



Release Notes for Cisco Security Manager 3.2.2

Revised: August 4, 2009

Introduction



Note

This document is to be used in conjunction with the documents listed in [Related Documentation, page 22](#). The online versions of the user documentation are also occasionally updated after the initial release. As a result, the information contained in the *User Guide for Cisco Security Manager 3.2.2* 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 21](#).

This document contains release note information for the following:

- **Cisco Security Manager 3.2.2 (Including Service Packs 1, 2, and 3)**

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 Catalyst 6500/7600 services modules (FWSM, VPNSM, VPN SPA, and ISDM-2). 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.

- **Auto Update Server 3.2.2**

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.



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

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 3.2.2, we recommend that you read this entire document. However, it is critical that you read the [“Important Notes” section on page 5](#), the [“Installation and Upgrade” section on page 14](#), and the [Installation Guide for Cisco Security Manager 3.2.2](#) before installing or upgrading to Cisco Security Manager 3.2.2.

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 in Security Manager 3.2.2 (Including SP1, SP2, and SP3)

The following changes have been made for Security Manager 3.2.2 Service Pack 3:

- Support for TLSv1 and SSLv3 communication protocols.
- Security Manager 3.2.2 Service Pack 3 provides fixes for various problems. For more information, see [Table 1 Resolved Problems in Security Manager 3.2.2 Service Pack 3, page 8](#).

**Note**

A service pack is also available for Cisco Performance Monitor 3.2.2. For more information, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.2.2/installation/guide/pm322irn.html.

The following changes have been made for Security Manager 3.2.2 Service Pack 2:

- Support for AIM-IPS on 12.4(20).
- Security Manager 3.2.2 Service Pack 2 provides fixes for various problems. For more information, see [Table 2 Resolved Problems in Security Manager 3.2.2 Service Pack 2, page 9](#).

The following changes have been made for Security Manager 3.2.2 Service Pack 1:

- 10 gigabit interface support for IPS Sensor 4260, 4270.
- Sybase 3813 EBF is integrated with the SP1 installation.
- CSTM patch is available from Common Services and is integrated into Installation.
- Cisco Configuration Engine 3.0 support. (See [Important Notes, page 5](#).)
- Security Manager 3.2.2 Service Pack 1 provides fixes for various problems. For more information, see [Table 3 Resolved Problems in Security Manager 3.2.2 Service Pack 1, page 9](#).

The following changes have been made for Security Manager 3.2.2:

- Support added for FWSM 4.0(1) and IPS 6.1.
- Trusted Flow Acceleration available on the FWSM 4.0(1)+ in routed firewall mode, for single and multiple contexts.

- Logical “redundant” interfaces can now be configured on security devices. This feature is separate from device-level failover, but you can configure both if desired.
- Upgrade of included applications: CiscoWorks Common Services 3.2, RME 4.2, CSA 5.2, AUS 3.2.2, and Performance Monitor 3.2.2.



Note With the introduction of AUS 3.2.2, CNS Event Gateway is no longer supported. See [Important Notes, page 5](#).

- New Deployment administrative settings for masking passwords and keys when viewing.
- Support for non-English, non-ASCII languages in SSL VPN Bookmarks and SSL VPN Customization policy objects for use on ASA 8.x devices.
- Retention of client preferences.

Installation Notes

- You can install Security Manager 3.2.2 server software directly, or you can upgrade the software on a server where either Security Manager 3.1, 3.1.1, 3.2, 3.2.1 is installed. In addition to reading these installation notes, we strongly recommend that you refer to the [Installation Guide for Cisco Security Manager 3.2.2](#) for important information regarding server requirements, server configuration, and post-installation tasks.
- Before you can successfully upgrade to Security Manager 3.2.2 from a prior version of Security Manager (versions 3.1, 3.1.1, 3.2, or 3.2.1 only), 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 3.2.2](#).
- Service Packs: Service packs cannot be installed by themselves. They are intended for installation on an existing installation of Cisco Security Manager 3.2.2. For more information, see [Cisco Security Manager 3.2.2 Service Pack 3 Download and Installation Instructions, page 4](#).
- 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.

Cisco Security Manager 3.2.2 Service Pack 3 Download and Installation Instructions

Service pack 3 is a cumulative update that also includes the updates that were found in service packs 1 and 2. You can apply Cisco Security Manager 3.2.2 Service Pack 3 to a Cisco Security Manager 3.2.2 installation whether that installation has service packs 1 or 2 installed or not.

**Note**

The Cisco Security Manager 3.2.2 Sybase Patch has been integrated in Cisco Security Manager 3.2.2 Service Pack 3 and is no longer available as a standalone patch. If you have already installed the Sybase Patch, you can install Cisco Security Manager 3.2.2 Service Pack 3 on top of your patched 3.2.2 installation. However, you do not need to install the Sybase Patch before installing Service Pack 3.

**Note**

A service pack is also available for Cisco Performance Monitor 3.2.2. For more information, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.2.2/installation/guide/pm322irn.html.

-
- Step 1** To download the service pack, log in to Cisco.com.
- Step 2** Go to <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=280033778>.
- Step 3** Go to "Latest Releases" and click on 3.2.2sp3. The Security Manager image is seen on the right-hand side.
- Step 4** Download the file fcs-csm-322-sp3-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** Install the Security Manager 3.2.2 FCS build on your server if you have not already done so.
- Step 8** Run the fcs-csm-322-sp3-win-k9.exe file that you previously downloaded.
- Step 9** In the Install Cisco Security Manager 3.2.2 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.

**Note**

The Daemon Manager is automatically stopped and restarted during the installation process.

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

Cisco Security Manager 3.2.2 Download and Installation Instructions

To download and install Cisco Security Manager 3.2.2:

Step 1 Log in to Cisco.com.

Step 2 Go to <http://www.cisco.com/go/csmanager>, then click Download Software.



Note RME is not included in the downloadable version of the installation utility. For information on installing Resource Manager Essentials, please refer to the [Installation Guide for Cisco Security Manager 3.2.2](#).

Step 3 Download fcs-csm-322-win-k9.exe.



Note Save the installation utility on a disk that is local to your server. Installation cannot succeed over a network connection to a remote volume, even if installation seems to succeed.

Step 4 Run the file that you downloaded. The InstallShield Wizard extracts files to a temporary directory and checks their integrity while it constructs the Cisco Security Manager Setup application, which starts automatically.



Note For detailed installation instructions, refer to the [Installation Guide for Cisco Security Manager 3.2.2](#).



Tip

If an error message says the file contents cannot be unpacked, we recommend that you empty the Temp directory, scan for viruses, delete the C:\Program Files\Common Files\InstallShield directory, then reboot and retry.

Important Notes

- If you have made any changes to the DCS.properties file in the \CSCOpX\MDC\athena\config folder in the installation directory (usually C:\Program Files), you should make a backup of the file prior to applying service pack 3 and then reapply those properties after applying service pack 3.
- If you are installing Cisco Security Manager 3.2.2 SP1, SP2, or SP3 in a high-availability (HA) environment, you must manually copy the monitor.pl script from NMSROOT to VERITAS bin folder.

```
copy %NMSROOT%\MDC\athena\ha\agent\monitor.pl %VCS_HOME%\BIN\CSManager\bin\monitor.pl
```

for example,

```
copy C:\Program Files\CSCOpX\MDC\athena\ha\agent\monitor.pl
   C:\Program Files\Veritas\cluster server\bin\CSManager\monitor.pl
```

- Cisco Configuration Engine 3.0 is not backward-compatible to older versions of Cisco Configuration Engine. Therefore, you will need to migrate to Cisco Configuration Engine 3.0 to work with Security Manager 3.2.2 SP1, SP2, or SP3.
- 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. The workaround for this is to use the CNS Config Engine. However, Config Engine does not support interactive commands. Also IOS routers must be configured for event mode to work with Config Engine. Config Engine discovery will not be supported if the IOS routers are running on callhome mode.
- Interface names are not case-sensitive in Security Manager, although they are case-sensitive in a Cisco Security Monitoring, Analysis, and Response System Appliance (MARS appliance). For example, outside and Outside are considered exclusive by a MARS appliance, while they are equivalent in Security Manager. As a result, when you perform a query for a Security Manager policy from an event generated in MARS, an interface name logged in the syslog event might not match the interface name of that policy in Security Manager. Syslog messages use lowercase for all interface names. To work around this problem, use lowercase for all interface names and in the definition of interface roles in MARS.
- If the client system used to access the MARS GUI is not on the same side of the NAT boundary as the MARS appliance and the Security Manager server, you can perform policy lookup in read-only mode. However, you cannot start the Security Manager client from the read-only policy lookup table to modify matching policies. The client system must be on the same side of the NAT as the MARS appliance and the Security Manager if you want to start the Security Manager client from MARS to modify the matching policy.
- Security Manager client must be on the same side of the NAT boundary as the MARS appliance and the Security Manager server to query MARS events from policies.
- For a list of known problems in MARS related to policy table lookup from MARS syslogs and events lookup from Security Manager policies, see *Release Notes for Cisco Security MARS Appliance 4.3.4 and 5.3.4*. The known problems in Security Manager related to these features are documented in the [Diagnostics, Monitoring, and Troubleshooting Tools](#), page 12.
- 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.
- You might receive a persistent error message such as “Internal Error, please save the logs and contact TAC.” If this should occur, please select **Tools > Security Manager Diagnostics** and send the resulting CSMDiagnostics.zip file to the Technical Assistance Center.
- 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 3.2.2. 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 (MARS) cross-launch panel to appear on the Cisco Security Manager Suite home page, you need to manually register the 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 MARS appliance, then click **Next**.
 7. Verify registration information, then click **Finish**. The MARS launch point will now appear from the Cisco Security Manager Suite homepage.



Note If you choose to add the cross-launch to 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

Service Pack 3 is a cumulative release that contains all problem resolutions included in Service Pack 3, as well as those in Service Packs 1 and 2.

Service Pack 2 is a cumulative release that contains all problem resolutions included in Service Pack 1, as well as those in Service Pack 2.

- [Table 1](#) identifies the problems resolved by Security Manager 3.2.2 (Service Pack 3).



Note A service pack is also available for Cisco Performance Monitor 3.2.2. For more information, see http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.2.2/installation/guide/pm322irn.html.

- [Table 2](#) identifies the problems resolved by Security Manager 3.2.2 (Service Pack 2).
- [Table 3](#) identifies the problems resolved by Security Manager 3.2.2 (Service Pack 1).
- [Table 4](#) identifies the problems that were documented in the Security Manager 3.2.1 release notes as known problems and that have since been resolved. For information on resolved problems that were resolved in earlier releases, please refer to the release note document for each previous release.

Table 1 *Resolved Problems in Security Manager 3.2.2 Service Pack 3*

CSCsj38020 —CSM3.1 Request for optimization of shared access-list generation.
CSCsl40417 —Support ACL sharing based on ACL types
CSCsw44997 —Zone Based Firewall: Create Map and Override are not shown correctly in the Activity Report.
CSCsx16443 —Apache security issue with all versions of Security Manager.
CSCsx62933 —OSPF Area ID for ASA does not support larger integer value.
CSCsy70973 —Interface: More than two named interfaces cannot be added to an FWSM 4.0 context.
CSCsy92108 —Support for TLSv1, SSLv3 in GDCS.
CSCsz01218 —Security Manager 3.2.1 SP1 stuck in infinite loop while modifying SNMP attributes.
CSCsz28025 —Security Manager misinterprets acl optimization enable as ACL and tries to remove it.
CSCsz31773 —Logging list configuration might cause AUS deployment to fail.
CSCsz33220 —Save button is not working in Global Policy Tool (GPT) in policy view for VPN policies.
CSCsz46172 —CSM Client stuck in Initializing.
CSCsz50340 —Latest ASDM(6.1(3)F Launch for FWSM 3.x and 4.x.
CSCsz56288 —Security Manager builds invalid IP pools.
CSCsz63632 —User ID containing \a and \b are unable to generate activity reports.
CSCsz84331 —No switchport is applied to port channel interface incorrectly.
CSCsz84352 —Issues with Revert Uncommitted ACL.
CSCsz87296 —Deployment on IPS/IOS-IPS deletes tunings for Retired and Enabled.
CSCta30810 —Failover: Physical interface issue with mac address table.

Table 2 *Resolved Problems in Security Manager 3.2.2 Service Pack 2*

CSCsv21124	Security Mgr will not discover FWSM context with classmap set connection timeout.
CSCsv92606	Missing config in config archive.
CSCsw45916	Duplicate Sequence errors when deploying in Security Manager.
CSCsw48664	Tomcat StdOut.log has XML transactions logged by default.
CSCsw82040	Log files are not getting purged.
CSCsx12066	Submit activity prior to Deploy goes on for ever.
CSCsx17980	Security Mgr cannot deploy to ASA if failover is configured on redundant interface.
CSCsx26449	Policy Override does not display after creation.
CSCsx28354	TFTP service allows directory traversal.
CSCsx30135	Security Mgr changes mode to auto-commit when upload FW conf for device archive.
CSCsx31985	Security Manager cannot discover multiple context devices from DCR.
CSCsx37128	Error messages needed to update config if interface deleted.
CSCsx38735	CSM 3.2.2 cannot launch ASDM 6.1F for FWSM 4.x.
CSCsx44063	Deployment hangs if FWSM serial access is enabled.
CSCsx49206	Huge GP extra CLI generated after RAVPN discovery and then deploy.
CSCsx51721	Archived configs for IPS are not purged.
CSCsx58036	RAVPN Device Deployment failure after Upgrade of pix 7.0 to pix 8.0.
CSCsx58433	Security Manager should send "firewall transparent" first to FWSM context.
CSCsx94256	Validation Error: Multiple interfaces with overlapping subnets.
CSCsy16777	Discovery Fails when the Router is added as Dynamic Device.
CSCsy28368	Policy locking does not throw error notification for edit new rule.
CSCsy28383	Policy locking does not show notification in create new rule case.
CSCsy29468	Unable to add interface for new device type 5505.
CSCsy39879	Security Manager removes dap/xml from PIX.
CSCsy47244	Security Manager IPS packages not downloaded from CCO due to wrong credentials.
CSCsy47474	FWSM: Revert uncommitted ACLs.
CSCsy57546	Line number needed when FWSM is in manual commit mode.
CSCsy74914	Security Manager config deploy fails when using IKE-proposal with DH group 5.
CSCsy94660	Discovery of a 7.0 IPS device fails on CSM 3.2.2.

Table 3 *Resolved Problems in Security Manager 3.2.2 Service Pack 1*

CSCsq38017	Client login screen does not show SP1
CSCsq89150	Do not use clear nat command when pushing new NAT commands
CSCsu76329	AUS credential is shown in clear text in GUI
CSCsv43684	Import Rules fails with internal error
CSCsv52723	Preview Config takes 4 min inside activity and 50 sec outside activity
CSCsv70916	Performance: Unable to discover 1000 config files in one shot
CSCsv71934	Performance: Modification of objects with nested objects is slow

Table 3 *Resolved Problems in Security Manager 3.2.2 Service Pack 1 (continued)*

CSCsv97676 —Security Manager should truncate names longer than 40 characters
CSCsw26400 —Security Mgr Client loading takes a long time in multi-user environment
CSCsw28920 —Missing option for connection type on Edit Endpoints for Device screen
CSCsw29271 —Security Manager overrides timezone and offset setting
CSCsw33490 —Wrong delta for fixup protocol DNS causes removal of cli
CSCsw65764 —Unsupported commands are negated during deployment
CSCsw65986 —10 GB support for IPS4270 and IPS 4260 in Security Manager
CSCsw66334 —Performance issue in Static NAT Add Dialog
CSCsw67974 —Security Manager 3.2.2 cannot discover IPS 6.2.1
CSCsw75393 —Pushing Post-S364 SigUpdate to IOS IPS enabled router disables most Sigs
CSCsw77208 —Security Mgr 3.2.2 automatic failover not working on HA servers
CSCsw86478 —Deployment fails with error “Fail to create idconf object”
CSCsw96216 —Deployment fails with java heap space error
CSCsw98868 —Security Mgr saved changes not actually saved for interface duplex/speed
CSCsx34005 —LDAP authentication credentials for Ciscoworks are sent in clear text

[Table 4](#) contains problems that were resolved in Security Manager 3.2.2.

Table 4 *Resolved Problems in Security Manager 3.2.2*

CSCsr20046 —MCP: “Report->Remote Access->Users->Session report” missing for ASA
CSCsr20738 —De-assigning SSL VPN does not remove SSO and cache file-system commands
CSCsr24558 —Policy static with nested service policy object: preview throws error
CSCsr27295 —SSL VPN - Proxy PAC removed after HTTP/HTTPS Proxy Svr configuration
CSCsr27386 —SSL VPN - Error when assigning multiple bookmarks to DAPs
CSCsr28004 —Web Filter: Nested policy object - conflict is not detected
CSCsr41074 —HTTP Policy: Assigned policy includes server port for FWSM
CSCsr41654 —Add Devices from File causes error in deployment
CSCsr43613 —CSM 3.2/3.1 rollback on FWSM 3.2 removes admin context crypto key
CSCsu03884 —CSM 3.2, 3.2.1 : Auto-backup fails to work
CSCsu10185 —CSM:Mail notification may not work as expected for policy expiration
CSCsm98683 —Network Information policy OOB settings ignored, deploy always goes thru
CSCsr29999 —Enable one-way TCP reset option should not appear in CSM UI
CSCsr41557 —Unauth NTP negation happening for a 6.0.5E2 device
CSCsr45632 —Unable to deploy authenticated NTP if Unauth NTP configured on sensor

Known Problems

This section contains information about the problems known to exist in Cisco Security Manager 3.2.2. 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.

- [Catalyst 6500/7600 Configuration, page 11](#)
- [Device Management, Deployment, and Discovery, page 12](#)
- [Diagnostics, Monitoring, and Troubleshooting Tools, page 12](#)
- [Firewall Services, page 13](#)
- [Installation and Upgrade, page 14](#)
- [IPS and IOS IPS, page 14](#)
- [PIX/ASA/FWSM Configuration, page 17](#)
- [Router Configuration, page 19](#)
- [Site-to-Site/Remote Access/SSL VPN Configuration, page 20](#)

Catalyst 6500/7600 Configuration

Table 5 *Catalyst 6500/7600 Configuration*

CSCsi17582—Cannot change the data port VLAN running mode after negating CLI on IDSM

Description: Deployment fails when you attempt to change the running mode of the data port VLAN from Trunk (IPS) to Capture (IDS) from the IDSM Data Port VLANs dialog box and the following error message is displayed:

```
Command Rejected: Remove trunk allowed vlan configuration from data port 1 before configuring capture
allowed-vlans
```

CSCsi17608—Deployment fails when allowed VLAN ID is modified on IDSM capture port

Description: If you modify the allowed VLANs of an IDSM data port that has been configured as a capture port and deploy configurations to the device, the following error occurs:

```
"Capture not allowed on a SPAN destination port"
```

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.

Device Management, Deployment, and Discovery

Table 6 *Device Management, Deployment, and Discovery*

CSCse99139—Rediscovery of inventory alone can create device-override building blocks

Description: Device level overrides for policy objects corresponding to object groups can be created after discovering only the inventory policies like interfaces.

CSCsh94602—Lost Connectivity to System Context After Changing admin Credentials

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.

CSCsi09797—Job state for completed jobs is “Deploying” for CNS-managed IOS routers

Description: After Security Manager successfully deploys the configuration file to CNS, and Cisco IOS routers configured for CNS poll and apply the configuration changes at the predefined polling period, the Status column in the Deployment Manager window continues to display the job state as “Deploying.”

CSCsk42070—Discovery fails with internal error when interface name has *, (, or)

Description: Cisco Security Manager 3.2 does not support ASA/FWSM interfaces that use *,(, or) in the interface name.

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.

Diagnostics, Monitoring, and Troubleshooting Tools

Table 7 *Diagnostics, Monitoring, and Troubleshooting Tools*

CSCsl51577—“Policy not found error” for lookup from default signature in MARS

Description: If you try to perform events lookup from the default signature, a “Policy not found” error message is displayed. However, if you edit the default signature and save it, the policy icon changes to show that a local policy is configured on the device and you can navigate to events in MARS.

CSCsl67356—Security Manager client does not launch because of browser settings

Description: When you try to start the Security Manager client from the read-only policy query window in MARS, the File Download dialog box appears prompting you to confirm whether you want to download the CsmContentProvider file to your system.

CSCsl94979—Device resolution for multiple context-FWSM fails during policy lookup

Description: The disconnection 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 the Security Manager GUI causes problems on FWSM blades with multiple contexts because a unique context cannot be identified during policy lookup from MARS events.

CSCsm50836—MARS credentials retained in cache after changing authentication option

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

Table 7 *Diagnostics, Monitoring, and Troubleshooting Tools (continued)*

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

Description: When you look up a 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.

CSCsm96824—Events lookup using Security Manager started from MARS fails

Description: If you configured the option to use Security Manager credentials for events lookup, neither the query page in MARS nor the login dialog box is displayed and events lookup fails.

Firewall Services

Table 8 *Firewall Services*

CSCsa98978—Hit Count does not expand FWSM devices with object-group enabled

Description: Although the GUI allows you to enable the Object Group Search option for FWSM devices, the FWSM does not expand object groups when listing access rules after a “show access-list” command and Hit Count results are inaccurately displayed.

CSCsb85487—Need warning when ACL deployment to IOS devices can cut off access

Description: Security Manager does not check if the firewall rules that you configured in Security Manager permit management traffic (SSH and HTTPS) to the IOS device being managed. As a result, after firewall rules are deployed to the device, connection to the device might be lost.

CSCsc81905—QIT: Empty ACL is deployed on 87x series routers for BGP port

Description: IOS 87x ISR routers do not support BGP as a routing protocol or as a service in ACLs when the device has only 24 MB of memory; however, BGP is supported when the device has more than 24 MB memory. Security Manager does not detect the amount of memory available on the device and cannot enforce any restrictions. As a result, job deployment containing an ACL with ACEs having BGP will fail.

CSCsc84443—IP HTTP server cli is not removed after the policy is unassigned

Description: IOS devices require that HTTP is used as the traffic type for authentication proxy, which generates the command `ip http server`. Security Manager does not remove the CLI when authentication proxy is unassigned from the device in Security Manager.

CSCsc85416—User configured AAA/AuthProxy CLIs are not removed from the device

Description: If an AuthProxy configured on an IOS device has a user-specified name that does not comply with the naming convention used by Security Manager, the name is not removed if the device is discovered and the policy is unassigned.

CSCsd26482—IOS “access-list” Standard ACL is not supported by Hit Count

Description: IOS devices use standard ACLs for filtering; however, standard ACLs are not recognized when Hit Count reports are generated.

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.

Table 8 *Firewall Services (continued)***CSCsg35578—Import ACE: Validation not done if the config is not in show run format**

Description: Some options are omitted from rules that are created using the Import Rules tool, for example, empty port values and destination port values that are not validated for 'eq' and 'neq' for IOS devices.

CSCsi18871—PIX 7.1 gtp-map subcommand order is not preserved

Description: Changes to the match-condition order for a gtp-map used in a PIX 7.0 or PIX 7.1 device do not get deployed to the device.

Installation and Upgrade

Table 9 *Installation and Upgrade***CSCsi10243—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.

CSCso59571—Liaison servlet error while logging in to CiscoWorks page

Description: When you try to log in to the Security Manager client after installing the 3.2, 3.2.1 or 3.2.2 software on your system, a popup message is displayed with the message "CMF session-id cannot be assigned". When you try to log in to the CiscoWorks home page on a 3.2, 3.2.1, or 3.2.2 server, the following message is displayed:

Forbidden

You don't have permission to access /cwhp/LiaisonServlet on this server.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

CSCsw22048—CSAgent is not stopped automatically during inline upgrade

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

IPS and IOS IPS

Table 10 *IPS and IOS IPS***CSCsh76667—Changing a custom sig to a different engine breaks config generation**

Description: After discovering a device that has a custom signature with the atomic-ip engine, deleting that custom signature, and creating a new custom sig with an engine different from atomic-ip, configuration preview will cause errors and the configuration will not be generated.

CSCsh86189—Sig update fails when using HTTP if console logging is on

Description: Signature update to a IOS IPS device can fail if using HTTP as protocol and if the device console logging is turned on.

CSCsh77105—Signatures removed from current.xml

Description: This defect occurs during deployment. If a signature "edit" parameter (severity, enable, disable, action, retired, or SFR) is the same as the value defined in the default, then it is assumed that the parameter is defined from default, even though the parameter might have been edited.

Table 10 IPS and IOS IPS (continued)

CSCsi01650—The show content option in context menu for victim addr is not working

Description: If you select Show Content from the popup menu in the Victim Address column then you will actually be seeing the content of the Attacker Address column.

CSCsi26525—OOB OPACL changes not synchronized after successful deploy

Description: Out-of-band (OOB) OPSIG/OPACL (signature ID 50000-59999) configuration changes on a device are not automatically synchronized during deployment.

CSCsi39380—Security Manager trying to deploy multiple IP addresses and fails

Description: Deployment of an NTP policy with policy objects fails under certain conditions.

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.

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.

CSCsm54911—Deploying AIM-IPS policy to router with NM-CIDS should be skipped

Description: Deployment to a IOS router containing NM-CIDs (router module) fails if AIM-IPS Interface Policy is accidentally deployed to the router.

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.

CSCsm92398—Dup policy obj cannot be edited/deleted after event action policy copy

Description: Deployment fails after (1) creating a policy object for Target Value Rating and another policy object for OS-Identification and then (2) copying the Event Action policy to an IPS 5.1 device. (Only the TVR is applicable to the 5.1 device.)

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.

CSCso08893—MultiUserWorkflow: Sensor of 1 activity validated w/IOS IPS of 2nd activ

Description: This defect occurs in Workflow mode with more than one user, for example, User1 and User2. User1 logs in, creates a new activity, creates a greenfield sensor, and clicks on Validate; the result is an AllowedHosts error, so User1 closes the activity. Next, User2 logs in, creates a new activity, creates a greenfield IOS IPS, and clicks on Validate; the result is an AllowedHosts error for the 1st device AND an InterfaceRule error for User2's IOS IPS device.

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.

Table 10 IPS and IOS IPS (continued)

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.

CSCso11716—IPSUpd AutoUpdSettings need activity, but in effect without Submit/Appro

Description: Some IPS automatic update take effect without submitting and approving an activity.

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.

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.

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.

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.

CSCsr19163—OS Id.'s ->Restrict to these IP address field should not map to BB

Description: When using 0.0.0.0-255.255.255.255 in the OS Identification field in Network Information, this value is automatically converted to BB call <any> which the customer does not want to be converted this way. This causes a problem for the monitoring task. When the customer modifies the Target Value Rating (TVR) in this screen the BB <any> is sent to the devices.

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.

CSCsr29626—Cannot access new local signature NSDB html page for S340 and onwards

Description: Security Manager fails to display the signature description from the local NSDB for signatures newly added into signature updates for version S340 or higher.

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.

CSCsv44809—Rules and AD profile name changes with multiple vs profile config

Description: This problem occurs after deployment of virtual sensors on an IPS 6.2 device. The rule profiles exchange names; for example, the rule profile name for vs1, originally rules1, becomes rules2.

Table 10 IPS and IOS IPS (continued)

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.

CSCsv85437—Analysis Engine stops on pushing sensor update on a device with 6.0(4)E1

Description: After updating an IPS device running 6.0.4E1 or 6.0.4aE1 and then applying an engine update, the Analysis Engine stops.

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.

CSCsv29271—Security Manager overrides timezone 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.

CSCsx63927—10G support is not available for IPS 6.1.2 devices

Description: User cannot discover or deploy 10 gigabit values in interface speed for IPS 6.1.2 devices.

CSCsx66810—CSM 3.2.2 SP1 will not handle IPS 6.2 with ipv6 variables in device

Description: Discovery and deployment of an IPS 6.2 device where an IPv6 variable is configured for Event Action Rules or Signatures in Cisco Security Manager 3.2.2 service pack 1 fails. Cisco Security Manager 3.2.2 SP1 will handle only IPv4 addresses. User must make sure that IPS 6.2 device does not contain any IPv6 variables before discovering it in Cisco Security Manager 3.2.2 SP1.

PIX/ASA/FWSM Configuration

Table 11 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.

CSCsd39283—Deployment fails on no allocate-interface command in ASA/PIX70 multimode

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.

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.

CSCse47710—Warning to change admin context should note connection loss

Description: Changing the admin context in multi- or mixed mode causes the connection between Security Manager and the device to be lost.

Table 11 *PIX/ASA/FWSM Configuration (continued)***CSCse51450—OSPF validations are not adequate**

Description: Security Manager does not prevent certain invalid OSPF configurations from being discovered.

CSCse57737—The user defined bridge group name cannot be rediscovered

Description: A bridge group name defined in the Security Manager user interface cannot be rediscovered.

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.

CSCsh98788—FAILOVER - No check for interface IP address conflict

Description: Creating a Failover policy that uses the same IP address as another interface, especially the Management IP address, does not produce a conflict message.

CSCsi05756—FAILOVER - No check for Failover-PPPoE interface conflict

Description: Assigning a PPPoE-enabled interface to a device's Failover configuration does not produce an error message. PPPoE and Failover should not be configured on the same device interface.

CSCsi05805—FAILOVER - No check for use of back-up interface

Description: Any interface designated as a backup interface should not be used for Failover. However, no checks are performed for this condition.

CSCsi09478—FAILOVER - Swap LAN/Stateful VLAN links on FWSM 2.3(x); deploy fails

Description: Swapping the VLAN interfaces assigned as LAN-based and Stateful Failover links on an FWSM 2.3(x) causes a deployment failure.

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.

CSCsi11390—FAILOVER - Use of de-allocated context interface as failover link fails

Description: De-allocating an interface from a security context, then assigning that interface as a failover link, and deploying these changes all at once causes a deployment error.

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 3.1.

Table 11 PIX/ASA/FWSM Configuration (continued)

CSCsi51062—ASA5505: Deployment fails for mgmt-only option set with four named interfaces configured

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.

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.

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.

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.

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.

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.

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.

Router Configuration

Table 12 Router Configuration

CSCsc77534—NAT interface deployment fails on 83x Series routers

Description: The deployment of NAT interface commands `ip nat inside` and `ip nat outside` fails on Cisco 83x Series routers.

CSCsc91151—Virtual interfaces not being removed from router configurations

Description: Virtual interfaces remain intact in a Cisco IOS router configuration even after you delete these interfaces from the Interfaces page in Security Manager.

Table 12 Router Configuration (continued)

CSCsf09088—PPP policy does not support if-needed and local-case keywords for AAA

Description: Security Manager partially discovers PPP configurations that contain the **if-needed** and **local-case** keywords for AAA.

CSCsh18926—NetFlow deployment fails on subinterfaces

Description: Deployment fails when NetFlow is configured on a subinterface, even though a validation error is not given.

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.

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.

CSCsq31931—Restoring 3.2 DB in 3.2.1-Validation shd be given for named ACL for HTTP

Description: If Security Manager is upgraded to 3.2.1 or the Security Manager database from an earlier release is restored in 3.2.1, you might receive a deployment error if a named ACL was assigned to HTTP.

CSCsq57891—NTP- Delta is not empty after redeploying without changes

Description: Deployment config has 'ntp server' configuration command even though no changes were made to the NTP policy.

CSCsr14267—Discovery failure when target OS version does not exist

Description: You can select an unsupported OS version when adding a new device by clicking on an OS version folder (indicated by the right arrow) in the Target OS Version tree, instead of clicking on an end node of the tree (indicated by a diamond-shaped icon). If you select an unsupported OS version, you will see receive a “failed to get version upgrade information for device” error during discovery of that device.

CSCsr45265—Negation is not getting generated for policies using nonexistent ACL

Description: Negation is not getting generated for policies using nonexistent ACL.

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.

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

Table 13 Site-to-Site/Remote Access/SSL VPN Configuration

CSCsd84663—Deployment fails on Cat6k when changing VPNSM/VPN SPA slot/subslot

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.

For detailed workaround information, see the Workaround enclosure.

CSCsi82256—CSM 3.1- VPN policy discovery fails when backup-servers use hostname

Description: VPN Policy Discovery fails when group-policy is configured with backup-servers using hostnames instead of an IP addresses. The workaround is to define backup-servers with IP addresses instead of hostnames.

Table 13 **Site-to-Site/Remote Access/SSL VPN Configuration (continued)**

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 <code>ssl certificate-authentication interface outside port 443</code> command and remote access VPN policies, the command is changed to the <code>no</code> form when you preview the configuration.
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.
CSCsr23893—Remote Access VPN - Activity validation reports error for http-form
Description: When HTTP form is selected as the authentication server in the AAA tab of the connection profile, a validation error occurs.
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.
CSCsv31933—CSM 3.2.2 migration: Onscreen kbd, internal pwd features set to default
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.
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.

Where To Go Next

Table 14 **Where To Go Next**

If you want to:	Do this:
Install Security Manager server or client software.	See Installation Guide for Cisco Security Manager 3.2.2 .
Understand the basics.	See the interactive <i>JumpStart</i> 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 <i>User Guide for Cisco Security Manager 3.2.2</i> .
Complete the product configuration.	See “Completing the Initial Security Manager Configuration” in the online help, or see Chapter 1 of <i>User Guide for Cisco Security Manager 3.2.2</i> .
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 2 of <i>User Guide for Cisco Security Manager 3.2.2</i> . <ul style="list-style-type: none"> Setting Up User Permissions Integrating Security Manager with Cisco Secure ACS

Table 14 *Where To Go Next (continued)*

If you want to:	Do this:
Bootstrap your devices.	See “Preparing Devices for Management” in the online help, or see Chapter 5 of <i>User Guide for Cisco Security Manager 3.2.2</i> .
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 <i>Installation Guide for Cisco Security Manager 3.2.2</i> .

Related Documentation

[Table 15](#) describes the product documentation that is available. For information on ordering printed documents, see [Obtaining Documentation and Submitting a Service Request](#), page 23.

Table 15 *Product Documentation*

Document Title	Available Formats
<i>Guide to User Documentation for Cisco Security Manager 3.2.2</i>	<ul style="list-style-type: none"> Printed version included with product. PDF on the product DVD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_documentation_roadmaps_list.html
<i>Installation Guide for Cisco Security Manager 3.2.2</i>	<ul style="list-style-type: none"> PDF on the product DVD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.2/installation/guide/instl.html
<i>User Guide for Cisco Security Manager 3.2.2</i>	<ul style="list-style-type: none"> PDF on the product DVD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.2/user/guide/UserGuide.html
<i>Supported Devices and Software Versions for Cisco Security Manager 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.2/compatibility/information/csmsdt322.html
<i>FAQ and Troubleshooting Guide for Cisco Security Manager 3.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2/troubleshooting/guide/FAQ_and_TS_Guide.html
<i>Migrating from CiscoWorks VPN/Security Management Solution to Cisco Security Manager</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/migration/guide/migr_gd.html

Table 15 Product Documentation (continued)

Document Title	Available Formats
<i>High Availability Installation Guide for Cisco Security Manager 3.1</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.1/high_availability/guide/igha.html
<i>User Guide for Auto Update Server 3.2.2</i>	<ul style="list-style-type: none"> PDF on the product DVD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.2/user/guide/aus32ug.html
<i>Supported Devices and Software Versions for Auto Update Server 3.2.2</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.2.2/compatibility/information/aus_dev.html
<i>Security Manager Integration with ACS</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_configuration_example09186a00808eada8.shtml
<i>Release Notes for Cisco Security MARS Appliance 4.3.4</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html
<i>Release Notes for Cisco Security MARS Appliance 5.3.4</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html
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*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0908R)

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

© 2004-2009 Cisco Systems, Inc. All rights reserved.