



Release Notes for Cisco Security Manager 3.2

Revised: June 20, 2008

Contents

- [Introduction, page 2](#)
- [What's New in Security Manager 3.2, page 3](#)
- [Installation Notes, page 4](#)
- [Cisco Security Manager 3.2 Download and Installation Instructions, page 5](#)
- [Cisco Security Manager 3.2 Service Pack 2 Download and Installation Instructions, page 5](#)
- [Important Notes, page 6](#)
- [Resolved Problems, page 8](#)
- [Known Problems, page 14](#)
 - [AUS Known Problems, page 14](#)
 - [Backup and Restore Known Problems, page 15](#)
 - [Catalyst 6500/7600 Configuration, page 15](#)
 - [Client Software, page 15](#)
 - [Deployment, page 16](#)
 - [Device Management, page 16](#)
 - [Diagnostics, Monitoring, and Troubleshooting Tools, page 17](#)
 - [Discovery, page 18](#)
 - [Firewall Services, page 18](#)
 - [Installation and Upgrade, page 20](#)
 - [IPS and IOS IPS, page 21](#)
 - [PIX/ASA/FWSM Configuration, page 26](#)
 - [Policy Objects, page 28](#)
 - [Router Configuration, page 28](#)
 - [Site-to-Site/Remote Access/SSL VPN Configuration, page 29](#)
 - [Tools, page 30](#)
 - [User Interface, page 31](#)
- [Documentation Updates, page 32](#)
 - [Using AUS with a Custom HTTPS Port Number for Security Manager Server, page 32](#)
 - [Limit on the Number of Keywords Supported for MARS Events Lookup from a Policy, page 32](#)
- [Where To Go Next, page 33](#)
- [Related Documentation, page 33](#)
- [Obtaining Documentation and Submitting a Service Request, page 35](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

Introduction

**Note**

This document is occasionally updated after initial release; therefore, a hardcopy or PDF version of the document might not contain the latest information. We recommend that you refer to the online version (http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2/release/notes/csmrn32.html) whenever possible.

**Note**

This document is to be used in conjunction with the documents listed in the [Related Documentation, page 33](#).

This document contains release note information for the following:

- **Cisco Security Manager 3.2 (including Service Pack 2)**

Cisco Security Manager (Security Manager) enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of firewall, VPN, and IPS services across IOS routers, PIX and ASA security appliances, and 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**

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, we recommend that you read this entire document. However, it is critical that you read the “Important Notes” section on page 6, the “Installation and Upgrade” section on page 20, and the *Installation Guide for Cisco Security Manager 3.2* before installing or upgrading to Cisco Security Manager 3.2.

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

- In Service Pack 2, support for the Cisco IPS E2 Engine Update. After E2 is released, all new Cisco IPS signature releases will require E2.
- Improved integration between Cisco Security Manager and CS MARS (requires CS MARS version 4.3.4, 5.3.4, or a later release).
 - Security Manager now supports integration with multiple instances of CS MARS.
 - Support for connection establishment and teardown syslog messages for policy lookup from MARS events and events lookup from Security Manager policies.
 - The Signature Summary table in Security Manager 3.2 (IPS > Signatures > Signatures) enables navigation to MARS to view the realtime or historical events detected by the selected signature. You can also select multiple signatures from the Signatures policy table and view events generated by them.
 - The Access Rules page in Security Manager 3.2 (Firewall > Access Rules) enables you to select an ACE and navigate to the realtime and historical events generated by the ACE in MARS. For events matching a rule, only events generated by access rules are displayed. However, for events matching a flow, events generated by connection setup/teardown are also displayed in addition to those generated by firewall access rules in the Query page of MARS. You can also look up historical and realtime events matching the source or destination address of an ACE.
 - The Query Results and Incident Details pages in MARS enable you to look up and modify the access rule in Security Manager that generated the event. Using MARS, you can also navigate from events that are generated during the establishment or tearing down of a TCP, UDP, or ICMP connection to the permit ACE in Security Manager for that specific event. You can start the Security Manager client from the read-only policy lookup table in MARS and modify the matching rules, without having to open the client in a separate session.
 - The Query Results and Incident Details pages in MARS enable you to look up and modify the signature in Security Manager that generated the event on IPS and IOS IPS devices. For IPS events, MARS displays the read-only popup window from which you can click Edit Signature to navigate to the Signatures policy page in Security Manager and modify the matching IPS signature. You can also click Event Action Filter from the read-only popup window to configure a filter on the basis of signature categories to remove one or more actions from the signature event.
- Support for FWSM 3.2(2) and 3.2(3).
- Support for ASA 7.2.2, 7.2.3, and 7.2.4.
- ASA 8.0/8.1 Support:
 - Firewall, Firewall Settings, and Platform support for all features that are backwards-compatible with 7.2.2 features.
 - Support for Netflow logging.
- Support for ASA 5580-20 and 5580-40.
- Support for 3200 Series routers.
- Support for 2600XM routers.
- Support for 1861 ISR router.
- Support for configuration of RACLs, Interfaces, VLANs, Port Security, and FlexConfigs on Catalyst 3550, 3560, 3560E, 3750, 3750E, 3750 Metro, 4500 Series, 4948, and 4948 10GE switches.
- Support for IOS 12.2(33) SRA and SRB on the 7600 platform.

- Cisco Security Manager 3.2 supports the Cisco Intrusion Prevention System Advanced Integration Module (AIM-IPS). You can install AIM-IPS in Cisco 1841, 2800 series, and 3800 series routers.
- Notification for expiring rules.
- Enhancements to the Copy Policies feature.
- Improved inventory import/export support.
- Enhancements to email notifications.
- Display of inheritance information for policies.
- Deployment schedules.
- Windows Vista support for Cisco Security Manager client.
- Support for Internet Explorer 7.x and Firefox 2.x.
- High-availability support for IEV.
- Cisco Security Manager 3.2 supports the Cisco IPS 4270-20 Sensor.

Installation Notes

You can install Security Manager 3.2 server software directly, or you can upgrade the software on a server where either Security Manager 3.0.2, 3.1, or 3.1.1 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](#) for important information regarding server requirements, server configuration, and post-installation tasks.



Note

The 12 known problems that were resolved in Security Manager 3.1.1 SP3 are not available in Security Manager 3.2. Therefore, if you upgrade to 3.2 from 3.1.1 SP3, you will lose the added functionality that was provided in 3.1.1 SP3.

Before you can successfully upgrade to Security Manager 3.2 from a prior version of Security Manager (versions 3.0.2, 3.1, or 3.1.1 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](#).



Note

Service packs cannot be installed by themselves. They are intended for installation on an existing installation of Cisco Security Manager 3.2. Service Pack 2 is a superset of Service Pack 1, so you can install Service Pack 2 with or without installing Service Pack 1 first. For more information, see [Cisco Security Manager 3.2 Service Pack 2 Download and Installation Instructions, page 5](#).

Cisco Security Manager 3.2 Download and Installation Instructions

**Note**

The 12 known problems that were resolved in Security Manager 3.1.1 SP3 are not available in Security Manager 3.2. Therefore, if you upgrade to 3.2 from 3.1.1 SP3, you will lose the added functionality that was provided in 3.1.1 SP3.

To download and install Cisco Security Manager 3.2:

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](#).

Step 3

Download fcs-csm-32-w2k-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](#).

**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.

Cisco Security Manager 3.2 Service Pack 2 Download and Installation Instructions

Service Pack 2 is a superset of Service Pack 1, so you can install it with or without installing Service Pack 1 first.

**Note**

Some of the known problems that were resolved in Security Manager 3.1.1 SP3 are not available in Security Manager 3.2 SP1. Therefore, if you upgrade to 3.2 from 3.1.1 SP3, you will lose the added functionality that was provided in 3.1.1 SP3.

To download and install Cisco Security Manager 3.2 Service Pack 2:

- Step 1** Log in to Cisco.com.
- Step 2** Navigate to <http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app>.
- Step 3** Download the file fcs-csm-320-sp2-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 FCS build (with or without Service Pack 1) on your server if you have not already done so.
- Step 7** Run the fcs-csm-320-sp2-win-k9.exe file that you previously downloaded.
- Step 8** In the Install Cisco Security Manager 3.2 Service Pack 2 dialog box, click **Next**, and then click **Install** in the next screen.
- Step 9** After the updated files have been installed, click **Finish** to complete the installation.

**Note**

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

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 17.
- Performance Monitor is not available for installation from the Security Manager 3.2 DVD. If you are running Security Manager 3.1 and Performance Monitor 3.1 on the same system and upgrade Security Manager to 3.2, Performance Monitor stops working. This problem occurs because of the difference in the version of Common Services between Security Manager 3.2 and Performance Monitor 3.1.

We recommend that you install Security Manager and Performance Monitor on separate systems. Also, we recommend that you do not upgrade Security Manager to 3.2 if you have Performance Monitor 3.1 running on the same server. The next version of Performance Monitor, 3.2, will be released shortly, at which point, both the applications can coexist on the same server.

- 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. 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 upgrade to Security Manager 3.2 from Security Manager 3.0.2, the ordering of BGP CLI “neighbor distribute-list acl” may be shown incorrectly in preview full configuration due to Security Manager 3.0.2 bugs [CSCsk55138](#) and [CSCsk55140](#). To correct this, please rediscover this 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, 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 2 is a superset of Service Pack 1, so it contains all of the problem resolutions included in Service Pack 1 as well as those in Service Pack 2 itself.

- [Table 1](#) identifies the problems resolved by Security Manager 3.2 Service Pack 2.

- [Table 2](#) identifies the problems resolved by Security Manager 3.2 Service Pack 1.

[Table 3](#) identifies the problems that were documented in the Security Manager 3.1.1 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.

**Note**

Known problems that were resolved in Security Manager 3.1.1 SP3 are not available in Security Manager 3.2. Therefore, if you upgrade to 3.2 from 3.1.1 SP3, you will lose the added functionality that was provided in 3.1.1 SP3.

Table 1 *Resolved Problems in Service Pack 2*

CSCsq42037—CSM should push AIM specific packages to AIM device

Description: This problem occurs after downloading (in Cisco Security Manager) an Advanced Integration Module (AIM)-specific 6.0(5)E2 package and standard 6.0(5) package from Cisco.com. The problem is that the user cannot deploy the AIM-specific 6.0(5)E2 package to AIM.

CSCsq02485—Deploy job fails when engine update is pushed to AIM

Description: This problem occurs after downloading (in Cisco Security Manager) the E2 engine upgrade package and an E2-based signature update from Cisco.com. The problem is that Cisco Security Manager fails to push the E2-based signature update to the Advanced Integration Module (AIM).

Table 2 *Resolved Problems in Service Pack 1*

CSCsl13733—Two policies in the same policy group have same order_id

Description: A duplicate order_id in the same policy group might occur when multiple firewall policy groups are modified with an insertion.

CSCsl37261—In a single interface dev,InlinePairName is stored even after cancelling

Description: While creating an inline interface pair, if you cancel the create dialog or an error occurs, the Cisco Security Manager interface retains the inline pair name.

CSCsl74264—Deployment or Config Archive rollback fails on IOS/IPS devices

Description: An error occurs when deployment job or Config Archive rollback is performed on an IOS/IPS device.

CSCsl85278—Edit is not working for inline pair when interface contains vlan-group

Description: In an IPS sensor, after the user clicks Interface and adds an inline pair, and then creates a VLAN group using that inline pair, the user cannot edit the inline pair. The inline pair can be edited if the VLAN group is deleted. After editing, the VLAN group can be added back.

CSCsl85296—Inline pair should not be listed in vlan-group for IDSM

Description: Cisco Security Manager lists IDSM inline interface pairs in the VLAN groups interface list.

CSCsm53472—Auto refresh text on Deployment Manager should be black

Description: The fonts used for the auto refresh text in Deployment Manager is difficult to read.

CSCsm63057—Rediscovery IOS router failed with JDOM exception while parsing XML input

Description: Discovery/Rediscovery/Deployment fails with a JDOM exception when http authentication has not been correctly set up on a device or if the user does not have the correct privilege level assigned.

Table 2 *Resolved Problems in Service Pack 1 (continued)***CSCsm78461—CSM does not discover vlan group assigned to VS for IPS device**

Description: The subinterface of a VLAN group assigned to a virtual sensor is not discovered under the following conditions: For an IPS device, use CLI to add an inline pair interface, and then create a VLAN group, using this inline pair interface, with a subinterface.

CSCsm79337—Performance tuning on platform validations

Description: While submitting changes to the device, Security Manager hangs for a long time at the validating screen.

CSCso00786—FWSM discovery completed before the policy discovery of VCs

Description: All policies are deleted on the Security Contexts when you deploy to a device or when you do a preview config.

CSCso00883—Scheduled deployment job reports 'device not available' at deploy time

Description: Scheduled deployment job reports that devices are not available when the scheduled time elapses. This problem is known to occur on Catalyst 6000 devices only.

CSCso06513—IEV reports stop working after upgrade to Security Manager 3.1.1 or 3.2

Description: After you upgrade from Security Manager 3.1 to 3.1.1 or 3.2, the three default reports in the IEV client started from Security Manager: Top Alerts, Top Attackers, and Top Victims, stop functioning.

CSCso09627—Change ids mode causes out of sync between CSM and router

Description: Synchronization between Security Manager and AIM-IPS modules is lost when the user attempts to configure more than one monitoring mode (inline and promiscuous).

CSCso20860—"access-list mode auto-commit" sent to standby unit fails discovery

Description: Security Manager 3.1.1 discovering an FWSM 3.1(x) blade in multi-context mode with active/active failover configured fails.

CSCso23669—Invalid VPN hard validation error for non-support for TACACS+

Description: TACACS+ should be supported for authentication for remote access purposes.

CSCso28542—IOSIPS CTs should not be used when user is not using IOSIPS feature

Description: Cisco Security Manager attempts to connect to the IPS subsystem during deployment on an IOS-IPS device even if the user is not managing the IPS subsystem on the device. This results in deployment failure if HTTPS is not configured on the device.

CSCso46006—FlexConfigs not editable

Description: In certain situations, a FlexConfig might become locked and uneditable.

CSCso51830—Preview delta contains "no pdm history enable"

Description: The "no pdm history enable" command is incorrectly imported as part of an object-group.

CSCso52320—Deployment to PIX 6.3 devices fails with error in transcript

Description: When you deploy large configuration changes to PIX 6.2 devices, deployment fails with the "Error: 24112 : IO error during SSL communication" message recorded in the transcript.

CSCso53513—LDAP Attr Map: predefined attribute name changed in 8.0

Description: Cisco Security Manager doesn't support changes to LDAP attributes in ASA 8.0.

CSCso60422—PIX Interface: add support on discovery "no shutdown" from config file

Description: Cisco Security Manager does not properly support the "no shutdown" command.

CSCso66342—Cannot discover WS-C3550-24-PWR, 3750-24TS

Description: Need support for importing Cisco Catalyst 3750-24TS switches and Cisco Catalyst 3550-24 PWR switches.

Table 2 *Resolved Problems in Service Pack 1 (continued)***CSCso75616**—IPS Discovery fails when hostname is entered w/o ip address

Description: Discovery of an IPS sensor fails if only the host name is supplied.

CSCso90637—Cannot add firewall rules after upgrade from 3.1 to 3.2

Description: After upgrading to Cisco Security Manager 3.2 from an earlier version, changes to the access rules of a firewall are not saved.

CSCsq01937—admin settings can't be retrieved properly after migration

Description: After upgrading to Cisco Security Manager 3.2 from an earlier version, admin settings are not retrieved properly.

CSCsq02803—FWSM Context discovery fails

Description: Context discovery fails for ASA multi mode devices running 2.x images with both standalone discovery and discovery through a chassis.

Table 3 *Resolved Problems in Security Manager 3.2***CSCsd30481**—PIX 6.3: needs warning for the Time Range object in access rules

Description: When you create an access rule for a PIX 6.x device, you can specify a time range in the GUI; however, the device does not support the time range feature in the ACE and no warning is displayed during activity validation or deployment.

CSCsd38176—Logging rate limit - discovery and deployment do not use logging level

Description: Values in the Logging Level column of the Individually Rate Limited Syslog Messages table are not used and are overwritten after rediscovery.

CSCsd39354—Some Windows users see no desktop shortcut or Start menu shortcut

Description: On a PC with many users, only the person who installs Security Manager Client can see the desktop and Start menu shortcuts that show that Security Manager Client is installed.

CSCsd61768—"policy-map" cmds renamed on initial deployment without policy changes

Description: Device import discovers an enabled policy map and its related commands as service policy rules and traffic flow objects. Security Manager does not preserve the original policy map names on a device.

CSCsg45483—Dynamic NAT rules duplicated without removing original rules

Description: Dynamic NAT rules that are discovered are duplicated by Security Manager without removing the original rules during the next deployment.

CSCsh42944—NAC policy deployment fails on Layer 2 interfaces

Description: Deployment fails for a Network Admission Control (NAC) policy. The **ip admission** command is not recognized on the device.

CSCsh57310—Static NAT network rule flagged as invalid

Description: A static NAT network rule that was discovered from a device configuration is flagged as invalid during activity validation.

CSCsh85196—Apache server fails to start due to dll name conflict

Description: If other software that uses OpenSSL (such as Legato or Veritas backup software) is installed on the same machine as Security Manager, the apache server fails to start.

CSCsh86808—Sig policy icon is blank after being removed from shared sig policy

Description: The signature policy icon appears blank when the device is removed from a shared signature policy.

Table 3 *Resolved Problems in Security Manager 3.2 (continued)***CSCsh91913—Auto Update fails on ASA devices with auto-signon**

Description: When you enable an SSL VPN connection profile on an ASA security appliance managed by AUS and configure the auto-signon command in an ASA user group, deployment of configuration changes to the device fails when you enable the device to request AUS for updates. This problem occurs when the same auto-signon commands have been configured in the same ASA user group on the device. Although deployment is shown as successful in the Deployment Manager window, an error is recorded in the AUS event report that the file was not downloaded to the device.

CSCsh93894—AUS deployment fails if PKI trustpoint sub-commands are in reverse order

Description: When you configure a PIX device with a PKI configuration, AUS deployment fails because Security Manager generates the CLI commands in the wrong order.

CSCsi04942—IEV error while installing only Common Services 3.0.5 or AUS 3.1

Description: When you install only Common Services 3.0.5 or AUS 3.1 from the Security Manager DVD, an IEV error message is displayed even if you did not select Security Manager 3.1 during installation.

CSCsi09998—LDAP server URL required for CA servers that do not run LDAP protocol

Description: In a site-to-site VPN configuration, the LDAP Server URL field in the CA Information tab of the PKI Enrollment dialog box is mandatory if one of the “CRL...” options is selected from the Revocation Check Support list. This means you cannot add a CA server to a PKI object without entering the URL of the LDAP server from which the CRL is downloaded, even if the CA server does not use LDAP as the querying protocol for revoking certificates on the device.

CSCsi11214—CDP disabled for mGRE tunnels when ODR defined for large scale DMVPN

Description: When you deploy to a large scale DMVPN topology after configuring On-Demand Routing (ODR) as the routing protocol, the Cisco Discovery Protocol (CDP) is not enabled for the multipoint GRE (mGRE) tunnels. This problem occurs when CDP is not enabled at the global level on all supported interfaces.

CSCsi11854—Static routes not generated on devices in GRE Dynamic IP tunnel

Description: In a hub-and-spoke VPN topology in which the assigned technology is GRE Dynamic IP, when you configure a static routing protocol as your secured IGP, the CLI commands for static routes are not generated for the protected networks in the tunnel.

CSCsi16871—SDP - Invalid characters not detected in device name formula

Description: Deployment fails due to invalid characters defined in the SDP device name formula.

CSCsi23683—Deployment fails when you reconfigure bridge-groups in transparent rules

Description: When you associate interfaces with another bridge-group and provision it in Security Manager, the deployment shows an error; however, the device in this case has been provisioned correctly.

CSCsi27208—OSPF Interface - field values cannot be removed and saved when editing

Description: If you delete the contents of a text field when editing an OSPF interface policy, Security Manager does not save the changes.

CSCsi34298—Webfilter: Deployment fails if overlapping filter commands are defined

Description: If two filter commands of the same type are defined with the same port ranges (service) or overlapping port ranges and overlapping networks, deployment to a device fails. The device does not accept overlapping filter commands.

CSCsi35479—HTTP policy: Commands generated for every deployment

Description: For ASA 7.2 HTTP Maps, if the body match maximum is set to 0 (zero), the device accepts the command as “body-match-maximum” but shows it in show run as “body-match-maximum 0”. This causes the delta to always contain the removal of the http policy-map subcommands and adding them back.

Table 3 *Resolved Problems in Security Manager 3.2 (continued)*

CSCsi45209—Static routing - deployment failure after DB upgrade

Description: Deployment and preview configuration fail for static routing policies after a database upgrade.

CSCsi50311—OSPF MD5 key not removed if interface authentication is clear-text/none

Description: When you change the authentication type used by an OSPF interface from MD5 to clear-text or disable authentication, the identification number of the MD5 authentication key (**ip ospf message-digest-key** command) is not removed from the interface after deployment.

CSCsi50493—DataLoader's load method needs to handle quotes

Description: The access rules table might not finish loading for a newly discovered device if the discovered configuration has access-list remarks that contain quotes or double quotes.

CSCsi55374—aaa authorization network cli not generated on a device for PPA policy

Description: If you select the Custom Method List option to use a remote AAA server for authorization in a PPP policy and modify the default authorization method defined in the AAA policy, the AAA authorization command for network connections is not generated on the device after deployment.

CSCsi56618—aaa authorization network cli is not generated in preview config for PPA

Description: If a router has been configured to use the default authorization method defined in the AAA policy for a PPP connection and the AAA network authorization settings are changed in the AAA policy, the **aaa authorization network {default | list-name}** command might not be generated in the preview configuration due to a conflict with the authorization method defined in the PPP policy.

CSCsi87422—Security Mgr does not allow overlapping globals on different interfaces

Description: When you create overlapping global rules on different interfaces for PIX/ASA/FWSM devices, Security Manager returns an error about overlapping IP ranges even though the global interfaces are different.

CSCsj16898—Inspection rule for WAAS is not discovered in FWSM 3.2(0)89

Description: WAAS inspection rules are not shown in the inspection rules table for FWSM devices.

CSCsj17336—Inspect rule: DCE RPC policy map and inspect rule not discovered

Description: DCE RPC inspection maps are not shown in the inspection rules table or the policy object manager.

CSCsj62074—Blocking: Unable to edit the interface under Router tab

Description: Unable to edit the interface name and direction of a blocking interface under the “Router” and “Catalyst 6500” tabs of the IPS Blocking policy.

CSCsj64024—Find is not working for contracted local rules

Description: Find/Replace does not find any matching results even though the value to search for does exist in the rule table.

CSCsj97405—AAA include/exclude command modelled incorrectly

Description: The AAA include/exclude commands can each have multiple instances, but the current rule file models them as a single instance command and therefore leaves only one instance after processing.

CSCsk19314—Upgrade 3.0.2 to 3.1.1: Deploy fails if dynamic NAT rules exist on dev

Description: Deployment to file or device might fail with a Null Pointer Exception for an IOS router device with NAT rules configured.

CSCsl41758—VLAN pair editing of interface - OK doesn't save changes

Description: After a vlan inline pair is created, if you try to modify the interface name, the edit vlan inline pair UI screen does not allow you to save the changed information.

Known Problems

This section contains information about the problems known to exist in Cisco Security Manager 3.2. 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.

- [AUS Known Problems, page 14](#)
- [Backup and Restore Known Problems, page 15](#)
- [Catalyst 6500/7600 Configuration, page 15](#)
- [Client Software, page 15](#)
- [Deployment, page 16](#)
- [Device Management, page 16](#)
- [Diagnostics, Monitoring, and Troubleshooting Tools, page 17](#)
- [Discovery, page 18](#)
- [Firewall Services, page 18](#)
- [Installation and Upgrade, page 20](#)
- [IPS and IOS IPS, page 21](#)
- [PIX/ASA/FWSM Configuration, page 26](#)
- [Policy Objects, page 28](#)
- [Router Configuration, page 28](#)
- [Site-to-Site/Remote Access/SSL VPN Configuration, page 29](#)
- [Tools, page 30](#)
- [User Interface, page 31](#)

AUS Known Problems

Table 4 *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.

Backup and Restore Known Problems

Table 5 Backup and Restore Known Problems

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.

Catalyst 6500/7600 Configuration

Table 6 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.

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.

Client Software

Table 7 Client Software

CSCsk41218—Client uninstall not cleaning out install dir; install JVM unintuitive

Description: When you upgrade to Security Manager 3.1.1 from 3.0.2, you are prompted that a Java Virtual Machine is being installed and you are asked if you want to override the directory. No is preselected, but you should select Yes.

CSCsm99798—Installing Security Manager client fails with CSA enabled

Description: When you install Security Manager client 3.2, security applications, such as Cisco Security Agent that are running on your system, might prevent the execution of certain installation steps and the operation fails.

Deployment

Table 8 *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”.

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.

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.

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.

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.

Device Management

Table 9 *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.

CSCsi31224—Preview failed after deploying config to AUS server

Description: A device’s certificate is changed after retrieving the config file from the AUS server. The certificate stored in Security Manager would be out of sync with the device, hence cause the preview to fail with certificate mismatched error.

Diagnostics, Monitoring, and Troubleshooting Tools

Table 10 *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.

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.

Table 10 *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.

Discovery

Table 11 *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.

CSCsi14676—Discovery hangs for FWSM with 100+ contexts

Description: When using HTTPS as the transport protocol, the connection to the security contexts in an FWSM can hang if the connectivity between the Security Manager server and the device is unstable.

CSCsi45142—AAA - source intf disc from global cmd instead of aaa subcommand

Description: The interface parameter is not discovered for the AAA-server building block discovered from IOS routers.

CSCsi70926—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 12 *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.

Table 12 Firewall Services (continued)

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.

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.

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.

Table 12 Firewall Services (continued)

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.

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.

Installation and Upgrade

Table 13 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.

CSCsl70951—Upgrade from 3.0.2 to 3.2: PIX 7.2 Neighbor Filter Policies Not Shown

Description: If you upgrade from Security Manager 3.0.2 to 3.2, and the inventory includes PIX 7.2 devices with RIP configurations, the device policies do not display two new multicasting policies. Delete the devices from the inventory and rediscover them.

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.
```

CSCsm22070—Inline upgrade from 3.0.2 to 3.2 fails if CSA is running

Description: If Cisco Security Agent is enabled on your system when you are performing an inline upgrade from Security Manager 3.0.2 to 3.2, the installation stops when the Stopping CSAgent screen is displayed.

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.

Table 13 *Installation and Upgrade (continued)***CSCso48972—Upgrade:3.0.2SP1 to 3.2 - Client Installer link on CSMS homepage fails**

Description: This defect is seen upon Cisco Security Manager 3.0.2 SP1 upgrade to Cisco Security Manager 3.2. The user sees an HTTP “403 Forbidden” error when trying to download the Cisco Security Manager Client Installer from the Cisco Security Management Suite Web page. Workarounds are available in the full description of this defect in the Bug Toolkit at [CSCso48972](#).

CSCso56912—Upgrade to Security Mgr 3.2 from 3.1.1 SP3 excludes fixes made to SP3

Description: The 12 known defects that were resolved in Security Manager 3.1.1 SP3 are not available in Security Manager 3.2.

IPS and IOS IPS

Table 14 *IPS and IOS IPS***CSCse95933—IPS related policies should be listed in device properties page**

Description: In the device properties page, under the policy object overrides, policies which are not needed for IPS are listed but should not be.

CSCsf24765—Summary page missing names for VLAN & promiscuous VLAN groups

Description: The Interface summary tab does not have columns for VLAN Pair name or VLAN group name. This can be observed after creating a VLAN pair or VLAN group and then viewing the Summary tab.

CSCsg24936—SigTuning: Handling of special policy names

Description: The IPS policy names “Default” and “Local” are used with special meaning, but a user can create a policy with these names, potentially causing confusion.

CSCsg25899—6.x related pol should not be listed for 5.x devices in copy & share policy

Description: When copying policies or sharing policies with an IPS 5.1 device as the source, the policy tree contains the IPS 6.0 policies Anomaly Detection and External Product Interface, even though these are IPS 6.0 policies.

CSCsg26218—Icon next to NTP shows the NTP is not default when it is not the case

Description: When an IPS 4240 device is added without configuring an NTP server, so that default NTP values are in effect, the icon next to NTP is shown with the dotted lines, which indicates, incorrectly, that the policy is changed from the default.

CSCsg38052—VLAN groups need to display “unassigned” VLANs

Description: When the VLAN groups are set to unassigned nothing is displayed in the vlan groups tab VLANs tab or the Summary page VLANs tab.

CSCsg51052—After Abort, progress bar continues to 100% and Status remains Started

Description: This defect occurs after clicking the Update via CCO button on the Tools > Admin > Licensing > IPS page. If “cancel” is clicked, the progress bar shows 100% and the operation is stopped, but the status displayed does not change from “starting.”

CSCsg80289—Warning message is displayed during blocking policy deployment.

Description: This defect occurs when configuring the user profile and master blocking policies on an IPS 6.0 device. A warning message appears even though deployment is successful.

Table 14 IPS and IOS IPS (continued)

CSCsh02407—Autoupdate setting value for a device should be same in device tree

Description: This defect occurs in the “Apply update To:” table on the Tools > Security Manager Administration > IPS update page. When a setting for one device is changed in one group, the setting for the same device listed under another group is not updated.

CSCsh36604—EAO: After editing row, the edited row is displayed as a last row

Description: For certain policies which contain information in a table, if a user edits a row, afterwards the edited row will be moved to the last row in the table.

CSCsh52484—Licensing Date Varies between sensor CLI and sensor

Description: The license expiration date seen in the Security Manager client can disagree with the expiration date seen by using the CLI.

CSCsh53265—IPS, IPS update admin page, check box initialization

Description: The check boxes for shared signature policies in the “Apply Update To:” table on the Tools > Security Manager Administration > IPS Update page do not precisely reflect the update policy of a device that has a local signature policy inherited from the shared signature policies.

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 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.

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.

CSCsi14306—Download config to device fails during major upgrade

Description: While applying the major upgrade 6.0(1) to a device running 5.x, the package is successfully pushed to the device, but the deployment job fails with the error “Failed to download config to device.”

CSCsi18661—Deploy of new variable does not work

Description: This defect occurs when creating a policy object and then configuring allowed hosts, anomaly detection, or signature setting policies. After deploying the configuration to the device, the policy object name will not be kept in the device.

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.

Table 14 IPS and IOS IPS (continued)

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.

CSCsi45590—Cannot add IOS IPS device with TrendMicro V version

Description: IOS IPS devices that have Trend signatures on the device cannot be discovered by Security Manager.

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.

CSCsj60530—Inventory alone discovery fails for IPS6.x device for submit operation

Description: Activity validation after “Inventory” discover a device with virtual sensor fail due to no Allowed Host.

CSCsi83852—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.

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.

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.

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 CSM to a device that has out-of-band changes fails, too. Removing one entry from the device lets both operations succeed.

CSCsm53921—http sig: Click Select for port with default value in box, throws error

Description: Attempts to change ServicePorts (which is set by default to WEBPORTS) results in an error for service-http signatures.

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 14 IPS and IOS IPS (continued)

CSCsm57132—EditUpdateSchedule: 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.

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.

CSCsm73453—Error message not displayed for unsuccessful deployment in autoupdate.

Description: Unsuccessful deployments are not properly reported by email notifications after autoupdate.

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.

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.

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.)

CSCsm93961—Green field device modify sig params disassociate sig update assignment

Description: If an IOS IPS device is added as a greenfield device without selecting the IPS option in the “Add New Device” wizard, and then a signature update is applied, validation will fail.

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.

CSCsm93975—Green field device lost i/f rule association after config generation

Description: Full preview details regarding interface association are not shown correctly for a greenfield device when the IPS option is not selected in the Add New Device Wizard even though the real device does not have IPS enabled.

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.

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.

Table 14 IPS and IOS IPS (continued)

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.

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.

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.

CSCso11030—AIM-IPS:CSM should not allow adding IDS-sensor as monitoring intf

Description: Security Manager allows the user to add interface IDS-Sensor0/0 on AIM-IPS modules; in addition, deployment is allowed by Security Manager.

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.

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.

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.

CSCso21621—AIM-IPS:Delete Monitoring Interface fails until switch screens and redo

Description: This defect occurs after the user imports an AIM-IPS device with a monitoring interface. When the user navigates to the AIM-IPS policy and tries to delete the monitoring interface in the AIM-IPS Service Module Monitoring Settings table, deletion fails. If the user navigates to a different policy and returns to the AIM-IPS policy, deletion succeeds.

PIX/ASA/FWSM Configuration

Table 15 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.

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 15 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.

CSCsi62494—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.

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.

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.

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.

Table 15 *PIX/ASA/FWSM Configuration (continued)***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.

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.

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.

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.

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.

Policy Objects

Table 16 *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 17 *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.

Table 17 Router Configuration (continued)

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.

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.

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

Table 18 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.

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.

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.

Table 18 *Site-to-Site/Remote Access/SSL VPN Configuration (continued)***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.

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.

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*.

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.

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 **ssl 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.

Tools

Table 19 *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 20 *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.

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.

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 0-21

If you want to:	Do this:
Install Security Manager server or client software.	See Installation Guide for Cisco Security Manager 3.2 .
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</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</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</i> . <ul style="list-style-type: none"> • 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 <i>User Guide for Cisco Security Manager 3.2</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</i> .

Related Documentation

[Table 22](#) describes the product documentation that is available. For information on ordering printed documents, see [Obtaining Documentation and Submitting a Service Request](#), page 35.

Table 22 Product Documentation

Document Title	Available Formats
<i>Guide to User Documentation for Cisco Security Manager 3.2</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/docs/security/security_management/cisco_security_manager/security_manager/3.2/roadmap/CSM32Map.html
<i>Installation Guide for Cisco Security Manager 3.2</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/installation/guide/csmig32.html

Table 22 Product Documentation (continued)

Document Title	Available Formats
<i>User Guide for Cisco Security Manager 3.2</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/user/guide/UserGuide.html
<i>Supported Devices and Software Versions 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/compatibility/information/csmsdt32.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
<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</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</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/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, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, 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, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, 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. (0805R)

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.

© 2004-2008 Cisco Systems, Inc. All rights reserved.

