



Release Notes for *Cisco Security Manager 3.1*

Revised: January 22, 2009,
CDC Date June 1, 2007

Contents

Contents, page 1
Introduction, page 2
What's New in Security Manager 3.1, page 3
Security Manager 3.1, page 5
Important Notes, page 5
Security Manager Resolved Problems, page 6
Security Manager Known Problems, page 14
Catalyst 6500/7600 Configuration, page 14
Client Software, page 14
Configuration Archive, page 14
Deployment, page 15
Device Management, page 16
Diagnostics, Monitoring, and Troubleshooting Tools, page 16
Discovery, page 17
Firewall Services, page 17
Installation and Upgrade, page 20
Miscellaneous Issues, page 21
PIX/ASA/FWSM Configuration, page 21
Policy Objects, page 23
Router Configuration, page 23
Site-to-Site/Remote Access/SSL VPN Configuration, page 24
Tools, page 26
User Interface, page 26
Auto Update Server (AUS) 3.1, page 27
AUS Resolved Problems, page 27
AUS Known Problems, page 28
IPS and IOS IPS in Security Manager 3.1, page 28
IPS and IOS IPS in Security Manager Notes, page 28
IPS and IOS IPS in Security Manager Resolved Problems, page 29



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

© 2007 Cisco Systems, Inc. All rights reserved.

[IPS and IOS IPS in Security Manager Known Problems, page 29](#)
[Documentation Updates, page 31](#)
[IPS Event Viewer, page 32](#)
[New Features in Security Manager 3.1, page 32](#)
[Where To Go Next, page 32](#)
[Related Documentation, page 33](#)
[Obtaining Documentation, Obtaining Support, and Security Guidelines, page 35](#)

Introduction

This document contains release note information for the following:



Note

Before using Cisco Security Manager 3.1, we recommend that you read this entire document. However, it is critical that you read the [“Important Notes” section on page 5](#), the [“Installation and Upgrade” section on page 20](#), and the *Installation Guide for Cisco Security Manager 3.1* before installing or upgrading to Cisco Security Manager 3.1.

- **Cisco Security Manager 3.1**

Cisco Security Manager (Security Manager) enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of VPN and firewall services across IOS routers, PIX and ASA security appliances, and Catalyst 6500/7600 services modules (FWSM and VPNSM). 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 through to large networks with thousands of devices. Scalability is achieved through a rich feature set of shareable objects and policies and device grouping capabilities.

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

- **Auto Update Server 3.1**

The Auto Update Server (AUS) is a tool for upgrading PIX security appliance software images, ASA software images, PIX Device Manager (PDM) images, Adaptive Security Device Manager (ASDM) images, and PIX security appliance and ASA configuration files. Cisco IOS routers that have dynamic IP addresses communicate with AUS that is running the Cisco Networking Services (CNS) Gateway Protocol to provide their IP addresses.

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

- **IPS and IOS IPS in Security Manager 3.1**

Security Manager supports fully native IPS provisioning. The predecessor of this native IPS provisioning was the cross-launched component of Security Manager known as IPS Manager.

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 3.1

- Upgrade from Security Manager 3.0 and 3.0.1.
- Integrated IPS features. While Security Manager 3.0 allowed you to cross-launch the IPS Management Center to access IPS functionality, Security Manager 3.1 provides fully integrated IPS features.
- Native integrated Catalyst 6500/Cisco 7600 Router and VACL management.
- Ability to cross-launch IPS Event Viewer 5.2 to monitor IPS sensors.
- Ability to test the communication between Security Manager and devices that have been or are being added to the inventory.
- Ability to discover site-to-site and remote access VPNs.
- Ability to discover IOS router configurations.
- Ability to preserve user-defined ACL names.
- High availability.
- Embedded read-only access to SDM, ASDM, IDM, and IEV for monitoring of individual devices.
- Navigation to access rule policy for ACL-related syslog messages from the real-time syslog viewer of SDM 2.3.4 and ASDM 5.2.2.
- Navigation to IPS signature policy for IPS events from IEV Realtime Dashboard and Views tab.
- Enhanced reporting features, including device-centric policy report and inventory report.
- Device, interface, and VPN up/down status reported in inventory report.
- Detailed activity report for firewall and IDS devices.
- Ability to configure SSL VPN on IOS and ASA 7.1/7.2 devices.
- Cross-launch of RME SWIM for OS management.
- Ability to use Security Manager user login credentials to connect to devices.
- Ability to use Telnet as a transport protocol to communicate with IOS and Catalyst 6500/7600 devices.
- Enhanced device certificate retrieval support including bulk retrieval through CLIs.
- Support for the following additional features on IOS devices:
 - SSL VPN
 - Additional Easy VPN features
 - Line access
 - SSH configuration
 - Local time
 - Comprehensive AAA support
 - HTTP server
 - PPP
 - DSL/ATM
 - DNS
 - NFP

- Bridging (wireless)
- QoS TAC enhancements
- Authentication proxy enhancements
- Additional interface settings, such as IP redirect, IP reply, virtual reassembly, and others
- Additional firewall features, such as support for IM blocking, java list, DOS settings, and voice service inspection
- Additional IPSec VPN features, such as large-scale DMVPN, AIM III
- Support for the following additional features on FWSM 3.1:
 - More than one pair of layer 2 interfaces
 - SNMPv2c
 - Skinny video
 - Asymmetric routing
 - FTP authentication challenge
 - Destination NAT for multicast
 - 4K global statements
- Support for the following features on ASA 7.2 devices:
 - Easy VPN HW client parity with PIX 501/506/VPN3002
 - Dual ISP support
 - PPPoE
 - Home/Business VLAN support
 - Enhanced auto-update support
 - Dynamic DNS
 - HA - sub-second failover
 - Virtualization - resource manager
 - Extended usage of DNS domain names
 - Generic input rate limiting
 - MPF-based regular expression classification map
 - N2H2 HTTPS/FTP filtering support
- Support for the following features on FWSM 3.2:
 - L2 NAT/PAT
 - TACACS+ command enhancements
 - Xlate table bypass
 - H323 GUP support
 - Cut through proxy enhancements
 - RTSP PAT
- Support for AIM III (IPSec/SSL VPN)
- Support for IPS 5.1/6.0 and IOS IPS in IOS 12.4(11)Tx

- Support for the following features on IPS 6.0 devices:
 - Virtual sensors
 - Anomaly detection
 - Passive OS fingerprinting
 - Simplified custom signature creation
 - Signature update wizard, preview and tuning of new signatures
 - IPS signature update license management
 - External product interface (linkage of IPS sensor with CSA MC)

Security Manager 3.1

Important Notes

- Before you can successfully upgrade to Security Manager 3.1 from a prior version of Security Manager, you must make sure that the Security Manager database does not contain any pending data, meaning 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 and then back up your database before upgrading. For instructions, see “Upgrading Server Applications” in the *Installation Guide for Cisco Security Manager 3.1*.
- If you have installed any service packs on your server and you restore a database that was backed up prior to installing those services packs, you must reapply the service packs after restoring the database.
- When you perform a policy query in Security Manager, interface names are not case sensitive. However, when you perform a policy query in CS-MARS, interface names are case sensitive. For example, outside and Outside are considered exclusive by CS-MARS, while they are equivalent in Security Manager. As a result, a name logged in the syslog event might not match the name 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 Security Manager.
- Although FWSM 3.1 can support multiple L2 interface pairs, Security Manager allows you to specify a maximum of two L2 interfaces (a single interface pair) and one associate management IP address. This means only one bridge group with two named interfaces associated is provisioned with a management IP address. A named interface is an interface that is configured with the “nameif” subcommand. If the device configuration contains a maximum of one bridge group and two named interfaces, it is valid for discovery. All other scenarios result in an error message and the commands are ignored during discovery. Furthermore, discovery does not show any bridge-group information in the GUI, but the bridge-group commands are generated during deployment. The bridge group 1 is deployed and used in the transparent rule policies if no bridge group exists in the device configuration. Discovery will stop and display an error if it imports an FWSM 3.1 device configuration that contains more than two named interfaces or more than one bridge group.
- 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.

- For the CS-MARS cross-launch panel to appear on the Cisco Security Manager Suite home page, you need to manually register the CS-MARS appliance on the Common Services application registration page. To do this, perform the following:
 1. From the Cisco Security Manager Suite home page, click the **Server Administration** link. The Common Services Admin page appears.
 2. Select **HomePage Admin > Application Registration**. The Application Registrations Status page appears.
 3. Click **Register**. The Choose Location for Registrations page appears.
 4. Select **Register From Templates**, then click **Next**.
 5. Select **Monitoring, Analysis and Response System**, then click **Next**.
 6. Enter the server name, server display name, and port and protocol information for the CS-MARS appliance, then click **Next**.
 7. Verify registration information, then click **Finish**. The CS-MARS launch point will now appear from the Cisco Security Manager Suite homepage.



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

Security Manager Resolved Problems

The following problems were documented in the Security Manager 3.0.1 release notes as known problems and have since been resolved.

Table 1 Resolved Problems

CSCsa81102—Need log input option when creating access rules for IOS devices

Description: Security Manager does not support the ACE option “log input” when you configure access rules on IOS devices that are managed by Security Manager. As a result, during discovery, Security Manager drops the option.

CSCsb64813—Installation fails on a server on which the PERL5LIB variable is set

Description: The PERL5LIB system environment variable is set on the server. During installation, an error message notes that perl58.dll cannot be found and installation fails.

CSCsb73828—System context should support NTP with interface

Description: If you enter an interface name when you configure an NTP server for the system context of an ASA device in multiple context mode, validation for that device fails.

CSCsc13977—Changes in ACS 3.3(x) do not take effect in Security Manager

Description: Changes that you make under Group Setup and Network Configuration in Cisco Secure Access Control Server (ACS) 3.3(x) are not reflected in Security Manager, even after you restart CiscoWorks Common Services and the Security Manager Client.

CSCsc39178—Changes lost when switching between Device view and undocked Map view

Description: Changes you made in Device view are lost after you edit the device in the undocked Map view. After you change the window focus from Device view to undocked Map view, you are not prompted to save the changes you made in Device view.

Table 1 *Resolved Problems (continued)***CSCsc42646—Full config needs negative form of some failover commands for PIX 6.x**

Description: If you remove a logical interface from Security Manager and you deploy the configuration to the device using AUS, the deployment fails.

CSCsc48462—ACEs with log-input option on IOS devices are removed after redeployment

Description: Although IOS devices support ACEs that have the option “log-input,” Security Manager does not support the feature. On deployment, the option is removed from the ACE.

CSCsc62714—Deployment fails if crypto ACL is not defined on peer device

Description: Deployment of a regular IPSec VPN fails on a PIX 6.3 device if one peer in the VPN topology uses an ACL to specify its protected networks and the other peers do not.

CSCsc66744—Client-server communication mechanism encountered “end of file” error

Description: While working in Security Manager from a client, the following error occurs: “Unknown Error. performBinaryRPC()...” When this occurs, “Premature EOF Error” entries are also logged in the client log file.

CSCsc80085—Router-SNMP community string is shown in clear text for all users

Description: The community strings defined in SNMP policies on Cisco IOS routers are displayed in clear text, even for users who are assigned roles with view-only permissions.

CSCsd04054—Router-quality of service (QoS) classes cannot be reordered

Description: You cannot reorder the classes in a QoS policy on a Cisco IOS router.

CSCsd09630—PIX deploy failed after changing IP address and DHCP address pool

Description: Deployment fails for DHCP relay commands and an error message states that the subnet of the DHCP server address pool range is not the same as the subnet of the DHCP server interface.

CSCsd13990—“dhcprelay” and “dhcpcd” commands are not generated in the correct order

Description: If you disable the DHCP server and then enable DHCP relay on the same interface, or if you disable DHCP relay and enable the DHCP server on the same interface, and you deploy both changes at the same time, deployment might fail.

CSCsd21256—A 72xx router cannot be used as remote client in EzVPN topology

Description: In an EzVPN topology configuration, deployment fails if a 72xx series router is used as a remote client device. The EzVPN client is supported on PIX Firewalls and Cisco 800-3800 Series routers only.

CSCsd21617—Need to modify the webfilter.xml template

Description: Even if you do not make changes to a configuration and the configuration is previewed or deployed, the filter commands are always cleared and redeployed.

CSCsd28385—Preview configuration error on Catalyst 6500/7600 devices

Description: Manually adding a Catalyst 6500/7600 device and then immediately running Preview Configuration without defining policies results in an error.

CSCsd28945—Problems duplicating certain object types

Description: You should not use the Create Duplicate option for the following object types: GTP maps, TCP maps, time ranges, AAA server groups, and PKI enrollments.

CSCsd28972—Routing commands not fully removed from router configurations

Description: Unassigning a routing policy from a Cisco IOS router does not remove all the CLI commands related to that policy from the device configuration.

Table 1 Resolved Problems (continued)

CSCsd30760—Optionally remove unreferenced ACLs based on admin settings

Description: Security Manager does not remove unused **access-list** commands from a device, for example, if an **access-list** command has a user-defined name (a name not automatically generated by Security Manager) and is not used by any command, for example, **access-group**.

CSCsd31803—Unassigning a preshared key policy removes Aggressive Mode option

Description: If you unassign a preshared key policy in a hub-and-spoke VPN topology, without first saving the policy, the Aggressive Mode option disappears from the UI page.

CSCsd31825—VPN NAT-0 rules not generated when NAT-0 rules are user-defined

Description: If a NAT exemption rule on a PIX 6.3, PIX 7.0 or ASA device already contains user-defined exemption rules, and you select the Do Not Translate VPN Traffic check box in the Translation Options page, Security Manager does not generate additional NAT exemption rules for the VPN traffic.

CSCsd32199—Need to reset FWSM to auto ACL mode before deploying a configuration

Description: Security Manager sets the FWSM device to manual mode when you deploy firewall rule delta information, then resets the device to auto mode when deployment is completed; however, the device remains in manual mode and deployment fails.

CSCsd33142—ACE with “interface” option causes “no access-group...” sent to device

Description: After you import or discover a PIX 6.3 device with an ACE using the “interface” keyword and the ACE is bound to the interface by the **access-group** command, if you deploy to the same device without making any changes, the ACE is removed from the ACL. This occurs if the ACL has other ACEs, or the ACL contains only the ACEs using the “interface” keyword. The **access-group** command for the ACL is removed from the device when the ACL contains only the ACEs using the “interface” keyword.

CSCsd35411—Wrong message in the audit log after successful discovery

Description: The audit report might contain a message saying that discovery failed even if discovery is successful. It is safe to ignore this message.

CSCsd37017—Minimized undocked map is not displayed when Map view icon is clicked

Description: If you minimize the undocked Map view, you cannot bring it to the front after clicking the Map View button on the toolbar or selecting the Show in Map View option.

CSCsd37024—Cannot work in undocked Map view because it is on top of modal dialog box

Description: The undocked Map view is displayed on top of an active dialog box and does not respond to user interaction.

CSCsd37558—Cannot unassign policy if content is being changed on a different device

Description: When you change a policy definition, other users are prevented from unassigning that policy from a different device.

CSCsd37616—Two users cannot assign same policy simultaneously on different devices

Description: If you assign a policy to a device, a different user cannot assign the same policy to a different device.

CSCsd37624—Cannot modify policy content if another user is performing unassignment

Description: If you unassign a policy from a device, a different user cannot edit the contents of that policy until you submit your changes.

CSCsd38886—Internal error on validation of VPN with Catalyst 6500

Description: If your VPN topology contains a Catalyst 6500 device and you have enabled the QoS Preclassify option in the IPsec Proposal, a message indicating that an internal error has occurred appears during validation.

Table 1 *Resolved Problems (continued)***CSCsd39543—Read-only operations require an open activity**

Description: If you have no activity opened, then click “Show Source Contents,” “Show Original Address Contents,” or “Show Translated Address Contents” from the shortcut menu in the Translation Rules table, you are asked to open an activity. These operations are read-only and do not require an opened activity.

CSCsd40127—Incorrect error message for time range objects

Description: If you enter an invalid time when you define a time range object, the error message that appears does not match the cause of the error.

CSCsd40376—GTP Map for PIX 7.0(4): No provision to configure permit response in GUI

Description: GTP Map in Security Manager does not support the permit response subcommand that was introduced in later versions of PIX OS software. The permit response subcommand from GTP Map CLI in PIX 7.0(4) and greater are dropped during the discovery process and not deployed when the GTP Map is deployed to the device.

CSCsd44545—Add New Version might not close dialog box in Workflow mode

Description: The New Configuration Version dialog box sometimes does not close when you select **Configuration > Add > Add New Version** from the Tools menu in Workflow mode. This happens if you do not have an open activity. The selection configuration version is added correctly, even though the dialog box does not close.

CSCsd45510—Configuring transparent FW on IOS devices supports only one bridge group

Description: When you configure transparent firewall on IOS devices, only one bridge group is supported. Bridge group 1 is dedicated to transparent firewall. If you use Bridge Group 1 for something else, and only one interface exists for that group, upon discovery, a validation error results.

CSCsd46022—AAA server loses its defined protocol and becomes uneditable

Description: A AAA server object that is part of a AAA server group loses its defined protocol and becomes uneditable after you change the protocol and fail to specify a key.

CSCsd46041—Validation fails if NAC is configured on an unsupported device type

Description: After you configure a NAC policy on a router, validation fails. This is because Security Manager allows you to configure a NAC policy on routers that do not support NAC.

CSCsd47010—Read-only users can create policies in Policy view

Description: Users with read-only (View) permissions can click the Add button in Policy view to create shared policies. In rare cases, this can lead to the deployment of blank policies that overwrite existing device configurations.

CSCsd49009—The “no dhcprelay command” order needs to be done correctly for ASA

Description: Deployment fails for DHCP relay commands and an error message states that the device cannot receive DHCP requests and forward them on the same interface.

CSCsd53532—After reinstallation, home page changes to CiscoWorks home page

Description: If you reinstall Common Services 3.0.3, Security Manager, and Auto Update Server (AUS) on an existing Security Manager server on which Security Manager and AUS are already installed, the home page defaults to the CiscoWorks home page instead of the Security Manager home page.

CSCsd55200—EzVPN Xauth username/password not configured on PIX 6.3 remote client

Description: The Ea3syVPN tunnel is not created because Xauth authentication fails on the PIX 6.3 remote client. Security Manager does not configure the Xauth username and password that is required for authentication.

CSCsd55435—Objects not displayed in Policy Object Manager after deleting overrides

Description: Deleting a policy object override causes the object on which the override is based to disappear from the Policy Object Manager.

Table 1 *Resolved Problems (continued)***CSCsd56449**—“Translating” message appears then deployment of PKI policy fails

Description: Deployment of a PKI policy fails if the URL specified for the CA server contains the CA server's hostname instead of its explicit IP address. Before the deployment failure, a “translating” notification appears to indicate that the device is trying to translate the host name.

CSCsd57440—Security Manager should correctly handle “boot system tftp” cmd for ASA

Description: If some boot images are already configured on an ASA device and you try to add another TFTP boot image, the deployment fails.

CSCsd58293—AAA servers discovered without a key do not use the global key

Description: If you discover a AAA server without a defined key on a Cisco IOS router, Security Manager does not properly discover and implement the global key in place of the missing server-specific key.

CSCsd58953—Deployment error displays incomplete information about failure

Description: Deployment fails and the error messages that appear do not supply adequate information about the error.

CSCsd59527—ASA: AAA accounting mode and server port not discovered correctly

Description: If you discover AAA servers configured on an ASA device, the group accounting mode is not defined in Security Manager with the default value and the server port is not defined according to the server protocol.

CSCsd59545—RADIUS AAA host key is changed by backoff exponential parameter

Description: Discovery of a router that uses the backoff exponential parameter as part of the definition of a RADIUS AAA host causes the correct key to this host to be overwritten upon deployment.

CSCsd60172—PIX/FWSM-Policies with nested network objects fail activity validation

Description: Activity validation fails on FWSM and PIX platform policies that contain network objects that refer to other network objects containing a single IP address.

CSCsd60698—PIX/ASA discovery creates AAA server groups with excessively long names

Description: Under certain circumstances, Security Manager might generate a name for a AAA server group that exceeds the maximum length supported by firewall devices. Any policy that uses this AAA server group fails validation.

CSCsd60868—Device credentials erased in rollback instances in Config Archive

Description: Device Credentials that were once displayed in the Device Properties menu can disappear after you roll back to an earlier configuration from Configuration Archive. This can occur when previous deployment was to file, or when previous deployment contained empty delta configurations.

CSCsd62598—Discovery fails after you change the Default Source Ports setting

Description: Discovery fails after you change the Default Source Ports setting on the Policy Object page of the Security Manager - Administration window to Use Secure Ports.

CSCsd62633—PIX/ASA rediscovery does not add AAA servers to AAA server groups

Description: Under certain circumstances, performing rediscovery on PIX/ASA devices does not add the AAA servers defined on the device to the related AAA server group.

CSCsd63562—Incorrect validation for xlate timeout on FWSM 2.3(3) device

Description: The minimum Translation Slot (xlate) timeout that you can set on the Timeouts Policy page is 30 seconds for FWSM 2.3(3) devices. However, Security Manager requires a minimum timeout of 1 minute.

CSCsd63938—FWSM interface table is empty and cannot be monitored

Description: The interface table in the Failover policy for FWSMs in single transparent mode and security contexts in transparent mode contains no information. As a result, you cannot set these interfaces to be monitored.

Table 1 *Resolved Problems (continued)***CSCsd66712—url-block commands cause deployment to fail**

Description: If you are specifying web filter settings for PIX/ASA devices for the first time, deployment might fail when you send **url-block** commands.

CSCsd67225—LDAP subcommand for aaa-server is dropped for Tunnel Group deployment

Description: A AAA Server host with LDAP protocol does not generate the subcommand “ldap-base-dn String” from Security Manager and the subcommand is removed from the device at deployment.

CSCsd67246—Job with multiple AUS-managed devices fails on first deployment

Description: After you deploy configurations to multiple AUS-managed devices in a single job, deployment to some of the devices fails and a “CALLHOME-PARSER-INVALID_ELEMENT” message is recorded in the transcript.

CSCsd68099—Job state is “Deployed” although device is still deploying

Description: If a deployment job contains both CNS managed and non-CNS managed devices, deployment status might not accurately reflect the actual deployment status of all the devices in the job. For example, deployment status might be “deployed” before all the non-CNS managed devices have finished deploying.

CSCsd69875—The no shut command is not generated for IOS transparent firewall BVI1

Description: If an IOS device does not have “bridge group 1 protocol ieee,” “bridge 1 route ip,” and “bridge irb” and you configure BVI1 IP address in both the interface UI page and Transparent Settings page, deployment fails.

CSCsd72206—Policy Query does not display the correct relationship for interfaces

Description: When source, destination, and service are in a policy query with no interface selected, and the source, destination, and service match rule values completely, the query and rule are deemed identical and the interfaces detail shows that “any” interface is identical to the rule interface value.

CSCsd73984—Policy Query not showing rule results in Policy view

Description: If you are in Policy view and you query a rule with a service that is contained in a service group used in the rule, the query results are blank.

CSCsd75967—SQL error during installation of Security Manager with ACS

Description: During installation of Security Manager, a dialog box shows that an interactive SQL error occurred. This problem occurs if a Sybase database engine is running while you are installing Security Manager.

CSCsd76242—Logging message does not generate CLI to enable/disable a syslog message

Description: Configuring the “Suppressed” setting for a syslog message on the Platform > Logging > Server Setup page has no effect when you deploy the configuration to the device.

CSCsd77059—Modify users in ACS mode cannot create/delete policies in Policy view

Description: Under certain circumstances, users who have Modify permissions in ACS mode cannot create or delete policies in Policy view.

CSCsd78965—Rule might have incorrect rule number if logging option is off

Description: An incorrect rule number results if you paste or add a rule at the same place more than once and logging is turned off.

CSCse09955—Cannot create network/host object that refers to object with single IP

Description: When defining a policy that requires a single IP address, an error occurs if you create a network/host object that refers to a second network/host object on which the required IP address is defined.

CSCse10636—NAC-Missing validation for subinterfaces triggers deployment failure

Description: The deployment of NAC interface commands (**eu max-retry** and **eu revalidate**) fails on subinterfaces.

Table 1 *Resolved Problems (continued)***CSCse23468—Rollback of context fails due to certificate mismatch**

Description: Rollback of a context fails because the device certificate was changed. On the next device operation, an error message states that the certificate is not trusted.

CSCse31816—AAA server cmd from IOS is not parsed correctly when reused by firewall

Description: If a AAA server discovered from an IOS device contains a leading “7” in its shared key and if the shared key is reused by a PIX/ASA/FWSM device, an error is issued on the key during activity validation.

CSCse33101—GUI notation “ASA” means user-input field applies to ASA and PIX 7.x

Description: The GUI adds notations next to user-input fields to indicate platform support. Currently, certain notations reference “ASA”; however, because the PIX 7.x platform uses the same software as ASA, the “ASA” notation applies to both ASA and PIX 7.x platforms (unless otherwise stated).

CSCse34675—Multimode: Rollback replaces the default config in the contexts

Description: When rollback of an admin context or another virtual context on ASA 7.0(5) multimode devices fails, it reverts to the factory default configuration instead of the device startup configuration.

CSCse43848—Deployment fails after upgrade if upgrade is installed on diff directory

Description: A data upgrade from Security Manager 3.0 to 3.0.1 fails if you install Security Manager 3.0.1 on a new server and in a different directory when compared to the directory in which it was originally installed. This might lead to a deployment failure because referenced configuration files are not available under configuration archive.

CSCse48038—Certificate is not retrieved during upgrade

Description: After you upgrade and restore to Security Manager 3.0.1 from 3.0, any device operation produces an error message notes that the certificate is not trusted. This is because the certificate is not retrieved during upgrade.

CSCse50096—Failover - ASA/FWSM should not pop up bootstrap window if no changes

Description: For both ASA and FWSM, the Bootstrap window is always displayed even if no changes are made to the LAN Failover policy.

CSCse57548—ASA 7.1 incorrectly deploys shutdown LAN FO intf command again

Description: Deployment fails for ASA 7.1 devices configured with LAN failover in multi mode.

CSCse58530—Web Filter: Incorrect validation for having UDP with URL buffer memory

Description: Deployment to a device might fail if a URL server with protocol UDP is defined along with the URL buffer memory.

CSCse58543—IOS: Deployment fails for UDP protocol with inspect HTTP

Description: If an inspection rule is configured with destination IP and protocol UDP, validation fails for UDP protocol with HTTP.

CSCse58554—Need validation for having aol as inspect protocol

Description: If an inspection rule is configured with “aol” as the inspect protocol on unsupported devices, a validation error results.

CSCse59578—Web Filter: Deployment fails for service port range in URL filter

Description: Deployment to a device might fail if two filter commands with the same source and destination addresses have overlapping service ports.

CSCse63692—Deployment fails on RA Catalyst 6500/7600 configured with FWSM and VRF-Aware IPSec

Description: In a remote access VPN, if you configure a Catalyst 6500/7600 device with a VRF-Aware IPSec policy and a FWSM blade, deployment fails due to the incorrect order of the CLI commands, which configure the FWSM blade before the VRF-Aware IPSec policy.

Table 1 **Resolved Problems (continued)****CSCse63971—Deployment fails after restore if upgrade is installed on diff directory**

Description: A restore operation of Security Manager 3.0.1 fails if you install Security Manager 3.0.1 on a new server and in a different directory when compared to the directory in which it was originally installed. This might lead to a deployment failure because referenced configuration files are not available under configuration archive.

CSCse70778—IOS: Transparent firewall deploy fails due to incorrect bridge group ID

Description: If **bridge-group** is configured on an IOS device and its ID is not 1, the deployment of the transparent policy fails.

CSCse78803—Invalid warning with parent policy

Description: An invalid validation warning might be issued about having an interface unbound to any access-lists.

CSCse78893—RADIUS and SDI deployment fails after upgrade to Security Manager 3.0.1

Description: After you upgrade Security Manager from 3.0 to 3.0.1, deployment might fail for AAA RADIUS or SDI servers.

CSCse79118—FWSM 3.1(x) Failover cannot be deployed due to out of sequence commands

Description: You will receive a deployment error if you make the following configuration changes for an FWSM 3.1(x) device and deploy those changes in the same deployment job:

- Define VLAN interfaces.
- Allocate the new VLAN interfaces to a security context.
- Create an active/active or active/standby failover policy.

CSCse79127—Deployment fails after changing FWSM failover mode

Description: If you change the failover mode for an FWSM running 3.1(x) from active/active to active/standby or from active/standby to active/active, you will receive the error “DOWNLOAD OPERATION FAILED : 24410 : Error parsing the show config response: Command Ignored, Configuration in progress...” when you deploy to the device.

CSCse79359—Cannot create multiple contexts for FWSM 3.1(2) or 3.1(3) in single job

Description: If you create multiple security contexts for an FWSM running 3.1(2) or 3.1(3) and deploy those security contexts in the same job, deployment fails with the error “DOWNLOAD OPERATION FAILED: 24410: Error parsing the show config response: Command Ignored, Configuration in progress...” for some security contexts and the error “DOWNLOAD OPERATION FAILED: 24015: IO error during SSL communication.” for other security contexts.

CSCse79360—VLAN created in Security Contexts policy deleted on second deployment

Description: If you modify the Security Contexts policy for a system context of an FWSM and reference a VLAN that does not exist in the Interfaces policy for the same system context, the VLAN is created on the FWSM when you next deploy to the system context. However, because the VLAN is not added to the Interfaces policy in Security Manager, the next time you deploy to the system context, the VLAN will be removed and any future deployments to virtual contexts that refer to that VLAN will fail because the VLAN is no longer defined in the system context.

Security Manager Known Problems

Catalyst 6500/7600 Configuration

Table 2 *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.

CSCsi31232—Catalyst 6500/7600 chassis discovery fails after upgrade from 3.0 to 3.1

Description: When you migrate a Security Manager 3.0 or 3.0.1 database to 3.1 in workflow mode, and try to discover the configuration of the upgraded Catalyst 6500 Series switch, Cisco 7600 Series router, or FWSM managed using the chassis before creating an activity, discovery fails.

Client Software

Table 3 *Client Software*

CSCsc91430—A blank error message is displayed when you update your client software

Description: During a service pack or point patch installation, a system prompt tells you to uninstall Security Manager Client. Unless you click the OK button, an error message that contains no text is displayed.

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.

Configuration Archive

Table 4 *Configuration Archive*

CSCsi11419—Rollback fails 50 percent of the time with Failover enabled

Description: After rolling back Failover configuration to the device, the secondary unit does not come up automatically and does not participate automatically in the Failover setup.

Deployment

Table 5 *Deployment*

<p>CSCsa84494—Discovery & view current config can't occur concurrently with deployment</p> <p>Description: Performing discovery or viewing the current configuration of a device while deployment is in progress might lead to unpredictable results.</p>
<p>CSCsc22934—ACL limitations on Layer 2 interfaces on IOS ISR devices</p> <p>Deployment fails if access rules containing certain options are associated with Layer 2 interfaces of ISR routers.</p>
<p>CSCsd38578—Deploying to a device with no policies erases the config on the device</p> <p>Description: The configuration on the device is erased if you deploy to the device before any policies have been defined in Security Manager.</p>
<p>CSCsd67440—Deployment fails after you restart the Daemon Manager</p> <p>Description: Deployment fails after you restart the Daemon Manager because the backend server process does not start.</p>
<p>CSCse10629—Deployment successful but not all delta commands deployed to device</p> <p>Description: Deployment appears to be successful; however, not all of the commands in the delta configuration are deployed to the device.</p>
<p>CSCse23064—Enrollment URL CLI causes failure in deployment to AUS managed device</p> <p>Description: Deployment to AUS-managed device fails if the deployment configuration contains the CLI command “enrollment url http:...”</p>
<p>CSCsi09797—Job state for completed jobs is “Deploying” for CNS-managed IOS routers</p> <p>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”.</p>
<p>CSCsi18673—Security Manager deployment may trigger ObjectGroup name warnings</p> <p>Description: Security Manager deployment details may show ObjectGroup name warnings. For example, ObjectGroup Netbios.udp is created from Policy Object Netbios. On networks with a large number of deployments this may cause an exceedingly large number of warnings, making it hard to monitor the deployments.</p>
<p>CSCsi18678—Security Manager deployment may trigger interface name warnings</p> <p>Description: Security Manager deployment details may show name warnings of the sort: “Interface defined on device does not have a name.” That is, some of the interfaces defined on a device do not have a defined name. Rules bound solely to these interfaces will not be deployed. On networks with a large number of deployments this may cause an exceedingly large number of warnings, making it hard to monitor the deployments.</p>
<p>CSCsi29146—Deployment using AUS fails after upgrade from 3.0 to 3.1</p> <p>Description: Security Manager deployment details may show 'Interface defined on device does not have a name' warnings if the interface name is empty. For example, some of the interfaces defined on a device do not have a name defined. Rules bound just to these interfaces will not be deployed.</p>
<p>CSCsi31224—Preview failed after deploying config to AUS server</p> <p>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.</p>

Device Management

Table 6 *Device Management*

CSCsc51908—Cannot add a system context from DCR into Security Manager

Description: If you try to import a system context that belongs to a multi-mode PIX Firewall 7.0 or an ASA device from DCR to Security Manager, the import fails and an error message results.

CSCsc78319—Security Manager does not support changing the device type in DCR

Description: The device icon in the Device selector does not match the device type and the Policies selector displays only the Flex Config policy when you click the Device View button in the tool bar.

CSCsd49045—Unclear error message when IOS SSL deployment exceeds maximum size

Description: Deployment to Cisco IOS router fails when SSL is the transport protocol and you see a confusing error message.

CSCsd71001—Not able to import AUS device from DCR

Description: You cannot import an AUS-managed device from DCR to Security Manager.

CSCse70089—RBAC-Authorization and duplicate display name errors when adding devices

Description: Authorization and duplicate display name errors occur when you add devices to a Security Manager server that uses Cisco Secure ACS for AAA.

Diagnostics, Monitoring, and Troubleshooting Tools

Table 7 *Diagnostics, Monitoring, and Troubleshooting Tools*

CSCsg13603—Device connectivity test takes a long time for unreachable devices

Description: When you test device connectivity while adding devices using the Add Device from Network or the Add New Device wizard, the device connectivity test takes a long time to complete if the device cannot be reached.

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.

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.

CSCsi27178—Several pages are blank in SDM 2.4 after discarding changes

Description: After you perform configuration changes for Cisco IOS devices using SDM 2.4 started from the Security Manager client and click Discard Changes to reset to the previously applied configurations, many of the pages are blank or empty.

CSCsi76604—Data archival does not work in IEV started from Security Manager

Description: Database archival feature that enables you to archive real-time events does not work in IEV started from Security Manager. However, this problem does not occur on a system in which IEV is installed separately from Cisco.com and started outside of Security Manager.

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.

Discovery

Table 8 *Discovery*

CSCse27578—Discovery/deployment of multiple FWSM VCs hangs
Description: Discovery or deployment hangs for multimode FWSM with several virtual contexts.
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.
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.
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.
CSCsi45204—QoS policy not discovered when WRED is enabled
Description: When Weighted Random Early Detection (WRED) is configured, discovery of an IOS device with a QoS policy fails to discover the QoS policy.

Firewall Services

Table 9 *Firewall Services*

CSCsa81103—Unable to create an access rule with TCP flags
Description: Security Manager does not support TCP flag specifications, such as urg, fin, psh, and ack, in access rules. As a result, during discovery, Security Manager drops the specifications.
CSCsa81104—Unable to create an access rule to match QoS parameters
Description: Security Manager does not support ACE options such as DSCP, ToS, or precedence. As a result, during discovery, Security Manager drops the options.
CSCsa98978—Hit Count does not expand FWSM devices with object-group enabled
Description: Although the GUI allows you to enable the Object Group Search option for FWSM devices, the FWSM does not expand object groups when listing access rules after a “show access-list” command and Hit Count results are inaccurately displayed.
CSCsb85487—Need warning when ACL deployment to IOS devices can cut off access
Description: Security Manager does not check if the firewall rules that you configured in Security Manager permit management traffic (SSH and HTTPS) to the IOS device being managed. As a result, after firewall rules are deployed to the device, connection to the device might be lost.
CSCsc81905—QIT: Empty ACL is deployed on 87x series routers for BGP port
Description: IOS 87x ISR routers do not support BGP as a routing protocol or as a service in ACLs when the device has only 24 MB of memory; however, BGP is supported when the device has more than 24 MB memory. Security Manager does not detect the amount of memory available on the device and cannot enforce any restrictions. As a result, job deployment containing an ACL with ACEs having BGP will fail.

Table 9 Firewall Services (continued)

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.

CSCsc87646—Deployment to IOS device fails if AuthProxy is assigned to L2 interface

Description: If you create AAA or inspection rules for “all” interfaces on an IOS device, deployment fails if the device is using Layer 2 port.

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.

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.

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.

CSCsh64420—Deployment fails modifying ACE in AAA ACL on FWSM3.1.1

Description: For FWSM3.1(1) context, if you modify the AAA rules table, then deploy the change to the device, you might get the following deployment error:

```
ERROR: Unable to find AAA ACE
Error acl_updated: aaa_acl_changed failed
ERROR: Unable to delete ACE from dependent modules
```

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.

CSCsh96644—FWSM ACL remarks may cause inline editing manual commit failure

Description: Deploying to FWSM 3.1(4) fails with an error saying “Specified remark does not exist” in the deployment transcript. This happens only when the “Let FWSM decide when to compile access-list” admin setting is unchecked and the access policies contain a number of comments.

Table 9 Firewall Services (continued)

CSCsi11697—Deploy fails after rollback operation followed by URL filter change

Description: When you use Security Manager to roll back an ASA 7.2(2) device to a configuration that contains default inspection class-map and policy-map “global_policy”. If you change Web Filter rules, then deploy the change, the deploy operation might fail.

CSCsi16937—FWSM: Need validation for non-standard netmask in address pool

Description: Deployment might fail if an IP address is configured with a non-standard mask for an address pool. Although the UI allows it, the only device version that allows non-standard masks is PIX/ASA 7.2+.

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.

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.

CSCsi23773—Always generates range CLI for TCP map

Description: If TCP Map is assigned in the “IPS, Qos and Connection Rules” then redundant tcp-options commands might be generated even if no changes are made to the TCP Map or related policy.

CSCsi27421—Deploy removes ACEs when creating ObjectGroup disabled for FWSM 3.1(3-4)

Description: If an access-list entry (ACE) with an object group is internally expanded into a number of ACEs and if one of the expanded ACEs is inserted into the access-list, FWSM 3.1(3)12 and later rejects this ACE with an error “found duplicate element”.

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.

CSCsi49748—Transparent rules not removed from device when deleted in Security Mgr

Description: If you delete the transparent firewall rules from Security Manager and deploy to the device, the rules are not removed from the device; however, Security Manager continues to show those rules as deleted.

CSCsi49794—AclNamePreserv: Deploy fails due to diff source addr in delta for static

Description: When you change an access list that is shared between a static command and another command, deployment to the device might fail.

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.

CSCsi51974—Hit Count: Disabled for inherited rules

Description: The Hit Count option, which is accessed from the Tools menu that is located below the Access Rules table, is disabled when you select access rules that belong to an inherited policy.

Table 9 *Firewall Services (continued)***CSCsi54973—Network objects with non-std netmask show “no value” with show cell cmd**

Description: Show cell contents for Sources/Destinations might show empty contents or “no value” if the cell contains a network with a non-standard mask.

CSCsi56443—Unable to create network obj from cell if cell contains IP address range

Description: The Create Network from Cell contents or Create Network from Selected Contents does not work if the cell contains an IP address range.

CSCsi91028—Need to upgrade network hashcode

Description: During import, a network policy object might not get reused, even if the contents in Security Manager are the same as the contents of the network being imported.

Installation and Upgrade

Table 10 *Installation and Upgrade***CSCsb65932—The Windows language version must be either English or Japanese**

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

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.

CSCsi06508—CSM reverts to CW Local authentication after upgrading from 3.0 to 3.1

Description: The authentication mode for Security Manager reverts from ACS authentication to CiscoWorks Local authentication after the server is upgraded from Security Manager 3.0 to Security Manager 3.1.

CSCsi24016—ACS permissions are not updated after upgrading from CSM 3.0.1 to 3.1

Description: Updated permissions are not added to the default user roles for Security Manager in ACS after upgrading from Security Manager 3.0.1 to Security Manager 3.1.

CSCsi31291—Installation incorrectly refers to RME 4.0.4 instead of RME 4.0.5

Description: The Select Components screen of the installation utility refers to RME 4.0.4 instead of RME 4.0.5.

CSCsi04116—AUS option cannot be deselected during inline upgrade from 3.0.1 to 3.1

Description: When you perform an inline upgrade from Security Manager 3.0.1 to Security Manager 3.1, the Auto Update Server 3.1 option in the component selection screen of the installation wizard is grayed out and selected by default. As a result, AUS 3.1 is always installed on your server system, leaving you with no choice to deselect it during inline upgrade.

Miscellaneous Issues

Table 11 *Miscellaneous Issues*

CSCsc96007—Database errors in multiuser environments

Description: Under extreme circumstances, errors might occur when many users try to simultaneously perform operations that write to the Security Manager database.

CSCse59404—Certificates are out of sync with IOS versions prior to 12.3T

Description: Certificate mismatch or not trusted errors result during deployment and discovery for IOS devices.

PIX/ASA/FWSM Configuration

Table 12 *PIX/ASA/FWSM Configuration*

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

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

CSCsc97346—Deploy and discover create new TCP Map object with number appended

Description: If you deploy a configuration to a device that uses a TCP Map object, then rediscover that configuration, a new object with a number appended to the object name might be added to the TCP Map objects list.

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.

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.

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.

CSCsd41095—AUS deployment fails if static settings in Security Manager duplicated

Description: If a device has duplicate MAC addresses in the static arp table and the static mac-address-table, or if Security Manager policies have duplicate MAC addresses in the arp table and the mac-address table, the AUS deployment might fail.

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.

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.

CSCse36406—Failover suspend-config-sync option is removed

Description: The suspend-config-sync option was removed from Security Manager because of a problem in configuration rollback.

Table 12 PIX/ASA/FWSM Configuration (continued)

CSCse41791—FWSM rollback fails when combined in one job with Catalyst rollback

Description: If you use one job to roll back the configurations of both an FWSM and a Catalyst device, the FWSM rollback fails. You must roll back the Catalyst device first, then use a second job to roll back the FWSM.

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.

CSCse48708—FWSM 2.x VCs interface table is empty after discovery

Description: After discovering FWSM 2.x security context devices, some of the vlan interfaces are missing from the devices' interface table.

CSCse50869—FWSM 3.1 discovery via config file creates context in router mode

Description: After you add and discover a FWSM 3.1(x) multi-mode, mixed OS mode device from a configuration file, all security context devices are created in Security Manager as “router” OS mode, even though some of them might really be “transparent” OS mode.

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.

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.

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.

CSCsi05756—PPPoE & FAILOVER - No validation that both features cannot co-exist

Description: Security Manager allows a user to configure failover along with PPPoE even though that configuration is not supported.

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.

CSCsi23903—FWSM 3.2 rollback does not work if it contains mac-add static command

Description: After you roll back the configuration of an FWSM 3.2 that contains the **mac-address-table static inside interface_name mac_address** command, the configuration on the device remains the same as what existed before rollback.

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.

CSCsi42889—Swapping interface names causes deployment failure

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

Table 12 *PIX/ASA/FWSM Configuration (continued)***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.

Policy Objects

Table 13 *Policy Objects***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.

Router Configuration

Table 14 *Router Configuration***CSCsc77534—NAT interface deployment fails on 83x Series routers**

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

CSCsc91151—Virtual interfaces not being removed from router configurations

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

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

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

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.

CSCsh18926—NetFlow deployment fails on subinterfaces

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

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.

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

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

Table 14 Router Configuration (continued)

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.

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.

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.

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.

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

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

CSCsb66843—Unable to delete the IPSec Profile

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

To work around this problem, reload the device, then manually remove the IPSec profile. If the configuration is saved to the startup-config, make a backup text file of the startup-config, remove the IPSec profile, reload the device, then copy the updated file to the device and save the changes to the startup-config.

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.

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.

Table 15 **Site-to-Site/Remote Access/SSL VPN Configuration (continued)****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 supports 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.

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.

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.

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.

Table 15 *Site-to-Site/Remote Access/SSL VPN Configuration (continued)***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.

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.

CSCsi20081—Activity validation error in Easy VPN topologies using the same server

Description: When you configure two Easy VPN hub-and-spoke topologies using the same hub device for the Easy VPN server, and define different VPN interfaces and protected networks for the hub, an activity validation error states that the same interface has been defined for the IPsec proposals on the Easy VPN server hub.

Tools

Table 16 *Tools***CSCse69546—Backup/restore fails when Cygnus Solutions software is installed**

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

User Interface

Table 17 *User Interface***CSCsb43414—File selector does not show the network drive**

Description: When you use Security Manager's file selector to select a file on the Security Manager server, network drives that are mapped on the server are not listed.

CSCsb84290—File selector is not refreshed when new files are added

Description: If you add files to the server when the "Choose File" dialog is open, the file selector does not refresh to display the new files.

CSCsb93985—Client may not display correctly after display properties are changed

Description: After changing the Windows display properties, the Security Manager client is not displayed correctly. For example, Device View and New/Delete Device buttons are not visible and the content area does not refresh correctly.

Table 17 *User Interface (continued)***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.

CSCsh63248—Add field in Device Manager to specify whether device is Admin Context or not

Description: When an Admin context (on a multi-context PIX/ASA, or FWSM device) is discovered as a standalone device in CSM, some activity validation warnings may be generated for SNMP-server entity and resource traps configured on the context device. Also, when a user context on a multi-context PIX/ASA, or FWSM device is discovered as a standalone device in CSM, deployments containing SNMP-server listen-port, SNMP-server entity and resource traps may fail.

Auto Update Server (AUS) 3.1

AUS Resolved Problems

Table 18 *Resolved Problems***CSCsd22934—Error occurs when a blank enable password is used**

Description: When you deploy configurations from Cisco Security Manager to AUS, deployment fails and the “INVALID_ENABLEPASSWORD_LENGTH” error is recorded in the transcript. This problem occurs when an AUS-managed device is added to the Cisco Security Manager inventory with a blank Enable password.

CSCsd67246—Deployment to several AUS-managed devices fails

Description: If you deploy configurations to several AUS-managed devices in a single job, deployment to some of the devices fails and a “CALLHOME-PARSER-INVALID_ELEMENT” message is recorded in the transcript.

CSCse86596—Cannot launch AUS after restoring a backup created from another server

Description: The error “HTTP Status 500 - Internal Server Error” is displayed when you try to launch AUS from a Security Manager server using a backup that was previously created from another Security Manager server.

CSCse88978—Cannot launch AUS after upgrading from Security Manager 3.0 to 3.0.1

Description: The error “HTTP Status 500 - Internal Server Error” is displayed when you try to launch AUS after you upgrade to Security Manager 3.0.1.

CSCse90140—Error received when ASA 7.1.1 or 7.1.2 tries to contact AUS server

Description: CALLHOME-PARSER-ERROR is received when the AUS-managed ASA device tries to contact the AUS server. This occurs when the ASA device is running an older version of ASDM.

AUS Known Problems

Table 19 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.

IPS and IOS IPS in Security Manager 3.1

IPS and IOS IPS in Security Manager Notes

- 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.
- If you back up your database, you must restore it on the same server.
- If you need to upgrade from IPS MC 2.1 to IPS MC 2.2, make sure that you check your sensor certificate before upgrading to IPS MC 2.2 to avoid a certificate validity problem.

Follow this procedure to diagnose this problem:

- a. Using Internet Explorer in a new web browser window, enter `https://10.1.2.3` in the Address box. (10.1.2.3 is the IP address of the sensor whose certificate you want to view.)
- b. If the sensor is using a nonstandard HTTPS port such as 1443, add it in the format `https://10.1.2.3:1443`.
- c. In the initial certificate warning dialog, click the button for viewing/examining the certificate. The validity period appears on the General tab. If this problem is affecting the user, the current time on the IPS MC will be outside the validity period.

Follow this procedure to work around this problem:

- a. Log into the sensor's CLI with SSH, using an account with administrative privileges.

- b. Enter the following CLI command (at EXEC mode): **tls generate-key**.
- c. Make a note of the fingerprint values, then return to the IPS MC and reimport the sensor.

**Caution**

Cisco Security Manager 3.1 does not support IOS version 12.4(11)T and later routers that use the Cisco CNS Configuration Engine to manage and deploy configurations.

**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.

IPS and IOS IPS in Security Manager Resolved Problems

Table 20 *IPS and IOS IPS in Security Manager Resolved Problems*

CSCsd46456—HTTP Credentials Changes not Propagating to IPS Manager

Description: When changes are made to HTTP credentials in Cisco Security Manager, they are not propagated to IPS Manager.

IPS and IOS IPS in Security Manager Known Problems

Table 21 *IPS and IOS IPS in Security Manager Known Problems*

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.

CSCsi31784—Greenfield IOS IPS device added at one sig level lower than the highest

Description: When using the Add Device > Add New Device option, sometimes the signature release level associated with the device is not the same as the highest level available in Security Manager.

Table 21 *IPS and IOS IPS in Security Manager Known Problems (continued)***CSCsi45326—IOS IPS - preview config does not work when device at S0V0**

Description: When Security Manager discovers an IOS IPS device that has no signature updates applied to it, and users make changes to the signature policy, then preview config does not show any of the IPS policies. Only CLI policies get displayed in the preview config.

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.

CSCsi56022—IOS IPS: all sigs in apply IPS wizard marked modified in sig update -1

Description: The signature delta preview table at the 3rd step of Apply IPS Update wizard, which can be launched from Tools > Apply IPS Update menu, does not show accurate information about modified and new signatures.

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.

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.

Table 21 *IPS and IOS IPS in Security Manager Known Problems (continued)***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.

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.

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.

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.

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

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

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

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

CSCsi44605—IPS variable names cannot contain special characters

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

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

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

Documentation Updates

Topics in this section describe updates and changes to the user documentation for Security Manager 3.1.

IPS Event Viewer

This section contains updates and changes to the *Online Help for Cisco Security Manager 3.1*.

Replace the note on modifying Cisco Security Agent policies to enable communication between IEV client and IEV server with the following information.

- To enable communication between IEV server and IEV client, you need to modify the Cisco Security Agent or any other anti-virus and network firewall software policies on the Security Manager server to configure TCP ports 60002 and 60003 as open ports. If the server has a preexisting installation of the full Cisco Security Agent, the standalone agent is not installed on the system when you install Security Manager. In such a case, configure the Cisco Security Agent network services to accept connections on TCP ports 60002 and 60003. However, if the server on which you install Security Manager was not previously installed with the full, commercial version of Cisco Security Agent, the Security Manager installer installs a customized, standalone agent on your server and opens the necessary TCP ports for communication between IEV server and IEV client.
- When you start IEV client from the Security Manager client system, IEV client automatically opens TCP port 5001 to establish communication with the IEV server.

The following is additional information regarding the guidelines when working with IEV started from Security Manager:

You cannot start IEV client from a Security Manager client if the Security Manager server has also been installed on the same system.

New Features in Security Manager 3.1

This documentation update applies to the *User Guide and Online Help for Cisco Security Manager 3.1*.

The following information is incorrect in the “What’s New in Cisco Security Manager 3.1” section of *Chapter 1, Getting to Know Security Manager*, and needs to be removed from the list of new features in 3.1.

Linkage between Security Manager and CS-MARS for logs.

Where To Go Next

If you want to:	Do this:
Install Security Manager server or client software	See Installation Guide for Cisco Security Manager 3.1 .
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 the “Checklist for Getting Started with Security Manager” topic in the online help, or see Chapter 1 of <i>User Guide for Cisco Security Manager 3.1</i> .
Define essential settings	See the “Define These Settings First” topic in the online help, or see Chapter 2 of <i>User Guide for Cisco Security Manager 3.1</i> .

If you want to:	Do this:
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 3.1</i> . <ul style="list-style-type: none"> Setting Up User Permissions Integrating Security Manager with Cisco Secure ACS
Bootstrap your devices	See the “Preparing the Devices for Security Manager to Manage” topic in the online help, or see Chapter 5 of <i>User Guide for Cisco Security Manager 3.1</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 3.1</i> .

Related Documentation

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

Table 22 Product Documentation

Document Title	Available Formats
<i>Installation Guide for Cisco Security Manager 3.1</i> ¹	<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/3.1/installation/guide/overv.html
<i>User Guide for Cisco Security Manager 3.1</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/3.1/user/guide/ug31.html
<i>Supported Devices and Software Versions 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/compatibility/information/sdt31.html
<i>FAQs and Troubleshooting Guide for Cisco Security Manager 3.x</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/troubleshooting/guide/trblsht.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

Table 22 Product Documentation (continued)

Document Title	Available Formats
<i>User Guide for Auto Update Server 3.1</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/auto_update_server/3.1/user/guide/ausug31.html
<i>Supported Devices and Software Versions for Auto Update Server 3.0</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/compatibility/information/smdev.html
<i>Installation and Release Notes for Cisco Performance Monitor 3.1</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/performance_monitor/3.1/installation/guide/pm31irn.html
Context-sensitive online help	Click the Help button in a window or dialog box.

1. Includes "Importing IPS MC 2.2 Data" using IpsMcDbUpgrade.pl.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.



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

© 2007–2008 Cisco Systems, Inc. All rights reserved.

