# Release Notes for Cisco Security Manager 3.3

**Revised: September 27, 2010**

**Note** Do not use this version of Security Manager to manage ASA 8.3 devices. This version of Security Manager configures ASA 8.3 devices in downward-compatibility mode, meaning that the device configuration does not use the new features introduced in version 8.3. Because of the extensive changes introduced with version 8.3, it is not downwardly-compatible with older ASA releases. If you want to manage ASA 8.3 devices with Security Manager, you must upgrade to Security Manager 4.0.

# Introduction

**Note** This document is to be used in conjunction with the documents listed in Related Documentation, page 19. 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. For more information about specific changes, please see Where To Go Next, page 18.

This document contains release note information for the following:

- **Cisco Security Manager 3.3 (including Service Packs 1 and 2)**

  Cisco Security Manager (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, and some services modules for Catalyst 6500 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.

  Security Manager supports multiple configuration views optimized around different task flows and use cases.

**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

- **Auto Update Server 3.3**

  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.

  To manage the devices in Security Manager, you must provide the device identity and the AUS information when you add a device. Security Manager uses the device identity information to retrieve the device IP address from an AUS that can be reached.

**Note** Before using Cisco Security Manager 3.3, we recommend that you read this entire document. In addition, it is critical that you read the "Important Notes" section on page 6, the "Installation Notes" section on page 4, and the *Installation Guide for Cisco Security Manager 3.3* before installing or upgrading to Cisco Security Manager 3.3.

This release note document includes ID numbers and headlines for each known problem identified in the document and a description of each. 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 Bug Toolkit. The release note enclosure contains symptoms, conditions, and workaround information.

# What's New

### Cisco Security Manager 3.3 Service Pack 2

Security Manager 3.3 Service Pack 2 provides support for changes to the mechanism used for downloading sensor and signature updates from Cisco.com.

Additionally, Security Manager 3.3 Service Pack 2 provides fixes for various problems. For more information, see Resolved Problems in Security Manager 3.3 Service Pack 2.

### Cisco Security Manager 3.3 Service Pack 1

Security Manager 3.3 Service Pack 1 provides fixes for various problems. For more information, see Resolved Problems in Security Manager 3.3 Service Pack 1.

### Cisco Security Manager 3.3

The following changes have been made for Security Manager 3.3:

- Support added for IPS 6.2 and 7.0. However, Security Manager does not support IPv6 capabilities. For more information, see the *User Guide for Cisco Security Manager 3.3* or the Security Manager online help.
- Support for the following Cisco IOS Software releases: 12.4(15)T, 12.4(20)T, 12.4(22)T, 12.4(24)T.
- Support added for the following ASA software releases: 8.1(2), and 8.2(1).
- Support added for the following FWSM software releases: 3.1(9-14), 3.2(4-10), and 4.0(2-4).

**Note** For complete device support information, including new releases supported in downward compatability mode, see *Supported Devices and Software Versions for Cisco Security Manager 3.3*.

- Support added for the Cisco Intrusion Prevention System Network Module (NME), which can be used in select integrated services routers. The router policy used to configure this module and the related Cisco Intrusion Prevention System Advanced Integration Module (AIM) has been renamed the IPS Module interface settings policy (in previous releases it was named the AIM-IPS interface settings policy).
- Support added for the Cisco ASA Advanced Inspection and Prevention Security Services Card SSC-5 (for use with ASA 5505 devices only).
- Support added for the Cisco Catalyst 6500 Series VPN Services Port Adapter (VSPA). This includes support for Cisco IOS Software release 12.2(33)SXI.
- Support added for the following Cisco 800 Series Integrated Services Routers: 861, 861W, 881, 887, 888SRST, 891, 892.
- Support added for the Cisco ASR 1000 Series Aggregation Services Routers, models 1002, 1004, and 1006, and the Cisco IOS Software versions they run: 12.2(33)XNA, XNB, and XNC. Support is limited to the following Cisco IOS XE Software consolidated packages: Advanced IP Services, Advanced Enterprise Services. The IP Base packages are not supported.
- Support added for Cisco Configuration Engine 3.0, which you can use for managing configuration deployments. You can no longer use lower versions of Configuration Engine.
- You can now export information to a comma-separated values file for the following IPS policies and features: signature policies, event action filters, event action overrides, and IPS licenses.
- Botnet Traffic Filter supported on ASA version 8.2+, providing monitoring of network ports for rogue activity and detection of infected internal endpoints sending command and control traffic to external hosts.
- You can now configure zone-based firewall policies for IOS devices running 12.4(6)T or higher. With zone-based firewalls, you can configure drop, pass, inspect, and web-filtering actions based on security zones, which are groups of interfaces, rather than configuring policies for each interface.
- You can now configure Cisco Express Forwarding (CEF) using the CEF interface settings policy for routers.
- The Advanced Settings interface settings policy for routers now allows you to configure the following features:
  - Interface throughput delay, which some routing protocols can use to determine the best path.
  - Maintenance Operation Protocol (MOP).
  - Unicast reverse path forwarding (RFP), which can be used to prevent denial of service (DoS) attacks.
- IKE Proposal objects now allow you to configure Diffie-Hellman groups 14, 15, and 16.
- You can now do the following with deployment schedules:
  - You can discard schedules in non-Workflow mode. In either Workflow or non-Workflow mode, discarded schedules are immediately removed from the table rather than staying until the purge date has passed.
  - You can now edit active schedules in Workflow mode (something you can already do in non-Workflow mode). In Workflow mode, and edited schedule changes to the Edit status, and you must resubmit and approve it.
  - Configuring an end date is now optional. You can define a schedule that runs indefinitely.

- When you create deployment jobs, changed devices are now organized in the device groups you have configured, if any, and you can select devices by selecting the group rather than individual devices. This makes it easier for you to select subsets of devices for a deployment job when you are managing a large number of devices and you want to create smaller deployment jobs to target specific groups of devices.
- A new inventory file comma-separated values (CSV) format is available for importing and exporting the device inventory. The new format, Cisco Security Manager, is equivalent to the CiscoWorks Common Services Device Credential Repository (DCR) format with some additional fields. The additional fields allow you to import the inventory without doing device discovery, so that you can add devices that are not currently active on the network.
- A Perl command is now available for importing or exporting network/host, service, and port list policy objects. The exported information includes device-level overrides for the objects.
- Security Manager backups are now automatically compressed, reducing the space used by backup files.
- Support for the Crypto Connect Alternate feature on Catalyst 6500/7600 devices running Catalyst OS 12.2(33)SXH or higher.
- Support for the following features on ASA 8.2: Double Authentication, SSL VPN Shared Licenses, and AnyConnect SSL VPN Client.
- Support for Dynamic Virtual Template Infrastructure (DVTI) in a hub-and-spoke Easy VPN topology on routers running IOS version 12.4(2)T and later, except 7600 devices.
- Support for Group Encrypted Transport VPN (GET VPN), which introduces the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing.
- Support for Generic Routing Encapsulation (GRE) tunneling protocol, which encapsulates a variety of protocol packet types inside IP tunnels, creating a virtual point-to-point connection to devices at remote points over an IP network. GRE can be configured on Cisco IOS security routers and Catalyst 6500/7600 devices in hub-and-spoke, point-to-point, and full mesh VPN topologies.
- When configuring IPS update servers, you can configure the proxy server to use NT LAN Manager (NTLM) V2 authentication as well as the already supported basic, digest, and NT LAN Manager (NTLM) V1 authentication. NTLM V2 is the most secure scheme.

# Installation Notes

You can install Security Manager 3.3 server software directly, or you can upgrade the software on a server where Security Manager is installed. The *Installation Guide for Cisco Security Manager 3.3* 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 3.3 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. For instructions, see “Upgrading Server Applications” in the *Installation Guide for Cisco Security Manager 3.3*.

For the *Installation Guide for Cisco Security Manager 3.3*, go to the list of Cisco Security Manager installation and upgrade guides on Cisco.com.

### Service Packs

Service packs cannot be installed by themselves. They are intended for installation on an existing installation of Cisco Security Manager 3.3. For more information, see Service Pack 2 Download and Installation Instructions, page 5.

If you have installed any service packs on your server and you restore a database that was backed up prior to installing those services packs, you must reapply the service packs after restoring the database.

# Service Pack 2 Download and Installation Instructions

Service pack 2 is a cumulative update that also includes the updates that were found in service pack 1. You can apply Cisco Security Manager 3.3 Service Pack 2 to a Cisco Security Manager 3.3 installation whether that installation has service pack 1 installed or not.

**Step 1** Go to http://www.cisco.com/go/csmanager, and then click **Download Software** in the Support box 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 (CSM) Software**, expand the **3.3** folder under All Releases, and then click **3.3sp2**.

**Step 4** Download the file fcs-csm-330-sp2-win-k9.exe.

**Step 5** To install the service pack, close all open applications, including the Cisco Security Manager Client.

**Step 6** Manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

**Step 7** Run the fcs-csm-330-sp2-win-k9.exe file that you previously downloaded.

**Step 8** In the Install Cisco Security Manager 3.3 Service Pack 2 dialog box, click **Next** and then click **Install** in the next screen.

**Step 9** After the updated files have been installed, click **Finish** to complete the installation.

**Step 10** 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.** 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 11** (Optional) Go to the client installation directory and clear the cache, for example, <Client Install Directory>/cache.

# Important Notes

- You can use IPv4 addresses only in Security Manager. Although some of the device software Security Manager supports allows you to use IPv6 addresses on commands, Security Manager does not support IPv6 addresses directly. If you want to configure IPv6 features using Security Manager, you can use FlexConfig policies.
- If you upgrade from a release earlier than 3.3 to Security Manager 3.3, and you use Cisco Configuration Engine, you must upgrade Configuration Engine to 3.0 at the same time. Security Manager 3.3 does not work with older versions of Configuration Engine.
- With the introduction of AUS 3.2.2, the CNS Event Gateway feature is no longer supported. As a result, IOS devices will not be managed by AUS. When you upgrade Security Manager with AUS—both inline and restore-based—all IOS devices that were previously linked with AUS will appear as not linked. Use Cisco Configuration Engine with Cisco IOS devices. Note that Configuration Engine does not support interactive commands. Keep in mind that you cannot discover policies on devices that use Configuration Engine in call home mode, although you can discover those running in event-bus mode.
- In IOS 12.3(14)T, many of the predefined inspection protocols were introduced; however, certain commands are not generated if inspection rules configured in Security Manager conflict with port definitions of predefined inspection protocols.
- 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 Security Manager 3.3. If you deploy back to the device, these commands are removed from the device because the commands 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 the Security Manager GUI 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.
- If you changed the HTTP or HTTPS port number on your Security Manager server to any port number other than the default value, connection to the server from the Security Manager client fails because the client tries to contact the server using the default port values. In Security Manager, two properties, HTTP_PORT and HTTPS_PORT, can be added to the client.info file located in the ..\Cisco Systems\Cisco Security Manager Client\jars folder on your client system to configure the port numbers you configured on your server. Add the following lines to the client.info file after opening it in a text editor such as Notepad and save the changes:

  ```
  HTTP_PORT=<port_number>
  HTTPS_PORT=<port_number>
  ```

  When you start the client the next time, it uses the updated port numbers, based on the protocol selected, to communicate with the server.
- For the Cisco Security Monitoring, Analysis, and Response System Appliance (CS-MARS) cross-launch panel to appear on the Cisco Security Manager Suite home page, you need to manually register the CS-MARS appliance on the Common Services application registration page. To do this, perform the following:

  1. From the Cisco Security Manager Suite home page, click the **Server Administration** link. The Common Services Admin page appears.
  2. Select **HomePage Admin > Application Registration**. The Application Registrations Status page appears.

3. Click **Register**. The Choose Location for Registrations page appears.
4. Select **Register From Templates**, then click **Next**.
5. Select **Monitoring, Analysis and Response System**, then click **Next**.
6. Enter the server name, server display name, and port and protocol information for the CS-MARS appliance, then click **Next**.
7. Verify registration information, then click **Finish**. The CS-MARS launch point will now appear from the Cisco Security Manager Suite home page.

**Note** If you choose to add the cross-launch to CS-MARS later, simply launch your web browser and enter http://*SecManServer*:1741, where *SecManServer* is the name of the computer where Cisco Security Manager Suite is installed. If you are using SSL, the default URL is https://*SecManServer*:443.

- 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.
- Avoid connecting 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.
- With the release of the S227 signature update on May 12, 2006, the minimum required version for 5.x signature updates was incremented from IPS version 5.0(5) to 5.0(6). Sensors running IPS 5.x software versions earlier than the minimum required version will fail until the sensor is upgraded to the supported level. Note that the minimum required version for 5.x signature updates is generally set to the latest available service pack within 30 to 45 days of that service pack's release.

**Caution** If you did not set Category CLI commands on your IOS IPS device to select a subset of IPS signatures that the device will attempt to compile, Security Manager will push CLI commands to enable the IOS IPS Basic category to prevent the device resources from being overloaded. These CLI commands are not managed by Security Manager after they are deployed. You can change these manually on the device to select another set of signatures to compile.

# Resolved Problems

- Table 1 contains problems resolved by Security Manager 3.3 Service Pack 2.
- Table 2 contains problems resolved by Security Manager 3.3 Service Pack 1.
- Table 3 contains problems that were resolved in Security Manager 3.3.

***Table 1 Resolved Problems in Security Manager 3.3 Service Pack 2***

| |
|---|
| **CSCtf02795—Deployment & preview gets stuck in DDP GPLDiff infinite loop.** |
| **CSCte83575—Network Object Import Does Not Correctly Import Nested Objects.** |
| **CSCtf23981—IPS-lic Autoupdate makes dev dirty & option to set time to download.** |
| **CSCte81211—Network Object Import Does Not Correctly Handle Network Range.** |

*Table 2 Resolved Problems in Security Manager 3.3 Service Pack 1*

| |
|---|
| CSCsz46172—CSM Client stuck in Initializing. |
| CSCsz58009—Validation fails with stack overflow on discovery of more IPS sig tuning. |
| CSCsz87296—Deployment on IPS/IOS-IPS deletes tunings for retired\enabled sometime. |
| CSCta30810—Failover: Physical interface issue with mac address table. |
| CSCta62887—CSM 3.3 cannot deploy "logging facility" on older PIX versions. |
| CSCta69399—CSM incorrectly handles '\t' when parsing configuration in the database. |
| CSCta83590—CSM 3.3 'no monitor-interface' ASA base license deployment failure. |
| CSCtb18465—Discovery fails for ASR router running 2.3.0t/2.3.1t images. |
| CSCtb25271—Changing VPN credentials override marks all devices using policy dirty. |
| CSCtb28203—[Failover]Interface Policy default of CSM is different from ASA for FO. |
| CSCtb54928—CSM 3.3 Can't deploy "failover polltime interface without holdtime. |
| CSCtb57280—[Failover]Deployment Fails in case of Active/Active Failover. |
| CSCtb59633—CSM-Mars Crosslaunch fails for IPS with MARS 6.0.4. |
| CSCtb62827—CSM3.3: InspectMapsPlugin fail to generate raw configlets on deploy. |
| CSCtb67715—CSM deploys transform-set after dynamic map configuration. |
| CSCtb72572—CSM 3.3 - cannot add PIX 6.3 anymore as a spoke in Ezvpn topology. |
| CSCtb75312—Hit Count - Hit Count Internal Failure error. |
| CSCtb81733—CSM discovery of EzVPN with certificates chooses wrong tunnel-group. |
| CSCtb82527—CSM tries to deploy pre-shared key for certificate based EzVPN topology. |
| CSCtb84188—CSM - crypto map is missing when deploying to AUS. |
| CSCtc16352—ADMIN cannot change config after READ ONLY user's unprivileged access. |
| CSCtc53926—CSM - deploys "authorization-dn-attributes UID" in the tunnel group. |
| CSCtc53954—CSM - certificate map - config might not be discovered in some cases. |
| CSCtc55916—BB Activity0 cache corrupted during Router Validation. |
| CSCtc56419—CSM - Policy view- logging setup returns an error. |
| CSCtc70513—Deployment failing with unmanaged plug-ins. |
| CSCtc78040—Wrong Default value is populated for Primary DN field. |
| CSCtc81240—CSM negates IP Pool if its associated to ISAKMP Pol. |

*Table 3 Resolved Problems in Security Manager 3.3*

| |
|---|
| CSCsd39283—Deployment fails on no allocate-interface command in ASA/PIX70 multimode<br><br>**Description:** If you deallocate a subinterface from a security context and delete it from the interface table, deployment fails on PIX 7.x and ASA devices in multiple context mode. |
| CSCse47710—Warning to change admin context should note connection loss<br><br>**Description:** Changing the admin context in multi- or mixed mode causes the connection between Security Manager and the device to be lost. |
| CSCsi51062—ASA5505: Deployment fails for mgmt-only option set with four named interfaces configured<br><br>**Description:** On an ASA 5505 device that has four interfaces configured using nameif, if you select the Management Only option for an interface that has backup interface configured, deployment to the device fails. |

*Table 3 Resolved Problems in Security Manager 3.3 (continued)*

**CSCsj36889—Deploy may fail after deleting a subinterface included in failover table**

**Description:** Deployment may fail after deleting a subinterface included in the Failover monitor table.

**CSCsl10243—Installer: Back button not working in system requirements window**

**Description:** On the System Requirements screen of the Security Manager installation, the Back button does not return you to the previous step.

**CSCsm13522—Deployment fails when creating a new management subinterface**

**Description:** On an ASA in transparent mode, an error may occur if you add a "Management Only" subinterface before configuring the "Management Only" interface.

**CSCsm52323—EA: Discovery/Deploy fails if device has multiple rows for a target value**

**Description:** Discovery fails for a device that has more than one row for a target value such as "high." Deployment from Security Manager to a device that has out-of-band changes fails, too. Removing one entry from the device lets both operations succeed.

**CSCsm65179—ASA ssl certificate-authentication interface cmd negated after discovery**

**Description:** If you discover configuration from an ASA device running 8.0(3) that contains the s**sl certificate-authentication interface outside port 443** command and remote access VPN policies, the command is changed to the **no** form when you preview the configuration.

**CSCsm79773—Default privilege for "aaa accounting command <tacacs+server-tag>" wrong**

**Description:** After import/discovery of a security appliance on which Accounting enabled but no Privilege Level set, the default Privilege Level is 1; it should be zero.

**CSCso17645—No validation error thrown when Interface assigned to VS are not created**

**Description:** This defect is seen after copying a virtual sensor policy, with interfaces assigned to the VS, from one IPS sensor to a second sensor of the same model. If the user unassigns the interface policy on the second sensor, and then submits and deploys, deployment fails but no validation error is thrown.

**CSCsq72376—Remote Access VPN - Changing Port Forwarding causes deployment error**

**Description:** If you change Port Forwarding for a deployed Dynamic Access policy from Auto-start to Disable, or from Enable to Disable, incorrect commands are deployed to the device; the subsequent deployment will fail.

**CSCsr07281—CCO not def & select download, applied and deploy cause no dep job crea**

**Description:** This problem occurs when the user leaves the Cisco.com or proxy server settings empty and schedules auto Download, Apply, and Deploy for selected devices. Cisco Security Manager does not check CCO or proxy server settings before allowing user to configure Auto deploy to device.

**CSCsr16722—ACS is not successfully re-registered during upgrade from 3.2 to 3.2.1**

**Description:** When upgrading from Security Manager 3.2 to 3.2.1, the Security Manager component is not successfully re-registered with the ACS server.

**CSCsr21222—IPS devices that fail deployment cannot deploy tuning to devices**

**Description:** When Security Manager fails to push a signature package to an IPS device in a deployment job because of an expired license or a device timeout, subsequent signature tuning deployments also fail.

**CSCsr30332—RAVPN - ASA Cluster Load Balance returns invalid hard validation error**

**Description:** Preview Configuration of a firewall configuration file containing invalid commands results in an error instead of a warning. In addition, the error message content is incorrect.

*Table 3 Resolved Problems in Security Manager 3.3 (continued)*

**CSCsr07721—When IPS auto update does not generate Change report correctly.**

**Description:** This problem occurs when the user clicks on the change report. The result is an error saying, "The changes you made for this activity are not available for viewing..." It happens for the activities/changes done as part of the IPS auto update.

**CSCsu29251—The default half connection timeout on the FWSM 3.2.4 is out of range.**

**Description:** The current default half connection timeout (the idle time after which a TCP connection is half-closed) for the FWSM 3.2.4 is 0:10:0, which is not in the valid range of 0:0:1 to 0:4:15. If you do not update the half connection timeout value, a validation error is generated.

**CSCsu96543—CSM generates extra delta for some default OSPF Interface, Logging, and Timeout configurations for PIX 8.0(4) devices.**

**Description:** This problem occurs when deploying other policies changes for PIX 8.0(4) device.

**CSCsw22048—CSAgent is not stopped automatically during inline upgrade**

**Description:** CSAgent cannot be stopped automatically due to a limitation within the application.

**CSCsw22788—NTP Servers with preferred value "True" are not discovered**

**Description:** During discovery, Cisco Security Manager will not recognize the NTP policies of a device that uses the 'prefer' keyword and also has source interface or authentication key defined.

**CSCsv60956—Job status for VS still shows "deploying" after sig update is done**

**Description:** This problem occurs after importing an IPS 6.0 device with a virtual sensor. After applying an IPS update and deploying the device, the deployment status for the virtual sensor is shown as "deploying" even after the deployment is successful.

**CSCsw24216—SSL VPN deploy to ASA 8.x fails when "Cache Compressed Content" is selected.**

**Description:** Deployment of SSL VPN settings to an ASA 8.x fails when Cache Compressed Content is selected on Remote Access VPN > SSL VPN > Other Settings: Performance tab.

**CSCsw29271—Security Manager overrides time zone and offset setting**

**Description:** If time zone settings are changed out of band after IPS device discovery, Security Manager overrides those settings during the next discovery.

**CSCsw38477—SSL VPN: CSD imported into File Repository with wrong path fails deploy**

**Description:** In CSM 3.2.2, SSL VPN deployment might fail with a "File IO error > Error while trying to access the file <downloaded_dir>\csd_3.4.0336.pkg." error, if CSD binary is changed. This error happens if you download a CSD image from CCO to an arbitrary location on the server and create a CSD resource (File BB) in CSM specifying this location.

**CSCsw39937—Device View does not display devices added after database restore**

**Description:** If you restore a database backup to a server running Security Manager, and the backup does not include the Security Manager database (for example, it includes AUS and CiscoWorks Common Services, or Performance Monitor and Common Services), the device tree might not appear in the Security Manager client.

# Known Problems

This section contains information about the problems known to exist in Cisco Security Manager 3.3. The known problems are arranged into the following tables.

**Note** 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 example provided, the known problem could be listed in either the Deployment table or the PIX/ASA/FWSM Configuration table.



## Device Management, Deployment, and Discovery

*Table 4 Device Management, Deployment, and Discovery*

| |
|---|
| **CSCsh94602—Lost Connectivity to System Context After Changing admin Credentials**<br>**Description:** If you change the credentials for the admin context when using HTTPS as the transport protocol, Security Manager cannot connect to the system execution space (for FWSM). Ensure that you define the same credentials for both the admin context and the system execution space when using HTTPS. |
| **CSCsy98103—Config-diff shows diff between two configs though they are exactly same.**<br>**Description:** If you discover a device, deploy it to file, view the configuration in the Configuration Archive window, and compare the configuration to the discovered configuration, the Config Diff Viewer might identify some differences because it does not consider comment lines when comparing the configurations. |
| **[1]CSCsz38530—Multiuser: device can be deleted while deploying changes**<br>**Description:** One user is able to delete a device from Security Manager while another user is deploying some changes to the same device. |
| **CSCsz81607—Last run entry not seen in Deployment Schedule on page refresh.**<br>**Description:** When you define deployment schedules, the schedules do not always generate jobs based on the hourly and daily schedule you define. |

1. New problem found in Security Manager 3.3.

# Diagnostics, Monitoring, and Troubleshooting Tools

*Table 5 Diagnostics, Monitoring, and Troubleshooting Tools*

**CSCsl94979—Device resolution for multiple-context FWSM fails during policy look-up**

**Description:** The disconnect between the Host Name field in the Device Properties page and the Host Name field in the policy page under the Device Admin section of Security Manager causes problems on FWSM blades with multiple contexts because a unique context cannot be identified during policy look-up from CS-MARS events.

**CSCsm50836—CS-MARS credentials retained in cache after changing authentication option**

**Description:** CS-MARS user credentials for events look-up are retained in the Security Manager cache even after you change the authentication mechanism to prompt the user for Security Manager credentials instead of CS-MARS credentials.

**CSCsm68564—Disabled rules not shown as inactive in read-only policy page in CS-MARS**

**Description:** When you look up a CS-MARS event generated by an access rule, disabled rules in the Security Manager rules table are not shown as inactive in the read-only policy query window.

**CSCsz35980—Performance Monitor: Alarms related to contexts are not deleted when device deleted**

**Description:** If you delete a multi-context FWSM and then add it again within four hours, some stale alarms that were not deleted with the device may be shown as events when the device is added again. However, these entries are removed from the database by the device table purger, which runs every four hours.

**CSCsz74628—Performance Monitor: Packet counters not updated in RA-VPN device page**

**Description:** When RA-VPN is configured on an 800-series router, Packets In and Packets Out counters are not accurate in Performance Monitor for any interface other than the first one defined.

**CSCsz74737—Performance Monitor: Site-to-site VPN charts updated with RA-VPN data.**

**Description:** Site-to-Site VPN charts on Summary > VPN page of Performance Monitor are updated with RA-VPN data.

**[1]CSCsz93991—Backup process takes nearly 2 hours if there is only 1 vCPU in VM image**

**Description:** When the user attempts to make a backup on a VM image that is deployed using 1 vCPU, the backup takes nearly 2 hours . This behavior is seen for the backups made from the CLI as well as backups made from Security Manager (Immediate backup and Scheduled Backup).

1. New problem found in Security Manager 3.3.

# Firewall Services

*Table 6 Firewall Services*

**CSCsc22934—ACL limitations on Layer 2 interfaces on IOS ISR devices**

**Description:** Deployment fails if access rules containing certain options are associated with Layer 2 interfaces on ISR routers.

**CSCsd60788—No port-map command generated if rules and predefined protocols conflict**

**Description:** IOS inspection **port-map** commands are not generated if inspection rules configured in Security Manager conflict with port definitions of predefined inspection protocols.

**CSCsk33350—Discovery of PAM Mappings with Inspection Rules is Incorrect**

**Description:** Port application mapping (PAM) commands are not associated correctly to the inspect rule on an IOS device during discovery.

*Table 6 Firewall Services (continued)*

**CSCsq75974—Static Rules ACL with Interface Source Are Not Discovered**

**Description:** If the device has a static rule referring to an access-list that uses an interface for source, Security Manager will not discover this static command.

**CSCsz53354—MAC Exempt List Must Be Orderable**

**Description:** Security Manager does not consider order for the MAC exempt list. Inserted entries are always added at the end.

# IPS and IOS IPS

*Table 7 IPS and IOS IPS*

**CSCsi47289—Policy object overridden at VS level is not deployed correctly**

**Description:** Policy object values are not deployed correctly if they are overridden at the virtual sensor level.

**CSCsm72033—Deployment Failed error on Event Action Rules**

**Description:** In the areas of Event Actions and Anomaly Detection, creating variables of the same name leads to Deployment errors.

**CSCsm89992—Deploy fails when version mismatch betn CSM and device**

**Description:** If the user creates a greenfield device, and the device has IPS metadata which is not registered in the Security Manager database, and then the user edits IPS policy and tries to deploy it to the device, deployment fails.

**CSCsm93970—Green field device Preview config does not show IPS pull down option**

**Description:** This defect occurs when a user creates a greenfield IOS IPS device, enables IPS, adds IPS policy, and previews it. The preview doesn't show the IPS drop-down option.

**CSCsm94535—COPY POLICY: Engine parameter not copied to IOS-IPS GreenField device**

**Description:** When copying from a live device at 12.4(15)T3 to a greenfield device at 12.4(11)T2, signature engine parameters are not copied.

**CSCso11145—CSM does not auto download IPS packages for Daily every 2 days**

**Description:** When IPS updates are scheduled to be downloaded with option set as “Daily” and every two days at a designated time, automatic download does not work at the correct intervals.

**CSCso11482—MultiContext not handled in ApplyIPSUpdate wizard upon SigEditParams**

**Description:** During IPS updates on IOS IPS devices, changes made in the Edit Parameters area are lost after deployment when more than one context is involved.

**CSCso17575—Intf Policy copy betn same IPS models but diff interface cards fails**

**Description:** For some IPS devices, including the IPS-4260, copying the interface policy from one device to an identical device fails when the interface configurations are different.

**CSCsr31140—Err loading pg if NTP policy from 6.1 dev is copied to 6.0/5.1 dev**

**Description:** “Error loading page” for the NTP page occurs if the user copies an NTP policy from an IPS device running 6.1.1 to an IPS device running 5.x or 6.0.4.

**CSCsr46030—Copy Interface & VS policy from a 6.1(1)E2 to 6.1(1)E2 fails**

**Description:** For IDSM devices running 6.1(1), virtual sensors cannot be copied.

**CSCsv59057—Sigupdate failed to an IOS device with NME module**

**Description:** Signature update on an IOS IPS device fails with the error “Signature update failed. Server internal error.”

*Table 7 IPS and IOS IPS (continued)*

**CSCsv85664—Security Manager swaps the name of the policies while deploying to device**

**Description:** This problem occurs after configuring Risk Category for all the virtual sensors in an IPS 6.1(1) device, and then editing the Event Action Rules, discovering, and deploying. Deployment sometimes exchanges the names of the rule profiles.

**CSCsv91055—Security Manager Deployment UI shows OOB for unsupported commands**

**Description:** For unsupported IPS commands, the deployment interface states that the changes are out of band.

[1] **CSCsx20448—IPS 6.2 unsupported devices should not be shown for Update**

**Description:** IPS auto-update applies an unsupported version to an older platform.

[1] **CSCsx33551—Rollback on IOS IPS Device Fails If SSH Is Not Enabled**

**Description:** Rollback from Configuration Archive and Deployment Manager fails for an IOS IPS device with the error message "Failed to communicate with device, Connection timed out," even though test connectivity is successful.

**CSCsx52318—CSM-IPS Editing service ports for signatures throws error**

**Description:** Editing service ports while doing a signature tuning throws an error - Invalid Values.

[1] **CSCsx93640—Rediscovery after OOB sigupdate does not update the virtual sensor**

**Description:** After rediscovery of an IPS sensor with a virtual sensor out-of-band signature update, the virtual sensor's signature level is not updated.

[1] **CSCsx98868—IOS IPS: Cannot deploy custom signature for "normalizer" engine**

**Description:** On IOS-IPS devices, when a Custom Signature with normalizer engine is deployed, it is not reflected on the device.

[1] **CSCsy03168—IOSIPS: SDEE properties cannot be discovered if SDEE is disabled**

**Description:** Although you configured the 3 SDEE properties with non-default values on a device where SDEE was disabled, after discovery Security Manager shows the default values for these properties.

[1] **CSCsy47123—Unable to unshared a shared policy for un-supported platform in dev view**

**Description:** Unassign the HTTP Proxy policy from device view might fail for devices that do not support the policy.

[1] **CSCsy47398—Rediscovery of Platform Settings Only Removes Virtual Sensors**

**Description:** Rediscovery of an IPS device results in the disappearance of the virtual sensor entries in the virtual sensors policy page and you get an error loading page when clicking on the virtual sensor policy in the table of contents.

[1] **CSCsy51377—Package download fails with error msg Download not enough space on disk**

IPS auto update or manual update fails with the error message:

Disk write error on file <filename>; not enough space on disk. Operation aborted.

[1] **CSCsy56978—IOS IPS version should be updated with changes in IOS version**

**Description:** The wrong "IPS Running OS Version" is shown for IOS IPS devices in device properties.

[1] **CSCsy60101—Signature Event Actions should be changed in GUI as per configured values**

**Description:** When you right-click on the Actions cell for a row in the Signature policy on an IPS device, the Add to Actions menu always shows the Deny Packet Inline and Produce Alert options even if those options are already selected for the signature.

[1] **CSCsy60393—Security Manager does not push "category ios_ips basic" command properly**

**Description:** Security Manager will not push "category ios_ips basic" CLI to the device. There are errors during deployment of IOS IPS configurations.

*Table 7 IPS and IOS IPS (continued)*

| |
|---|
| [1]**CSCsy89865—Not able to do signature update on IPS-4260 running 5.1(8)E2.9S342.0** |
| **Description:** You are unable to apply some signature update packages even though they are applicable for the device. The device is grayed out in the Apply IPS update wizard. |
| [1]**CSCsz33707—Licenses are not shown in IPS tab post ACS Integration without refresh** |
| **Description:** License status of the devices added after integrating Security Manager with ACS are shown as non-retrievable. |
| [1]**CSCsz35545—Pre-ACS integrated devices are shown in IPS updates page** |
| **Description:** Devices added to Security Manager before ACS integration are being shown in the IPS Auto Update page, however not in Device view. In addition, auto update on these devices is not being allowed. |
| [1]**CSCsz72119—AU: Sig update applied to dev with invalid lic when SP is also selected** |
| **Description:** Auto update Sig Update applied to a device with an invalid license when the service pack is also selected. |
| [1]**CSCsz72156—AU does not apply minor update if the dev is at lower Engine/Sig level.** |
| **Description**: This issue occurs when a sensor is at an engine level of E1 or E2 and the latest sensor package contains an E3 engine. |
| [1]**CSCsz58009—Validation fails with stack overflow on discovery of more IPS sig tuning** |
| **Description:** Unable to validate activity message is seen during activity validation. |

1. New problems found in Security Manager 3.3.

# PIX/ASA/FWSM Configuration

*Table 8 PIX/ASA/FWSM Configuration*

| |
|---|
| **CSCsd12592—Need to catch conflicting NAT commands during validation** |
| **Description:** Deployment fails for NAT commands and an error message states that the NAT command is a duplicate and was already defined on the device. |
| **CSCsd61906—PIX contact credentials (username/password) are deployed every time** |
| **Description:** After you configure your username, password, and privilege level on the Contact Credentials page, the information is sent to the device during every deployment. |
| **CSCse51450—OSPF validations are not adequate** |
| **Description:** Security Manager does not prevent certain invalid OSPF configurations from being discovered. |
| **CSCse59177—FWSM interface alias causes deployment to fail** |
| **Description:** Security Manager does not support interface alias for FWSM devices. If you try to configure interface alias on an FWSM, it might result in deployment failure for a security context. |
| **CSCsh20731—FAILOVER - Active/Active deploys to Standby unit and returns errors** |
| **Description:** When deploying to a virtual context that is designated for Failover group 2 (and subsequently becomes the Standby context on the Primary unit), numerous errors are returned for every command deployed. |
| **CSCsi09814—Configuration updates fail for CNS-managed PIX Firewall devices** |
| **Description:** Although Security Manager successfully deploys the configuration file to CNS, PIX Firewall devices configured to use CNS as the transport server cannot retrieve updates from CNS at the preset polling time and an error is entered in the device log file. |

*Table 8 PIX/ASA/FWSM Configuration (continued)*

**CSCsi19584—Removing an interface used in access rules can cause deployment to fail**

**Description:** Deployment to a firewall device (FWSM, ASA or PIX) might fail if an interface on that device has been deleted from within Security Manager when access rules still refer to that interface.

**CSCsi24397—SLA: needs add activity validation for interface roles**

**Description:** When an SLA monitor object is used in route tracking by static route, PPPoE, or DHCP, no commands for the SLA monitor are generated if the SLA monitor object references an interface role that cannot be resolved to a valid interface policy on the device.

**CSCsi33347—Auto-update: Changing order of AUS servers does not generate commands**

**Description:** On a 7.2 ASA/PIX with multiple AUS servers, changing the order of the AUS servers does not generate any commands.

**CSCsi42889—Swapping interface names causes deployment failure**

**Description:** Swapping interface names among the interfaces on a device causes a deployment to fail.

**CSCsi44546—RIP configuration commands in PIX/ASA 7.2(1) cannot be fully managed**

**Description:** RIP configuration commands in PIX/ASA 7.2(1) cannot be fully managed using Security Manager.

**CSCsl51451—Enable DHCPD auto configuration with interface option not discovered**

**Description:** The command `dhcpd auto_config` *`client_if_name`* `[[vpnclient-wins-override] interface` *`if_name`*`]` is not discovered by Security Manager. Keywords after *`client_if_name`* are not supported in Security Manager.

**CSCsm82107—Discovery of a multi-mode ASA added to CSM as a new device fails**

**Description:** After adding a new multiple-mode ASA to Security Manager, attempts to discover it fail, with an "Invalid device type or version" message.

**CSCsr17662—Deployment of ips command truncated if containing class map is changed**

**Description:** Security Manager does not currently support configuration of the `sensor <sensor_name>` portion of the `ips` command, although it will pass that portion through during initial deployment of a so-configured device. However, with `ips {inline | promiscuous} {fail-close | fail-open} sensor <sensor_name>` configured on a device, if the containing class map changes for any reason, Security Manager will redeploy only the `ips {inline | promiscuous} {fail-close | fail-open}` portion of the command.

# Router and Catalyst Switch Configuration

*Table 9 Router and Catalyst Switch Configuration*

**CSCsi20458—802.1x - Number of retries command not generated correctly**

**Description:** The **dot1x max-req value** command is generated at the global level of the device configuration instead of the interface level.

**CSCsi24091—Deploy fails if you change access to trunk mode & enable DTP negotiation**

**Description:** Deployment might fail when you attempt to modify the physical port configuration type from access to trunk mode for a Catalyst switch and keep the Enable DTP negotiation check box selected in the trunk port mode.

**CSCsi25845—PPP - No validation for multilink support on device**

**Description:** Deployment fails because PPP policy includes multilink commands that are not supported on the device.

*Table 9 Router and Catalyst Switch Configuration (continued)*

| |
|---|
| [1]CSCsy61195—Deployment Fails when Changing BGP AS Number on ASR Device<br><br>**Description:** Security Manager shows an error saying "BGP autonomous system 'xyz' already configured on the device'" for an ASR device when deploying a BGP configuration. |
| [1]CSCsz55274—Deployment to an ASR Fails when Configuring an Interface IP Address<br><br>**Description:** Deployment to an ASR device from Security Manager fails with error messages saying "Auto-negotiation is enabled. Speed cannot be configured." |

1. New problems found in Security Manager 3.3.

# Site-to-Site/Remote Access/SSL VPN Configuration

*Table 10 Site-to-Site/Remote Access/SSL VPN Configuration*

| |
|---|
| CSCsd84663—Deployment fails on Cat6k when changing VPNSM/VPN SPA slot/subslot<br><br>**Description:** If you change the slot or subslot of a VPNSM or VPN SPA blade on a Catalyst 6500/7600 device, either in a VPN topology that was deployed, or in an IPsec proposal that was assigned to the device in a remote access VPN and deployed, deployment fails when you try to redeploy the VPN topology or device.<br><br>For detailed workaround information, see the Workaround enclosure. |
| CSCsl20196—ACL object CLI generation should use object-groups when applicable.<br><br>**Description:** Cisco Security Manager currently does not use the discovered object-groups while configuring VPN protected networks. |
| CSCso63006—Discovery fails while trying to import a Regular IPSec VPN.<br><br>**Description:** This failure happens when an ACE is present which has an interface as source or destination. Do not use the interface as the source or destination. Use the host <ip-address> or object-group <group-name> instead. |
| CSCsq66815—Side-effects due to missing Protected Network's assignment usage info.<br><br>**Description:** The usage association is not shown for policy objects, such as ACLs, used in protected networks of a site-to-site VPN. This might result in not detecting ACL name conflict validations during validation. |
| CSCsv31933—CSM 3.2.2 migration: Onscrn kbd, internal pwd features set to default<br><br>**Description:** During migration to CSM 3.2.2, the onscreen keyboard and internal password features are set to their default settings in the ASA SSL VPN Other Settings policy, rather than what is configured on the device for these two features. This is applicable to only those ASA devices for which an SSL VPN policy was configured in CSM before migrating to CSM 3.2.2. |
| CSCsv98168—CSM: Static routing option on DMVPN generates incorrect routes on hub<br><br>**Description:** Security Manager deploys the following route on the hub(s) of a DMVPN with static routing: ip route (network behind spoke) Tunnel0. However, it should deploy the following route instead: ip route (network behind spoke) (tunnel IP of spoke). |
| [1]CSCsz11601—DVTI and EzVPN discovery issue occurs if secondary hub is configured.<br><br>**Description:** In an EzVPN topologies with DVTI configured, discovery of the VTI interface for the secondary hub is not supported. |
| [1]CSCsz74432—Assignment of shared VPN policies not working from Policy view.<br><br>**Description:** Assignment of shared policies does not work for VPN policies from Policy view. |

*Table 10 Site-to-Site/Remote Access/SSL VPN Configuration (continued)*

| |
|---|
| **CSCsz92007—CSM: Should allow semicolon delimiter in PKI certificate subject name.**<br>**Description:** Discovery of PKI certificate subject name on IOS devices is not discovered correctly if multiple PKI certificate subject names are separated by semicolons. |
| [1] **CSCsy83931—VPN policy discovery fails when tunnel source defined with IP address.**<br>**Description:** VPN policy discovery fails if a tunnel source is identified using its IP address instead of its interface name. This is applicable to all VPN topologies, for example, point-to-point, hub and spoke, and full mesh. |
| [1] **CSCsz60736—CSM not generating a workable configuration with unique tunnel source.**<br>**Description:** Security Manager does not generate workable VPN configurations when provisioning a GRE-based VPN topology in a unique tunnel source scenario. |
| [1] **CSCsz72524—DMVPN does not work even though spoke connectivity is selected.**<br>**Description:** Direct spoke-to-spoke communication does not work in a DMVPN topology. Spoke-to-spoke communication continues to happens through the hub, even though spoke-to-spoke connectivity is enabled. |
| [1] **CSCsz79453—CSM discovery fails when NAT IP address is configured with LPIT.**<br>**Description:** Site-to-site VPN discovery fails with this error: "Missing a valid crypto map on the device." |

1. New problems found in Security Manager 3.3.

# Where To Go Next

*Table 11 Where To Go Next*

| If you want to: | Do this: |
|---|---|
| Install Security Manager server or client software. | See the *Installation Guide for Cisco Security Manager 3.3*. |
| 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 the *User Guide for Cisco Security Manager 3.3*. |
| Complete the product configuration. | See "Completing the Initial Security Manager Configuration" in the online help, or see Chapter 1 of the *User Guide for Cisco Security Manager 3.3*. |
| Manage user authentication and authorization. | See the following topics in the online help, or see Chapter 2 of the *User Guide for Cisco Security Manager 3.3*.<br>• Setting Up User Permissions<br>• Integrating Security Manager with Cisco Secure ACS |
| Bootstrap your devices. | See "Preparing Devices for Management" in the online help, or see Chapter 5 of the *User Guide for Cisco Security Manager 3.3*. |
| Install entitlement applications. | Your Security Manager license grants you the right to install certain other applications—including specific releases of RME and Performance Monitor—that are not installed when you install Security Manager. You can install these applications at any time. See the Introduction to Component Applications section in Chapter 1 of the *Installation Guide for Cisco Security Manager 3.3*. |

# Related Documentation

Table 12 describes the product documentation that is available. For information on ordering printed documents, see Obtaining Documentation and Submitting a Service Request, page 20.

***Table 12 Product Documentation***

| Document Title | Available Formats |
|---|---|
| *Guide to User Documentation for Cisco Security Manager 3.3* | • Printed version included with product.<br>• PDF on the product DVD-ROM.<br>• Online document under Cisco Security Manager Documentation Roadmaps on Cisco.com. |
| *Installation Guide for Cisco Security Manager 3.3* | • PDF on the product DVD-ROM.<br>• Online document under Cisco Security Manager Install and Upgrade Guides on Cisco.com. |
| *User Guide for Cisco Security Manager 3.3* | • PDF on the product DVD-ROM.<br>• Online document under Cisco Security Manager End-User Guides on Cisco.com. |
| *Supported Devices and Software Versions for Cisco Security Manager 3.3* | Online document under Cisco Security Manager Compatibility Information on Cisco.com. |
| *FAQ and Troubleshooting Guide for Cisco Security Manager 3.3* | Online document under Cisco Security Manager Troubleshooting Guides on Cisco.com. |
| *Migrating from CiscoWorks VPN/Security Management Solution to Cisco Security Manager* | Online document under Cisco Security Manager Install and Upgrade Guides on Cisco.com. |
| *High Availability Installation Guide for Cisco Security Manager 3.3* | Online document under Cisco Security Manager Install and Upgrade Guides on Cisco.com. |
| *User Guide for Auto Update Server 3.3* | • PDF on the product DVD-ROM.<br>• Online document under Cisco Security Manager End-User Guides on Cisco.com. |
| *Supported Devices and Software Versions for Auto Update Server 3.3* | Online document under Cisco Security Manager Compatibility Information on Cisco.com. |
| *Security Manager Integration with ACS* | Online document under Cisco Security Manager Configuration Examples and TechNotes on Cisco.com. |
| *Release Notes for Cisco Security MARS Appliance 6.0.1* | Online document under Cisco Security Monitoring, Analysis and Response System Release Notes on Cisco.com. |
| Context-sensitive online help | Click the Help button in a window or dialog box. |

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation* on Cisco.com, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.