</td>
</tr>
<tr>
<td>Manage user authentication and authorization.</td>
<td>See the following topics in the online help, or see Chapter 7 of <em>Installation Guide for Cisco Security Manager 4.7</em>.</td>
</tr>
<tr>
<td>Bootstrap your devices.</td>
<td>See “Preparing Devices for Management” in the online help, or see Chapter 2 of <em>User Guide for Cisco Security Manager 4.7</em>.</td>
</tr>
</tbody>
</table>

Product Documentation

For the complete list of documents supporting this release, see the release-specific document roadmap:

- *Guide to User Documentation for Cisco Security Manager*
  Lists document set that supports the Security Manager release and summarizes contents of each document.
- For general product information, see:
  - [http://www.cisco.com/go/csmanager](http://www.cisco.com/go/csmanager)

Obtain Documentation and Submit 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 “Product Documentation” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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.

© 2015 Cisco Systems, Inc. All rights reserved.