Release Notes for Cisco Security Manager 3.2.1

Revised: April 26, 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 29. 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 3.2.1* supersedes any information contained in the context-sensitive help included with the product. For more information about specific changes, please see Documentation Updates, page 26.

This document contains release note information for the following:

- **Cisco Security Manager 3.2.1 (Including Service Pack 1)**

  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.

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

- **Auto Update Server 3.2.1**

  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. Cisco IOS routers that have dynamic IP addresses communicate with AUS that is running the Cisco Networking Services (CNS) Gateway Protocol to provide their IP addresses.

  Security Manager can interoperate with AUS. 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 3.2.1, 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 17, and the *Installation Guide for Cisco Security Manager 3.2.1* before installing or upgrading to Cisco Security Manager 3.2.1.

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 3.2.1

- Support for ASA 8.0 and 8.1 SSL VPN configurations. Support for SSL VPN on ASA 7.x is removed in Security Manager 3.2.1. The Security Manager 3.2.1 installer provides a warning if any ASA 7.x SSL VPN configurations are detected in the case of an upgrade.
- New File Policy Object to support SSL VPN files.
- ASA 7.2.4 and FWSM 3.1(9), 3.2(4) are now supported. The following software is also supported, but is treated as the indicated software version:
  - FWSM 3.2(5) is treated as 3.2(4).
  - IPS 6.1.1 is treated as 6.0. Features unique to 6.1.1 are not supported.
- ACL name preservation is now supported in additional IOS and ASA/PIX policies.
  - IOS policies now include: VTY, Console, HTTP, QoS, NAC, SNMP, Advanced Interface Settings, Dialer, VLAN ACL, IPS AIM, IPS Interface RulesClient Connection Characteristics for Easy VPN,User Group Policy for Easy VPN and for Remote Access VPN, Protected Network for IPsec VPN.
  - ASA/PIX policies now include: RIP, Dynamic Access under Remote Access VPN; User Group Policy for Easy VPN and for Remote Access VPN (ASA, PIX 7.x, PIX 6.3); Protected Network for IPsec VPN.
- Support for the 881 and 888 Integrated Services Routers.
- Support for policy object name validation using special leading characters.
- Support of AIP SSM-40--Cisco Security Manager 3.2.1 supports the Cisco Adaptive Security Appliance (ASA) 5500 Series Advanced Inspection and Prevention Security Services Module 40 (AIP SSM-40) in the ASA5520 and 5540. It has the same software feature set as the AIP SSM-10 and the AIP SSM-10. It requires ASA 8.0.3 and IPS 6.0(4).

- Security Manager <> CS MARS Linkage Enhancements (requires CS MARS 6.0.1)
  - Linkage support for virtual sensors
  - Ability to use a CS-MARS global controller for linkage to Security Manager
  - Support for ASA 8.1 netflow events
- You can now use CS-MARS global controllers to integrate CS-MARS and Security Manager.
- Modification to Services policy objects.
- Service object group discovery.
- Remote access VPN policy TOC redesign.
- Easy VPN enhancements.
- Upgrade of included applications: Common Services 3.1.1, RME 4.1.1, AUS 3.2.1, Performance Monitor 3.2.1, CSA 5.2.0.263.
- Support for running Security Manager in VMware ESX Server 3.5.
- Client support for Windows XP SP3 and Windows Vista SP1.

Installation Notes

- You can install Security Manager 3.2.1 server software directly, or you can upgrade the software on a server where either Security Manager 3.1, 3.1.1, or 3.2 is installed. In addition to reading these installation notes, we strongly recommend that you refer to the *Installation Guide for Cisco Security Manager 3.2.1* for important information regarding server requirements, server configuration, and post-installation tasks.
- Before you can successfully upgrade to Security Manager 3.2.1 from a prior version of Security Manager (versions 3.1, 3.1.1, or 3.2 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 3.2.1*.
- Service Packs: Service packs cannot be installed by themselves. They are intended for installation on an existing installation of Cisco Security Manager 3.2.1. For more information, see Cisco Security Manager 3.2.1 Service Pack 1 Download and Installation Instructions.
- 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 3.2.1 Service Pack 1 Download and Installation Instructions

Step 1 To download and install Cisco Security Manager 3.2.1 Service Pack 1, log in to Cisco.com.

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

Step 3 Download the file fcs-csm-321-sp1-win-k9.exe.

Step 4 To install the service pack, close all open applications, including the Cisco Security Manager Client.

Step 5 Manually stop the Cisco Security Agent (CSA) from **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 6 Install the Security Manager 3.2.1 FCS build (with or without Service Pack 1) on your server if you have not already done so.

Step 7 Run the fcs-csm-321-sp1-win-k9.exe file that you previously downloaded.

Step 8 In the Install Cisco Security Manager 3.2.1 Service Pack 1 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.

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

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

Cisco Security Manager 3.2.1 Download and Installation Instructions

To download and install Cisco Security Manager 3.2.1:

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 3.2.1.*

Step 3 Download fcs-csm-321-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 3.2.1.*

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

- 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 13.
- 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 3.2.1. 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 a 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 3.2.1, 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

Table 2 contains problems that were resolved in Security Manager 3.2.1 Service Pack 1.

Table 1 contains problems that were resolved in Security Manager 3.2.1.

Table 1 Resolved Problems in Security Manager 3.2.1 Service Pack 1

CSCsr11663—Policy Object cannot be referenced for sweep signatures in IPS device

Description: The GUI does not support the policy object selector under the following conditions: Edit the signature with ID 2100, which has a sweep engine; click on the Edit parameter and click on the Engine, then Src (or Dst) Addr Filter and click on the field. The user will be unable to reference a Policy object (variable) for the src and dst addr filter parameter for sweep signatures.

CSCsr15293—Security Mgr hangs on device props when retrieving device certificate

Description: The Security Manager Client hangs when you click the **Retrieve From Device** button on the Device Properties > Credentials panel to retrieve the certificate thumbprint from the device.

CSCsr22080—The portlist with neq is deploying only range less than the neq value

Description: Deployment of "neq" option in a service or portlist object is not correct.

CSCsr24673—Fail to save bypass mode change for 6.1(1) IPS NPE

Description: For IPS 6.1(1) E2 devices, a null pointer exception is encountered if the "Bypassmode" is changed and the Save button is clicked under either of these conditions: (1)IPS > Interfaces > Physical Interfaces or (2) IPS > Interfaces > Summary.

CSCsr25652—PKI: "no email" command generated after discovery

Description: The email subcommand under the trustpoint CLI should not be negated upon a discovery and deployment from Security Manager.

CSCsr27477—SSL VPN: Dynamic Access+ Policy > Port Forward Lists cleared erroneously

Description: Previewing a configuration shows the Port Forwarding Lists that were created within the DAP configuration as being cleared erroneously.

CSCsr27692—Editing the AIM-IPS policy in policy view throws error pop-up

Description: This problem occurs in policy view (shared policy view) in the AIM-IPS policy under Interfaces > settings > AIM-IPS after edit and save, but you can continue after clicking OK.

CSCsr29794—SSL VPN: Deployment shows success even if customization download fails

Description: When deploying SSL VPN policies that include portal customization with unicode UTF-8 characters, deployment status can be displayed as "Deployed Sucessfully" even if the ASA device rejects the portal customization xml file.

CSCsr30143—Policy map type inspect dns preset_dns_map non-empty delta

Description: Preview policy-map type inspect DNS always shows delta.

CSCsr30149—crypto ca trustpoint <trustpoint_name> non-empty delta

Description: Import an ASA device that has Public Key Infrastructure (PKI) configured for VPN, and one or more trustpoints with the "fqdn none" option employed. Subsequent deployment removes the "fqdn none" command if the trustpoint has an enrollment type "self" or "terminal."

CSCsr30178—Exception occurs discovering P2P IPSec VPN with ASA/PIX as one of the peers

Description: PIX and ASA do not support crypto ACL with ICMP service and a type specified.

Table 1 Resolved Problems in Security Manager 3.2.1 Service Pack 1 (continued)

CSCsr31890— Restore of SSL VPN config should be done in continue download on err mode

Description: If the configuration option stopDownloadOnError is enabled, when rollback of an SSL VPN configuration fails, Security Manager will try to restore the initial SSL VPN configuration present in the device before the rollback was started. If a CLI fails the download, then Security Manager will stop downloading the rest of the CLI.

CSCsr49267—DDP: extra leading spaces in an ACL remark

Description: On ASA/PIX/FWSM devices, the ACL remark might get negated in the delta.

CSCsr50925—Address pool should not be copied to ASA transparent device

Description: Activity validation fails with an error that the address pool is not supported on the given device.

CSCsr56864—Validation error for interface role policy object when override removed

Description: An error is shown when you try to validate changes or open the interface policy editor for interface roles that are non-overridable.

CSCsr61447—SSL VPN: ASA 8.0(3)31 and 8.1(1)6 smart tunnel and auto start not discovered

Description: ASA 8.0(3)12 and later use a different smart tunnel command syntax. When an ASA device running 8.0(3)12 or later is imported into Security Manager, and the device contains the cli "smart-tunnel auto-start ..." in its configuration, the group policy GUI shows a blank smart tunnel field and the smart tunnel object is not discovered.

CSCsr66804—"NetworkBBTextFieldSelect" throws exception when range is used

Description: Security Manager allows you to create networks using a range format (e.g., 10.20.0.0-10.20.255.255), but an exception results when a range is entered or selected.

CSCsr66997—Support for IPS 6.0.5 or later - unauthenticated NTP support

Description: Currently, Security Manager supports configuration of the Authenticated NTP Server (Platform > Device Admin > Server Access > NTP). Security Manager supports configuration of NTP Server IP Address, Key and Key ID. To configure Unauthenticated NTP Server, you are no longer required to enter a Key and Key ID when configuring an NTP server.

CSCsr73955—Add device from file fails when using CS-MARS format .csv seed file

Description: When attempting to add multiple new devices to Security Manager via the Add Device From File function (CSM client application > File menu > New Device... > Add Device From File option), even if you provide a valid CS-MARS format .csv seed file, the Security Manager client application still shows an error.

CSCsu22923—Increase the VRF name length limit to 30 characters

Description: Security Manager throws a UI validation error.

CSCsu32601—New VPN dynamic route gets generated during deployment

Description: New VPN dynamic route is incorrectly generated during deployment.

Table 2 Resolved Problems in Security Manager 3.2.1

CSCsf27513—Cisco Secure Desktop 3.1 GUI not up-to-date with application versions

Description: When you create a Secure Desktop Configuration object from the Policy Object Manager window, spelling errors, outdated software program versions, and non-support of recent component releases are noticed during the configuration of a group-based VPN feature policy. This occurs because Security Manager 3.1 and 3.2 support only CSD Release 3.1.1, which works with ASA 7.1, in which these GUI inconsistencies exist.

CSCsg89249—Deployment fails on ASA 7.2(1) when removing IKE policy

Description: When you try to remove an IKE policy configuration from an ASA device that is running OS version 7.2(1) or 7.2(2), deployment fails.

Table 2 Resolved Problems in Security Manager 3.2.1 (continued)

CSCsg94596—Deploy fails on live ASA 7.2(1) RA server while removing IKE policy **Description:** In a remote access VPN configuration, when you unassign IKE proposals from a live ASA 7.2(1) device, deployment fails due to an error with the **no crypto isakmp** command.
CSCsh57280—Standby group change removes crypto map in H&S/RA VPN with HA **Description:** In a hub-and-spoke or remote access VPN configured with High Availability, if you change the standby group number after a deployment, the crypto map is removed from the interface on a subsequent deployment.
CSCsi19059—No validation error when large tunnel key value turns negative in DMVPN **Description**: In a hub-and-spoke VPN topology, when you define a tunnel key with a large value in a DMVPN policy and save the changes, the tunnel key changes to a negative value after deployment. No error is displayed when you validate your activity, but an error message appears on submission and deployment.
CSCsj29304—Unable to Deploy IPS Category Settings Using SSH **Description:** You cannot use SSH when deploying IOS-IPS category settings to a device. Instead, configure the device to use SSL for deployment.
CSCsl62494—Discovering “http redirect” requires IP address on the related interface **Description:** An “http redirect” is not discovered for an interface if no corresponding “http <ip> <mask>” exists. Discovery for “http redirect” (and for “http authentication-certificate”) requires IP address/mask assignments on the related interfaces.
CSCsl83852—AIM IPS's parent deploy not allowed under some condn, child dependency **Description:** Deployment to an AIM-IPS or to its parent router should be possible individually or together, but under some conditions, deployment to both fails on 28xx routers.
CSCsm04760—IDSM discovery failure reason not shown in discovery page **Description:** Discovery is only partially successful for a Catalyst switch with two IDSMs.
CSCsm16499—Validation not done for references to event lists in logging filter **Description:** If you copy only the logging filters policy and not the event lists policy from the source device to the target device, deployment fails when you attempt to configure logging filters for event lists that are not available on the target device.
CSCsm33274—Renaming a PPPoE user assigned to a VPDN group fails **Description:** If you attempt to edit the name of a PPPoE user which is already assigned to a VPDN group, the new name is not picked up.
CSCsm41387—Validate should capture AIM IPS settings on irrelevant interfaces **Description:** This defect occurs when discovering a router (R1) without AIM-IPS and discovering a second router (R2) with AIM-IPS. After a copy operation, the source interfaces of R1 are listed in the UI for R2, even though R2 does not have the interfaces on it. Also, the IDS-Sensor is on 0/1 but after the copy operation it is shown as IDS-Sensor 0/0.
CSCsm46412—User name/password deployment to system context fails on FWSM 3.2 **Description:** A user name/password credential cannot be applied to a FWSM 3.2 system context; deployment fails.
CSCsm49694—Default Sigs: Discover ignores tuned event actions, other changes fine **Description:** The CLI can be used to edit properties such as fidelity, alert, event action, retire, and enable on default signature engines supported by IOS IPS. After such editing and then discovery in Security Manager, the changes in these properties are not preserved for the following two engines: Normalize and Service-RPC.
CSCsm51774—ServicePorts changes of service-smb-advanced signature not discovered **Description:** After tuning a service-smb-advanced engine signature by changing the fidelity and changing the Service Port value, discovery works for the fidelity change but not for the Service Ports change.

Table 2 Resolved Problems in Security Manager 3.2.1 (continued)

CSCsm57132—EditUdpateSchedule: Doesn't change date, shows old date but works on cur **Description:** The EditUpdateSchedule dialog box produces unreliable results.
CSCsm69126—WF: Not able to add inline pair in first attempt **Description:** The add, edit, and delete actions have no effect on the Interface Inline Pair, Vlan Pair, or Vlan Group when in Workflow mode with all activities closed. However, second and subsequent attempts are successful.
CSCsm78094—Deploy fails when VS is created in IDSM discovered via Cat6K **Description:** Deployment fails when a virtual sensor is created in an IDS module that is discovered on a Catalyst 6000-series switch, but deployment succeeds when the IDS module is discovered directly.
CSCsm78920—Unable to save more than one NTP server in multiple mode **Description:** If you add multiple NTP server entries on a PIX/ASA in multiple-context mode, and then click Save, only one entry is actually saved.
CSCsm84971—Deleting Timeout policy does not reset timeout values to defaults **Description:** Removing a Timeout policy does not reset timeout parameters to their default values; the expected result.
CSCsm86452—Not able to edit physical Interface settings for IDSM **Description:** The user is not able to modify the Description and Default VLAN for an IDS module.
CSCsm95151—Preview/deploy error when configs reference non-existent policy maps **Description:** When an QoS policy class map has an ACL that is shared with another policy map, removing the interface associated with the QoS policy class map causes an error.
CSCsm97107—Webfilter server n2h2 command is generated on redeployment **Description:** On FWSM 3.2, when the Webfilter url-server type is selected in N2H2/SmartFilter, the **url-server** command will be removed and redeployed on each deployment to the device.
CSCsm98494—OOB change on device, no changes in CSM - detects OOB but skips deploy **Description:** Under certain conditions, Security Manager detects out-of-band changes on an IOS IPS device but does not push them to the device.
CSCsm99625—Deployment to FWSM shows success despite failed cmd in transcript **Description:** When deploying configuration changes from Cisco Security Manager to a FWSM, saving the configuration on the device fails; however, deployment reports it as successful.
CSCso00820—Incorrect message during discovery failure of Catalyst 6500 Series IDSM **Description:** If you are adding a Cisco Catalyst 6500 Series switch that contains an Intrusion Detection System Services Module (IDSM), and import fails during discovery of the IDSM, the resulting error message will contain non-specific information.
CSCso02731—Typo in router validation properties file **Description:** Detailed error messages are not displayed in Missing Interface Intercept ACL validation errors due to a typo in the properties file.
CSCso06762—Deployment fails when deleting new service object in ASA 8.x device **Description:** ASA 8.x supports new service object groups that are not supported by Security Manager 3.2. If you configure a new service object group and use it in ACEs in the device, Security Manager 3.2 can discover the device; however, the access list is only partially discovered. The ACEs using the new service object group will not be discovered in Security Manager.
CSCso07931—Unable to modify SNMP port for ADMIN context in multiple mode **Description:** SNMP Port value cannot be changed for Admin context on an ASA in multiple mode.

Table 2 Resolved Problems in Security Manager 3.2.1 (continued)

CSCso17504—Unable to delete NAT0 ACL & static rules from GUI after deployment **Description:** Deleting rules from NAT > Translation Rules on a PIX/ASA/FWSM device sometimes does not work after a discovery or an activity approval.
CSCso32942—Wrong delta generated when AIM & NAT are assigned ACL with underscore **Description:** When a device has an ACL object with an underscore in its name assigned to both a NAT policy and an AIM-IPS monitoring policy, deployment to the device fails.
CSCso33321—Database restore from versions earlier than 3.0.2 to 3.2 is not blocked **Description:** Although Security Manager 3.2 supports upgrades only from the following previous versions: 3.0.2, 3.0.2 SP1, 3.1, 3.1.1, 3.1.1 SP1 and SP2, restoring a Security Manager database earlier than 3.0.2 goes through properly on a 3.2 server, without any error message or termination of this operation.
CSCso11735—DownloadUpd at specified time also applies downloaded sigupd to devices **Description:** IPS devices receive an update instead of a download only when the server is at a more recent signature level.
CSCso02500—Import plain IOS device, 1st deploy to it pushes ips signature category **Description:** Deploying a router (IOS IPS device) with no IOS IPS enabled can result in Security Manager pushing the ISP signature category command to the device.

Known Problems

This section contains information about the problems known to exist in Cisco Security Manager 3.2.1. 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.

- AUS Known Problems, page 12
- Catalyst 6500/7600 Configuration, page 12
- Deployment, page 13
- Device Management, page 13
- Diagnostics, Monitoring, and Troubleshooting Tools, page 13
- Discovery, page 15
- Firewall Services, page 15
- Installation and Upgrade, page 17
- IPS and IOS IPS, page 18
- PIX/ASA/FWSM Configuration, page 21
- Policy Objects, page 23
- Router Configuration, page 23
- Site-to-Site/Remote Access/SSL VPN Configuration, page 24

- Tools, page 25
- User Interface, page 26

AUS Known Problems

Table 3 AUS Known Problems

CSCsc89457—AUS GUI does not close automatically when exiting CiscoWorks

Description: A user logs out from the CiscoWorks session after launching AUS, but the AUS GUI remains open. If another user with a different role opens a new CiscoWorks session, other users can navigate the AUS GUI briefly in the original window. This problem occurs whether the CiscoWorks server or the Cisco Secure Access Control Server (ACS) manages authentication and authorization for AUS.

CSCsd25476—Configuration file download for an AUS-managed ASA device fails

Description: If you configure an ASA device in transparent mode and use AUS to deploy configuration changes from Security Manager to the device, deployment is shown as successful, although the device does not contain the deployed changes. The AUS event report shows that the file was successfully sent to the device without error and a “Wakeup information for process auto-update lost” message is recorded in the device log.

Catalyst 6500/7600 Configuration

Table 4 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.

Deployment

Table 5 Deployment

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 of ISR routers.
CSCsd70915—GTP Map: Deployment fails due to PDP and signaling timeout issues **Description:** When you deploy an inspection rule with the **gtp-map** command, the deployment fails and an error message states that the signaling timeout value is less than the PDP timeout value.
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".
CSCsr43613—CSM 3.2/3.1 rollback on FWSM 3.2 removes admin context crypto key **Description:** Rolling back configurations on FWSM 3.2 removes the crypto key from the device, preventing device access.

Device Management

Table 6 Device Management

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.

Diagnostics, Monitoring, and Troubleshooting Tools

Table 7 Diagnostics, Monitoring, and Troubleshooting Tools

CSCsi08390—IEV installation fails on systems without C: drive **Description:** During installation of Security Manager server 3.1 on systems that do not contain C: drive, IEV server fails to install and an error message is displayed. Also, an error is logged in the server installation log file.
CSCsi86335—Cross-launch of IEV client fails if Symantec application is running **Description:** You cannot start IEV client from Security Manager client on a system in which the Symantec Client Firewall Port Scanning Module or Symantec Secure Port application is running.
CSCsk28603—Security Manager client not brought to focus during lookup from MARS **Description:** If your Security Manager client session is active when you perform policy lookup from the MARS GUI, the existing Security Manager client window is not brought to the foreground or into focus by default.
CSCsk55251—MARS events matching the first instance of duplicate rule not shown **Description:** If you create duplicates of a base rule in the Access Rules page of Security Manager, the events matching the second identical rule are only displayed in MARS when you perform a lookup.

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

CSCsk78778—Error not shown for unavailable ACE during MARS events lookup **Description:** An error message is not displayed if you delete an access rule in Security Manager and perform lookup from the MARS events query results page that was opened by performing a lookup from the same access rule in Security Manager.
CSCsk94278—Read-only policy page in MARS is blank after starting Security Manager **Description:** When you start the Security Manager client from the read-only policy query page in MARS, the read-only page is refreshed and is displayed blank. However, you are prompted to install the Security Manager client and the page for downloading the application is opened.
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.
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.
CSCsr20046—MCP:”Report->Remote Access->Users->Session report" missing for ASA **Description:** The Report > Remote Access > Users > Session report in Cisco Performance Monitor does not show a report for ASA security appliances.

Discovery

Table 8 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.

CSCsl70926—Unable to Rediscover a PIX Device After Upgrading the OS

Description: If you upgrade the operating system version on a PIX device, rediscovering policies on the device might fail if the device includes RIP policies. Unassign the RIP policy before rediscovering the device.

Firewall Services

Table 9 Firewall Services

CSCsa81103—Unable to create an access rule with TCP flags

Description: Security Manager does not support TCP flag specifications, such as urg, fin, psh, and ack, in access rules. As a result, during discovery, Security Manager drops the specifications.

CSCsa81104—Unable to create an access rule to match QoS parameters

Description: Security Manager does not support ACE options such as DSCP, ToS, or precedence. As a result, during discovery, Security Manager drops the options.

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.

Table 9 Firewall Services (continued)

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.

CSCsd33025—Deployment fails on a device with too many AAA server groups

Description: If Security Manager tries to deploy AAA server groups to a device that already has the maximum number of AAA server groups, deployment fails.

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.

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.

CSCsh68101—Activity Report: Issues with access rules table

Description: Rule section changes are not reported in the activity reports.

CSCsh94210—Problems matching interface when reusing AAA policy objects

Description: AAA Server policy objects cannot be reused because of mismatched interfaces. This might result from an interface role used to define an interface that is not matched to a physical interface after rediscovery. For PIX/ASA7.x devices, this might result from using "inside" (or an interface name that starts with "inside") to describe the interface.

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.

CSCsk12692—Unsupported CLIs in the previous version are negated after upgrade

Description: After you upgrade from Security Manager 3.0.1 to 3.1 or Security Manager 3.0.2 to 3.1.1, the command "ip http server" is deployed to an IOS router if the router already has the command "ip http secure-server". Command "ip http server" will turn on the HTTP server on the router.

CSCsr24558—Policy static with nested service policy object: preview throws error

Description: If a nested service object is used in a Policy Static rule, deployment might give an error that there is a protocol mismatch and fail to deploy to device.

CSCsr25786—AAA server object should have activity validation for no i/f specified

Description: For ASA/PIX 7.x and above, and FWSM 3.x and above, when no interface is specified in a AAA server object, there is no error or warning message on this during activity validation.

CSCsr28004—Web Filter: Nested policy object - conflict is not detected

Description: Deployment to the device might fail for filter commands on PIX/ASA/FWSM devices if there are services with overlapping ports.

CSCsr45372—Deployment fails when service object name exceeds 64 characters

Description: When you create a service policy object in Security Manager with a name that exceeds 64 characters., then deploy the configuration to a ASA/PIX 8.x device, a deployment error results, stating that the service object group name exceeds the maximum size of 64 characters.

Installation and Upgrade

Table 10 Installation and Upgrade

CSCsb65932—The Windows language version must be either English or Japanese

Description: On your Security Manager server *and* on every PC on which you install Security Manager Client, you must use either the English (United States) or Japanese version of Windows.

CSCsj97840—Installer is overwriting gatekeeper.cfg file (multihome file)

Description: Multihome configuration does not work after upgrade.

CSCsk39707—Installer fails to upgrade the HA agent files into the Veritas directory

Description: Security Manager Veritas Cluster Server (VCS) agent files are not updated after installation of Security Manager.

CSCsl85305—Inline upgrade from 3.1 to 3.2 fails on a server with Cisco Secure ACS

Description: When you perform an inline upgrade from Security Manager 3.1 to 3.2 on a server in which Cisco Secure ACS is running, the following message is displayed:

```
Error: C:\PROGRA~1\CSCOpx\objects\db\win32\dbunic9.dll is used by another running process.
```

CSCso17613—Starting AUS/CS from CSMS page fail for non-default HTTPS port number

Description: If you modified the HTTPS port number on your Security Manager server by running the **changeport.exe** <*port_num*> **-s** command at the NMSROOT/MDC/Apache directory prompt (where NMSROOT is the directory in which Security Manager is installed) and also updated the client.info file on your Security Manager client with the server port number, starting AUS or Common Services from the Cisco Security Management Suite page fails.

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.

CSCsq50248—CSAgent does not shut down during inline upgrade

Description: In some situations, the Cisco Security Agent cannot be shut down by the Cisco Security Manager installer and must be shut down manually.

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.

CSCsr23626—Cisco Security Manager Client is not available from Start menu

Description: If you select the option to not create shortcuts during Security Manager installation, the Cisco Security Manager Client application is not available from the Start menu.

IPS and IOS IPS

Table 11 IPS and IOS IPS

CSCsh67506—Dynamic IP address IOS router imported by CNS cannot be discovered

Description: Discovery and deployment of IOS IPS devices through CNS servers does not work. In the Add Device Wizard, the Option IPS should not be selected; the device should be created as an IOS only device. If the device had already been created as an IPS device, then there will be errors while discovering and deploying the IPS-related policies, but all other policies will get discovered/deployed properly.

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 an d 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 defects 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.

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.

CSCsi33159—Greenfield device is showing 5.1(4)E1 but should be 5.1(5)E1

Description: This defect occurs when adding a new IPS device. For a 5.1(5)E1 device, the device version is shown, incorrectly, as 5.1(4)E1.

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

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

CSCsi44605—IPS variable names cannot contain special characters

Description: For IPS devices (only) in Security Manager the special characters - and _ are not allowed. If they are used, validation will fail when attempting to create network policy objects.

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.

Table 11 IPS and IOS IPS (continued)

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.
CSCsm92364—Not able to apply license for IPS 4270 device after applying a trial ver **Description:** Licenses for IPS 4270-20 devices are not applied correctly if a trial version has already been used on that particular device.
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.
CSCsm98683—Network Information policy OOB settings ignored, deploy always goes thru **Description:** For some Network Information policy changes, Security Manager goes through the Deployment without performing an out-of-band check.
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.
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.

Table 11 IPS and IOS IPS (continued)

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 allows 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.
CSCsr29999—Enable one-way TCP reset option should not appear in CSM UI **Description:** For IPS 6.1.1 devices, Security Manager shows the Enable one-way TCP reset option, but it is not supported and will not generate a delta during deployment.
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.
CSCsr41557—Unauth NTP negation happening for a 6.0.5E2 device **Description:** For default settings for the NTP option on an IPS 6.0.5 E2 device, Security Manager negates unauthorized NTP under certain conditions.
CSCsr41654—Add Devices from File causes error in deployment **Description:** When devices are being imported through the "Add Devices from file" option, some errors appear for IP address format in the Event Action Rules policy.
CSCsr45632—Unable to deploy authenticated NTP if Unauth NTP configured on sensor **Description:** When managing an IPS 6.1(1)E2 device, NTP server details are lost after configuration of unauthenticated NTP.
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.

PIX/ASA/FWSM Configuration

Table 12 PIX/ASA/FWSM Configuration

CSCsb17962—Service objects with same content can cause problems during discovery

Description: If multiple service objects have different names but the same definitions, the wrong service object might be used during discovery. Because the service objects are equivalent, deployment using a service object with a different name does not cause problems.

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 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.f

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.

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.

Table 12 PIX/ASA/FWSM Configuration (continued)

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.

CSCsi51062—ASA5505: Deployment fails for mgmt-only option set with 4 nameif configur

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.

CSCso17366—Preview Configuration not displaying generated CLI for copied policies

Description: The CLI commands generated by copying a policy (specifically Logging Filters in this case) from one device to another may not be displayed in Preview Configuration, although the policy was copied successfully.

CSCso80308—Security Manager 3.2 does not support interface names with () signs

Description: Cisco Security Manager 3.2 does not support ASA/FWSM interface names with () signs.

Table 12 PIX/ASA/FWSM Configuration (continued)

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.
CSCsr41074—HTTP Policy: Assigned policy includes server port for FWSM **Description:** When creating an HTTP policy, an HTTP server port number is provided. Following assignment of this policy to a device, the generated CLI includes this port number, which will cause deployment to fail. Instead of using a shared HTTP policy, enable the HTTP server on devices individually (via Device View).

Policy Objects

Table 13 Policy Objects

CSCso30566—Error shown when previewing config after creating an extended ACL **Description:** After you create an extended ACL on a router in Security Manager, if you preview the configuration, you might get an error in some cases.

Router Configuration

Table 14 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.
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.

Table 14 Router Configuration (continued)

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.

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

Table 15 Site-to-Site/Remote Access/SSL VPN Configuration

CSCsb66843—Unable to delete the IPsec Profile

Description: If you have DMVPN or VRF configured on an IOS router and you try to change or remove this configuration in Security Manager, deployment fails and you receive a message that the IPSec profile is still in use and cannot be deleted. This is an IOS problem, not a problem intrinsic to Security Manager.

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.

CSCse94752—Support for IOS version 12.2(33)SRA on 7600 devices

Description: Some commands integrated into Cisco IOS Release 12.2(33)SRA, such as **crypto engine slot** *slot/subslot* {**inside | outside**}, on Cisco 7600 Series Routers are not supported during deployment and discovery.

CSCsf32244—Deployment fails on preconfigured Easy VPN spoke

Description: When you configure a spoke in an Easy VPN topology using Security Manager, and the spoke is already configured as a remote client in an Easy VPN that is not managed by Security Manager, deployment fails if both configurations are on the same external interface.

CSCsg70106—Activity validation takes several minutes to complete

Description: An activity’s validation process takes a long time to complete because the Security Manager’s database is very large. This may be due to the number of devices, objects, policies, and VPN configurations defined on the server.

CSCsh14709—Deployment fails on ASA 5505/PIX 6.3 Easy VPN remote client

Description: In an Easy VPN topology, you cannot modify specific CLI commands including interface settings, on an ASA 5505 or PIX 6.3 device that is configured as a remote client.

For a list of the CLI commands that cannot be modified, see the *Commands That Cannot be Configured When Easy VPN is Enabled* section in *FAQs and Troubleshooting Guide for Cisco Security Manager 3.x*.

Table 15 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 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.
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.
CSCsq83195—Dynamic Access policy is empty after upgrading to Security Manager 3.2.1 from 3.1.1 SP3, 3.1 **Description:** Security Manager 3.1.1 did not support PIX/ASA 8.x devices directly; these were imported as 7.x devices. Following an upgrade to Security Manager 3.2.1, these remain mapped as 7.x devices. However, in Security Manager 3.2.1, SSL VPN is not supported for 7.x, and as such the Dynamic Access policy is empty.
CSCsr12355—SSL VPN portal customization object, application list missing entries (ASA 8.1.1.5 only) **Description:** While discovering SSL VPN configurations from an ASA device running 8.1.1.5, the application list in the SSL VPN portal customization object may not be populated correctly in Security Manager. The application list on Security Manager's portal customization object editor may show missing entries.
CSCsr18316—SSL VPN - ASA 7.x SSL VPN deployment failed **Description:** Security Manager 3.2.1 does not support SSL VPN for ASA 7.x; however, it does not prevent you from assigning IPSec, SSL and SSL group policies to the Remote Access connection profile on these devices. Deployment will subsequently fail.
CSCsr20738—De-assigning SSL VPN does not remove SSO and cache file-system commands **Description:** After discovering an ASA 8.x device with WebVPN configured with SSO and cache file-system parameters, if you de-assign the SSL VPN policies, the SSO and the cache file-system configurations are not removed.
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.
CSCsr27295—SSL VPN - Proxy PAC removed after HTTP/HTTPS Proxy Svr configuration **Description:** After configuring http pac, if you switch to http proxy, then the http proxy commands do not appear in the device configuration.
CSCsr27386—SSL VPN - Error when assigning multiple bookmarks to DAPs **Description:** A deployment error occurs when multiple bookmarks are referenced by a dynamic access policy (DAP) and one of those bookmark names has a space in it.
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.

Tools

Table 16 Tools

CSCse69546—Backup/restore fails when Cygnus Solutions software is installed **Description:** Backup/restore fails when Cygnus Solutions software is installed and Cygnus mounted drives are being used.

User Interface

Table 17 User Interface

CSCsc66055—Client is unresponsive when TACACS+ server is unavailable

Description: The Security Manager client stops responding when the Cisco Secure ACS that is performing user authentication goes down or becomes unavailable.

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 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 from your Security Manager 3.2 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.
```

CSCsk11268—A User Can Open Multiple Sessions in Non-Workflow Mode

Description: If a user adds a space before or after the username when logging in, the session is considered different from a session without the extra space when working in non-Workflow mode. This can lead to problems when the user tries to submit changes to the database.

Documentation Updates

Topics in this section describe updates and changes to the user documentation for Auto Update Server 3.2 and Security Manager 3.2.1.

Understanding IPS Licensing Restrictions

Some IPS devices, such as the IPS 4270 or the AIP SSM-40 in an ASA device, require that you have a Cisco.com account to update the license. Security Manager allows you to configure either Cisco.com or a local server as an IPS Update server. However, if you use a device that requires a Cisco.com account, you must configure Cisco.com as the IPS Update server; you cannot configure a local server as the IPS Update server.

This restriction will be reflected in the following topics in the “Managing the Security Manager Server” chapter:

- “Updating IPS License Files” will include this information:

  Before You Begin

  If you use Cisco.com, you must first configure the IPS Update server to be Cisco.com, so that you can specify the username and password. You must use Cisco.com for licensing if you are using a device that requires it; for example, an IPS 4270 or an AIP SSM-40 in an ASA device requires a Cisco.com account. For information on configuring Cisco.com as the IPS Update server, see “Configuring the IPS Update Server.”

- “Automating IPS License File Updates” will include this information:

  Before You Begin

You must first configure the IPS Update server to be Cisco.com, so that you can specify the Cisco.com username and password. For information on configuring Cisco.com as the IPS Update server, see “Configuring the IPS Update Server.”

- “Configuring the IPS Update Server” will include this information:

Tip If you are using a device that requires a Cisco.com login for updating licenses, such as an IPS 4270 or an AIP SSM-40 in an ASA device, you must configure the IPS Update server as Cisco.com. You cannot use a local server.

Understanding ASCII Limitations for Text

The user guide and online help will be updated with the following information in the “Working with the Security Manager User Interface” chapter:

“Devices typically restrict text to ASCII characters. If you include non-ASCII characters in Security Manager text fields that are used to generate commands in a device configuration file, the presence of those characters can prevent the configuration file from loading on the device. For example, a non-ASCII character in an interface description for an FWSM can prevent the device from loading the startup configuration when you restart the device.

Make sure that you do not include ASCII characters in any text field in Security Manager.”

Policy Discovery Restriction for Adding Devices Using Configuration Files

One of the ways you can add devices to Security Manager is to use the device’s configuration file. This method adds the device without Security Manager contacting the device. However, if you add a device using a configuration file, and discover security policies while adding the device, Security Manager cannot successfully discover policies that require that files be downloaded from the discovered device. This especially affects devices that include the **svc image** command in a web VPN configuration. The following paragraph will be added to the “Adding Devices to the Device Inventory” section in the “Managing Devices” chapter of the user guide as one of the cons of adding devices using configuration files:

“Also, you cannot successfully discover policies that require a connection with the device. For example, if a policy points to a file that resides on the device, adding the device using the configuration file will result in a Security Manager configuration that includes the **no** form of the command, because Security Manager cannot retrieve the referenced file from the device. For example, the **svc image** command for web VPNs might be negated.”

Using AUS with a Custom HTTPS Port Number for Security Manager Server

This documentation update applies to the *Online Help for Auto Update Server 3.2*.

The following is additional information regarding using AUS to manage devices added to Security Manager, and applies to the “Interoperation of AUS and Cisco Security Manager” topic:

If you change the HTTPS port number of the Security Manager to any port number other than the default value using the changeport.exe command, you must also update the port number of AUS in the Port field of the Auto Update Server Properties dialog box (click Edit Server from the Auto Update field in General page of Device Properties). Otherwise, deployment to AUS-managed devices fails.

Limit on the Number of Keywords Supported for MARS Events Lookup from a Policy

This documentation update applies to the *Online Help for Cisco Security Manager 3.2*.

Replace the line describing the limit on the number of keywords supported during MARS events lookup from a Security Manager policy in the “Obtaining Events for an Access Rule Policy” section of the “Using Monitoring, Troubleshooting, and Diagnostic Tools” topic with the following description:

If the number of keywords or the sum of the number of sources, destinations, and protocols for an ACE or a signature exceeds the permissible limit of 150, an error message is displayed in the MARS GUI. The error message displays the possible cause and recommended action.

Where To Go Next

Table 18 Where To Go Next

If you want to:	Do this:
Install Security Manager server or client software.	See *Installation Guide for Cisco Security Manager 3.2.1*.
Understand the basics.	See the interactive *JumpStart* guide that opens automatically when you start Security Manager.
Get up and running with the product quickly.	See “Getting Started with Security Manager” in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager 3.2.1*.
Complete the product configuration.	See “Completing the Initial Security Manager Configuration” in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager 3.2.1*.
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 2 of *User Guide for Cisco Security Manager 3.2.1*. • Setting Up User Permissions • Integrating Security Manager with Cisco Secure ACS
Bootstrap your devices.	See “Preparing Devices for Management” in the online help, or see Chapter 5 of *User Guide for Cisco Security Manager 3.2.1*.
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 *Installation Guide for Cisco Security Manager 3.2.1*.

Related Documentation

Table 19 describes the product documentation that is available. For information on ordering printed documents, see Obtaining Documentation and Submitting a Service Request, page 30.

Table 19 Product Documentation

Document Title	Available Formats
Guide to User Documentation for Cisco Security Manager 3.2.1	• Printed version included with product. • 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/3.2.1/roadmap/CSM321Map.html
Installation Guide for Cisco Security Manager 3.2.1	• 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/3.2.1/installation/guide/csmig321.html
User Guide for Cisco Security Manager 3.2.1	• 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/3.2.1/user/guide/UserGuide.html
Supported Devices and Software Versions for Cisco Security Manager 3.2.1	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2.1/compatibility/information/csmsdt321.html
FAQ and Troubleshooting Guide for Cisco Security Manager 3.2	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
Migrating from CiscoWorks VPN/Security Management Solution to Cisco Security Manager	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
High Availability Installation Guide for Cisco Security Manager 3.1	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
User Guide for Auto Update Server 3.2	• 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
Supported Devices and Software Versions for Auto Update Server 3.2	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.2/compatibility/information/aus_dev.html

Table 19 Product Documentation (continued)

Document Title	Available Formats
Security Manager Integration with ACS	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6498/products_configuration_example09186a00808eada8.shtml
Release Notes for Cisco Security MARS Appliance 4.3.4	On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html
Release Notes for Cisco Security MARS Appliance 5.3.4	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.

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.