



Release Notes for *Cisco Security Manager 3.0*

Revised: March 27, 2006, OL-9952-01

CDC Date: March 27, 2006

These release notes contain the following sections:

- [Introduction, page 1](#)
- [Cisco Security Manager, page 2](#)
- [Auto Update Server, page 13](#)
- [IPS Manager, page 14](#)
- [Where To Go Next, page 25](#)
- [Related Documentation, page 26](#)
- [Obtaining Documentation and Submitting a Service Request, page 27](#)

Introduction

This document contains release note information for the following:

- **Cisco Security Manager 3.0**

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.



Corporate Headquarters:

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

© <2006> Cisco Systems, Inc. All rights reserved.

- **Auto Update Server 3.0**

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.

Cisco Security Manager (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 Manager for IPS Sensors 3.0**

Cisco Security Manager supports IPS provisioning with the IPS Manager for IPS Sensors. The predecessor of IPS Manager was Management Center for IPS Sensors (IPS MC).

Cisco Security Manager

Notes

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.

Known Problems

This release note document includes ID numbers and headlines for each known problem identified in the document. Also included is a description of each. If you accessed this document from Cisco.com, you can click on 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.

Catalyst 6500/7600 Configuration

Table 1 *Catalyst 6500/7600 Configuration*

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.

CSCsd72445—System context rollback to full configuration fails

Rolling back the system context configuration to full configuration in the archive pulled from CVDM fails because the order of the commands in the configuration is not correct. The configuration omits a version at the beginning.

Client Software

Table 2 *Client Software*

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.

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 3 *Configuration Archive*

CSCsd44499—Approver only user cannot make changes in Config Archive

Description: The Add button in the Configuration Archive is unavailable if you have approver privileges. If your CiscoWorks role is Approver, you cannot use the Add or Fetch features.

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.

CSCsd60868—Device Credentials are erased in certain 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.

Deployment

Table 4 *Deployment*

CSCsa84494—Discovery & view current config cannot occur concurrently with deployment

Description: Performing discovery or viewing the current configuration of a device while deployment is in progress might lead to unpredictable results.

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

Deployment fails if access rules containing certain options are associated with Layer 2 interfaces of ISR routers.

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.

Table 4 *Deployment (continued)***CSCsd38578—Deploying to a device with no policies erases the config on the device**

Description: The configuration on the device is erased if you deploy to the device before any policies have been defined in Security Manager.

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.

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.

CSCsd67440—Deployment fails after you restart the Daemon Manager

Description: Deployment fails after you restart the Daemon Manager because the backend server process does not start.

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.

Device Management

Table 5 *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.

Discovery

Table 6 *Discovery***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.

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.

Table 6 *Discovery (continued)***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.

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.

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.

Firewall Services

Table 7 *Firewall Services***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.

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.

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.

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

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 7 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 on 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 an 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.

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.

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.

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.

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.

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.

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.

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

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.

Table 7 *Firewall Services (continued)***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.

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.

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.

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.

CSCsd70915—GTP Map: Deployment fails due to PDP and signaling timeout problems issues

Description: When you initially 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.

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.

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.

Installation

Table 8 *Installation***CSCsb64813—Installation fails on a server where the PERL5LIB variable is set**

Description: PERL is installed and a system environment variable is set for PERL5LIB on the server. An error message during installation tells you that perl58.dll cannot be found. Installation fails.

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

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

Table 8 *Installation (continued)***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 that already has Security Manager and AUS installed, the default home page is set to the CiscoWorks home page instead of the Security Manager home page.

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.

Maps

Table 9 *Maps***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.

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.

Miscellaneous Issues

Table 10 *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.

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.

Table 10 *Miscellaneous Issues (continued)***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.

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.

NAT Configuration

Table 11 *NAT Configuration***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.

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.

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.

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.

CSCsc97346—Deploy and discover creates 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.

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.

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.

CSCsd13990—"dhcrelay" and "dhcpd" 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.

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

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.

CSCsd49009—Location of “no dhcprelay command” in generated CLI is wrong

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.

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.

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) 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.

CSCsd63562—Incorrect validation for xlate timeout on FSWM 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.

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.

Policy Objects

Table 13 *Policy Objects*

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.

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**.

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.

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.

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.

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.

Router Configuration

Table 14 *Router Configuration*

CSCsc77534—NAT interface deployment fails on 83x Series routers

Description: The deployment of NAT interface commands (<CmdBold>ip nat inside<NoCmdBold> and <CmdBold>ip nat outside<NoCmdBold>) fails on Cisco 83x Series routers.

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.

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.

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.

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.

Site-to-Site VPN and Remote Access VPN Configuration

Table 15 *Site-to-Site VPN and Remote Access 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 will fail and you will 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.

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.

CSCsc77179—Deployment of VPN to PIX 7.0 device fails

Description: If you delete a VPN that uses the Answer-only Connection Type option for VPN interface SA negotiation and you create a new one that uses the Originate-only option, deployment to a PIX 7.0.1-7.0.5 device will fail. This is due to a known bug on the device (CSCsc27972).

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.

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.

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.

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.

User Interface

Table 16 *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.

Table 16 *User Interface (continued)***CSCsb93985—Client may not display correctly after display properties are changed**

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

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.

Auto Update Server

Known Problems

Table 17 *AUS***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.

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.

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.

CSCsd58137—IOS devices fail to connect to the CNS Event gateway running on AUS

Description: Cisco IOS devices fail to connect to the CNS Event gateway running on AUS when the default CNS bootstrap password configured in AUS was not changed on the machine where you installed AUS.

CSCsd46253—Blank screen appears when you launch AUS after restoring backup

Description: A blank screen appears if you launch AUS after you restore backed-up data from one server to another server.

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.

IPS 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.
- The IPS Version 5.0(6) Service Pack is expected to be released in March 2006. Upon its release, the minimum required version for 5.X Signature Updates will change from IPS version 5.0(1) to IPS version 5.0(5). Approximately 30 days after the release of 5.0(6), the minimum requirement will again be incremented to IPS version 5.0(6). Attempts to install signature updates on sensors running IPS 5.X software versions earlier than the minimum required versions will fail until the sensor is upgraded to the supported level. If you are currently running IPS Version 5.X software versions earlier than 5.0(5), we recommend that you upgrade to 5.0(6) upon its release. Customers currently running 5.0(5) should upgrade to version 5.0(6) within 30 days of its release to ensure continued signature support. (Customers running 5.0(5) engineering/patch versions MUST upgrade to 5.0(6) before installing signature updates that are released after 5.0(6).)
- 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, you must check your sensor certificate before upgrading to IPS MC 2.2 to avoid a certificate validity problem.
 - Follow this procedure to diagnose this problem: Using Internet Explorer in a new web browser window, enter `https://10.1.2.3` into the Address box. (10.1.2.3 is the IP address of the sensor whose certificate you want to view.) If the sensor is using a non-standard HTTPS port such as 1443, add it in the format `https://10.1.2.3:1443`. In the initial certificate warning dialog, click the button for viewing/examining the certificate. The validity period appears on the “General” tab. If this issue 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: Log into the sensor's CLI with SSH, using an account with administrative privileges. Enter the following CLI command (at EXEC mode): `tls generate-key`. Make a note of the fingerprint values, then return to the IPS MC and re-import the sensor.
- If you plan to migrate data from IPS MC 2.2 to IPS Manager, refer to “Importing IPS MC 2.2 Data” in the *Installation Guide for Cisco Security Manager 3.0*.

Known Problems

Configuration Comparison Tool

Table 18 Configuration Comparison Tool

<p>CSCsa76625—Signature wizard with engine parameters not working</p> <p>Description: In IPS MC 2.1, Custom Signature Wizard (CSW) for IPS 5.x does not allow you to configure the engine parameters (tune parameters); instead, it asks you to go to the Signature Summary page to tune the newly created custom signature.</p>
<p>CSCsa88926—When SSL certificate expires there is no warning or error</p> <p>Description: You cannot update IDS sensor signatures from IPS MC. The update appears to proceed but nothing actually occurs (when logged into the sensor, the IPS MC does not show up when 'sh users' is run, and there is no broadcast indicating services are stopping for the update process).</p>
<p>CSCsb09029—Custom signatures not listed in configurations on different sensors</p> <p>Description: In the Configuration Compare tool, Custom Signatures are not displayed when the source is sensor and the destination is another Group/Sensor.</p>
<p>CSCsb17024—Current vs Running Config does not list master blocking sensors</p> <p>Description: Under certain conditions when using the Configuration Comparison tool, the master blocking sensor configuration doesn't appear on the Configuration Comparison page.</p>
<p>CSCsb21227—IPS MC/SecMon backup fails if third party backup software is installed</p> <p>Description: IPS MC VMS backup stays at 10% and is not completed when a third-party backup system is being used.</p>
<p>CSCsb21907—CronSchedule assumes default locale is US</p> <p>Description: IPS MC throws java.text.ParseException when you have set a non-US locale in IPS MC Server.</p>
<p>CSCsb41544—NAT to IPS MC changes must be deployed before sigupdate</p> <p>Description: Changing the NAT value on the identification page and then doing a signature update does not work.</p>
<p>CSCsb84964—Current Vs Running Config does not list event action filters</p> <p>Description: The Configuration Comparison Tool does not list SigEvent Action Filters under the current configuration.</p>
<p>CSCsb90717—Out-of-band signature update requires re-import to be seen in IPS MC</p> <p>Description: Get Version fails to save after updating 5.0 Sensors if signature updates are out-of-band.</p>
<p>CSCsc00446—Error message does not indicate change in certificate fingerprint</p> <p>Description: A change in certificate on the device causes Query Interface to fail for an IPS 5.x device with the following incorrect message: “Object loading failed. An error occurred trying to get the interface information. An error occurred while trying to determine the sensor version. Detail = untrusted server cert chain”.</p>
<p>CSCsc13966—IOS IPS SDF Type is not listed in Configuration > Copy</p> <p>Description: Config Copy tool does not list IOS IPS SDF Type in available items when you select all devices under a group as targets.</p>
<p>CSCsc22445—Error message does not report change in TLS enable</p> <p>Description: Reimport of a sensor generates the following popup message box (in part): Re-import of sensor sensor9 failed. The error message should indicate that TLS enable changed.</p>

Table 18 Configuration Comparison Tool (continued)**CSCsc42221—No “filters” option in the Copy Wizard**

Description: When you are using IPS MC 2.1 or 2.2 and VMS 2.3 to copy filters from sensors running 4.x to other sensors running 4.x, there is no “filters” option in the Copy Wizard.

CSCsc53020—New Signature ID assigned to custom signature when copied with wizard

Description: When you copy custom signatures from a device/group to another device/group, the Signature Copy wizard assigns a new signature ID for the destination signature in IPS MC. This behavior is seen on all supported device types: IDS 4, IPS 5, and IOS IPS.

CSCsc59131—Deploy log does not get created

Description: IDS logs are not created in the product log directory.

CSCsc70057—Event action filters with event variables are not being copied properly

Description: EAFs configured with event variables are not properly copied using the Configuration Copy Wizard for IPS 5.x devices.

CSCsc70067—Event action filters not being copied from 5.x devices to Global group

Description: Config Copy Tool does not copy the configuration to the group “Global.”

CSCsc72868—Last Generated Config does not list master blocking sensors

Description: Master Blocking Sensors are not listed in Config-Diff for Last Generate/Last Deployed Configuration.

Custom Signature Wizard

Table 19 Custom Signature Wizard**CSCsb00157—IPS MC displays event actions not supported for TROJAN-BO2K engine**

Description: The Custom Signature Wizard will show event action options that are not supported by some engines (such as TROJAN-BO2K, TROJAN-TF2K, TROJAN-UDP)

Database

Table 20 Database**CSCsc30724—Exception in IDS_Import.log specifies database error**

Description: The IDS_Import.log shows a database-related error if you add a 5.0(1) sensor and then try to add a second one too quickly. This symptom does not indicate a problem with IPS MC. Allow time for the addition of the first sensor to be finished.

Deployment

Table 21 *Deployment*

CSCin32177—Filter is not imported properly if it contains system variables

Description: Filter is not imported properly.

CSCsa35454—Quick Deploy re-generates all devices even when only one is edited

Description: Quick Deploy will generate and deploy a newly imported sensor configuration even if there have not been any changes to the config.

CSCsa57690—Not listening for sensor events after deployment

Description: For IPS 5.x devices, IPS MC 2.1 does not listen to sensor events after deployment to know the post deployment device status.

CSCsa91964—IPS MC deploys Event Action Filter names incorrectly

Description: After the creation of a custom signature from the IPS MC on a IPS 5.1 device with signature S205, deployment to the device will fail.

CSCsb00375—IPS MC does not retain the user-profile names during deploy

Description: IPS MC does not retain the user-profile names during deployment.

CSCsb03424—Address and net mask are not validated in Allowed Hosts

Description: IP address and netmask are not validated on Allowed Hosts page.

CSCsb12336—Deploying NTP settings from the group level does not work properly

Description: NTP server settings cannot be deployed from the global level when NTP settings are configured at the device level.

CSCsb16166—Required parameters of custom signatures not validated

Description: When using IPS MC 2.1 to create a custom signature for a 4.x device, IPS MC does not validate for all fields. If you do not tune the custom signature just created and try to generate and deploy to the device, deployment fails with a validation error.

CSCsb17807—Invalid filter IP address range causes deployment failure

Description: Custom filters added to or copied into sensor configurations from the IPS MC do not deploy because of an error. The IPS MC does not generate an error before deployment.

CSCsb50235—IPS MC should wait during deploy if sensor is busy

Description: Deploy to a sensor with configuration which requires sensor to rebuild its internal table. Immediately after the deployment, deploy it again. Deployment will fail.

CSCsb76969—Deployment fails for custom signatures: "sensorApp not responding"

Description: Deploy fails with the following error in Progress Viewer: BAD PARAMETER Missing Parameters at least one parameter must be specified

CSCsb88059—Deploy uses saved credentials instead of current device credentials

Description: Once device credentials settings are changed in IPS MC, deployment fails when you try to deploy configurations saved prior to device credential changes.

CSCsb94625—5.x custom signature parameters appear as "User Defined" not "Default"

Description: In the IPS MC 2.2 IPS 5.x tuning applet, a custom signature's parameters that are not tuned show up as "User Defined" rather than "Defaulted". This bug does not affect any functionality. However, it is confusing to the user to see signature tuning parameters in the GUI marked as user defined, when they are actually the default values. Also when accessing the sensor via CLI, parameter values which have default values do not display a keyword "defaulted".

Table 21 Deployment (continued)

CSCsc00425—Deploy: Error message does not indicate change of certificate

Description: Change in certificate on the device may cause the deployment from IPS MC to the device to fail with the following incorrect error message shown in the progress viewer window. “Unable to process Sensor Config Deploy - Can't get sensor version”.

CSCsc11816—second reimport of sensor fails; warns that sensor already exists

Description: The second reimport of a sensor fails with the following message while the first reimport for that sensor was successful: “ReImport Sensor Completed, sensor=<name>,status=A Sensor with the name <name> already exists in the system. re-import FAILED for <name>.”

CSCsc27361—IPS MC does not deploy the OPSig, which was deleted from device

Description: IPS MC does not deploy OPSigs that were deleted from the device.

CSCsc42736—Cannot Set SDEE Max Alerts or Max Messages for IOS IPS 2.2(1)

Description: Cannot set SDEE Max Alerts or Max Messages for IOS IPS 2.2(1).

CSCsc43198—Deploy actually failed but progress viewer says successful

Description: When an IOS IPS device has memory issues, they could be caused by a known problem about the SSH process not releasing memory. Deployment to the IOS device fails even though the UI may show that deployment succeeded.

CSCsc43420—Re-import fails after downgrading a sensor

Description: Re-import fails after downgrading the sensor.

CSCsc51299—Custom signature deploy failures after Sigcopy-Softcopy

Description: After you copy a custom signature for IPS 5.x device using Signature Copy Wizard, deployment might fail with following error message: “An exception occurred during deploy, file=signatureDefinition,detail= Export of the sensor file signatureDefinition failed:An exception occurred during the export of signatures, detail = Error on line 1: Attribute ‘xmlns’ was already specified for element ‘struct’.”

CSCsc57687—After Quick Deploy, Generate but not Deploy is completed

Description: If the license expires and is refreshed when IPS MC is running, operations such as Deploy/QuickDeploy/Signature Update/Auto download/Sensor health & welfare may not work even after license is refreshed.

CSCsc67483—IPS MC sending protected fields with custom signatures

Description: After you create a custom signature from the IPS MC on a IPS 5.1 device with signature S205, deployment to the device fails.

CSCsc71031—Deploy fails after a 5.1 major signature update

Description: After you upgrade a 5.0 sensor to 5.1, the deployment from IPS MC to that sensor fails with “unspecified” errors.

Intrusion Prevention System

Table 22 *Intrusion Prevention System*

CSCsc21489—JRE 1.4.2_08 client on same box as Security Manager server does not work
Description: IPS MC window suspends operation when launched in the same IPS MC server box. Java does not launch from that server and the Java Control Panel or Java Web Start does not run.
CSCsd04137—AutoUpdate fails to do minor update for IDS4x devices
Description: All signature updates and service pack/minor rev upgrades fail on 4.0(x) sensors.
CSCsd14292—IPS rules not imported into IPS MC
Description: IOS IPS Rules configured on inactive interfaces (interface that is done) will not be imported.
CSCsd14765—MC does not detect OOB when sig disable/enable on the IOS IPS device
Description: The Sensor Health and Welfare tool does not report out-of-band detection for devices were not imported into IPS Manager running on Security Manager.
CSCsd22884—Blank space in device display name leads to error
Description: In IPS MC during reimport, deploying and saving the changes in the Identification page results in an error stating 'Invalid Sensor Name'.
CSCsd24511—After upgrade, reimporting of IOS IPS device fails until sigupdate
Description: Reimporting IOS IPS devices fails with a error message of Null in the Progress Viewer.
CSCsd27301—BT:Syncing with Security Manager database fails during IPS MC DB upgrade
Description: DbUpgrade process fails during syncing with Security Manager with the message “Error in connecting to Security Manager Device Manager”.
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. This occurs when HTTP credentials are changed to (1) HTTPS with IPS Config = enable-tls true, (2) HTTP with IPS Config = enable-tls false, or (3) HTTP with IPS Config = enable-tls false.
CSCsd47977—SigUpdates Fail After Changing IP Address of Sensor
Description: The signature update fails with the following error message: The update of sensor <sensor-name> was stopped because the version the sensor is running is not compatible with the update package. The version in the configuration data is not the version reported by the sensor.
CSCsd68158—Auto download signature updates stop after 2 hours of downloading
Description: This problem occurs when you configure Auto Download to download signature update files from Cisco.com. The download times out (after 2 hours) if there are too many files to download from Cisco.com.

Reports

Table 23 *Reports*

CSCsa82957—Audit log contains error message after sigupdate

Description: Under certain conditions, an error message is seen in the Audit Log report after a signature update. This error occurs when a version number is in an unexpected format. IPS MC supports only major, minor, service pack, and signature level updates without virus numbers, for example, 5.0(2) S100.0. This error will occur when your version number is, for example, 5.0(0.2) S10. Note the “0.2” that causes the error.

CSCsa84230—Go to check box does not work on Completed Device Inventory report page

Description: On the Completed Device Inventory report page, the “Go to” check box does not work.

CSCsa99452—Modified By field shows no value in Sensor Version report

Description: The IDS Sensor Versions report displays “N/A” as the value in the “Modified By” column for all types of devices.

CSCsb04121—Device Inventory Report does not showing NAT address for IOS IPS

Description: For IOS IPS devices imported with NAT address, IPS MC 2.1 shows the NAT address value as N/A in the Device Inventory report.

Signature Tuning

Table 24 *Signature Tuning*

CSCsa85535—Deploying with all Event Actions enabled works incorrectly

Description: Deploying the configuration enabling all the Event Actions does not deploy all Event Actions.

CSCsb01664—Group level settings not shown when overriding

Description: During signature tuning, if override of group level settings is chosen, the Signature Tuning page refreshes and loads with default settings instead of loading with group level settings.

CSCsb01800—Group settings not inherited when device has default values

Description: When a signature is tuned at the group level, the import overrides the source as device even though the device has default settings.

CSCsb02047—Custom signature name change not reflected in GUI

Description: The custom signature name cannot be changed in the signature tuning applet for IPS 5.x in IPS MC 2.1.

CSCsb03503—SigTuning applet behaves differently for custom signatures

Description: In IPS MC 2.1, the signature tuning applet for IPS 5.x devices may not properly show the 'Changed/default' icon for Custom Signatures.

CSCsb04106—Event actions are not selected while editing Signature Properties page

Description: If no event action is selected, the generate will fail with the following message: An error occurred while adding the IDS5 signature information into the generated configuration, id =65000 sigid=255. Details: null, id =0 sigid=0.

CSCsb13334—Deploy fails after sigupdate if tune specify service ports

Description: Tuning some Normalizer engine parameters for sensor versions with signature level S149 or S150 (either at the Group level or the sensor level), then updating the sensor to S151 or beyond causes deployment to fail with the following error message from the Progress Viewer: “the union is protected”.

Table 24 *Signature Tuning (continued)***CSCsb16249—Tune Param Src field shown inconsistently for custom sigs after import**

Description: The “Tune Param Src” field is shown inconsistently under certain conditions. This problem occurs for custom signatures created at the group level after you generate, deploy, and reimport a device.

CSCsb75706—Not able to tune sig with blanked out non-mandatory fields

Description: In IDS 4.x sensors, user is unable to tune signature 7101 without setting values for two non-required parameters (e.g., ThrottleInterval and ResetAfterIdle). Normally, values do not need to be specified for non-required parameters.

CSCsc10841—Required params. not ID'd in custom sig. with sweep-other-tcp engine

Description: CustomSig of sweep-other-tcp type doesn't list required sig parameters.

CSCsc41756—GroupLevel Mandatory tuning w/default deploys 0 instd of 100

Description: The default value 100 of Choke Threshold (for a signature in the String.TCP engine) is not deployed to the device.

CSCsc41833—Signature params with encrypted data should be displayed for OPSigs

Description: Signature parameters that are protected are not displayed on the signature tuning screen for IOS IPS and IDS 4 devices.

CSCsc43120—Wrong choke threshold value on IOS IPS device following Quick Deploy

Description: The value of the ChokeThreshold displayed in IPS MC is incorrect for signatures that do not have the ChokeThreshold parameter specifically defined. The device uses an internal value of 0 for the Choke Threshold for signatures that do not have the Choke Threshold parameter defined. However, the default value of the Choke Threshold displayed in IPS MC is 100. For example, for the signature 3150, the Choke Threshold value displayed in IPS MC is 100 while the value displayed on the device is 0.

CSCsc48036—CustomSig deploy fails with Unexpected error, generate passes

Description: Deployment fails on a 5.0(1) sensor with a custom signature of engine application-policy-enforcement-http, “Regex List in order” set to no, and an active Regex active entry.

CSCsc54504—In multi-context, editing of both contexts not allowed together

Description: When you are working with a signature with more than one context for tuning, you cannot edit both contexts at the same time. (They can be edited in series but not in parallel.)

Signature Update

Table 25 *Signature Update***CSCsa84272—Signature update fails when parent group has pending changes**

Description: Under certain conditions, signature updates fail for IPS 5.x devices.

CSCsa90236—Created by user name is set to system for sensors after update

After signature update, IPS MC 2.1 shows the 'Created-by' field as “system” instead of the correct username.

CSCsb08376—Devices page doesn't reflect the SigUpdate details for 5.x sensors

Description: After a signature update, the old signature release level is still shown on the device page.

Table 25 *Signature Update (continued)***CSCsc44972—Error message is not clearly displayed during SigUpdate**

Description: During signature update, an error message is not clearly displayed in the Progress Viewer.

CSCsc82537—Auto update fails multiple updates to a sensor w/o license

Description: Multiple failures occur for the same sensor during auto update.

User Interface

Table 26 *User Interface***CSCsa55627—TLS setting cannot be changed**

Description: IPS MC 2.1 does not allow the user to either view or modify the TLS settings after the device is imported into IPS MC.

CSCsa60182—Regular expressions with . , characters cause errors

Description: Deploying a configuration to an IPS 5.x device from the IPS MC results in an error upon completion. If you view the status messages from the real-time Progress Viewer, you see a message that reports a regex error.

CSCsa60656—alt-tcp-reset interfaces are not allowed for interface pair

Description: Alternate tcp reset interfaces are not allowed for interface pairing.

CSCsa70617—Sensor Health tool does not report the mainApp failure correctly

Description: Sensor Health tool does not report the mainApp failure correctly.

CSCsa74236—Inconsistency in 4.x and 5.x sensor Statistics information

Description: On the Devices > Statistics page, IPS MC does not list the component “Interface” for a 4.x sensor although it is available for a 5.x device.

CSCsa83811—Cannot Undo Sensor Move

Description: If a sensor is moved to a different group using the Identification page, and the pending configuration is then deleted, the sensor will not revert to its original location or group.

CSCsa87433—Granting privilege to Help Desk user in Deploy page does not work

Description: If a Help Desk user is given Admin privileges to Deploy page (View, Generate, Approve, Deploy), the Quick Deploy icon on the Actions and Notifications panel is disabled and says: “You are not authorized to Generate and Deploy configurations.”

CSCsb00962—Source Addr and Dest Addr Range is not validated in filters

Description: Source address and destination address are not validated in filters.

CSCsb02080—IPS MC does not create EAF with the name given by the user

Description: The filter names that are defined by the user are not deployed to the sensor.

CSCsb02571—Configuration > History page does not list master blocking sensors

Description: Master Blocking Sensors are not displayed in “History Page” for a 4.x device.

CSCsb02977—IOS IPS signature actions propagated down to unsupported devices

Description: Unsupported event action options are inherited at device level for IOS IPS phase 1 (IPS subsystem version: 2.000(000)) devices.

CSCsb04133—Target value rating of zero not supported

Description: Target Value Rating for an IP address as “zero value” is not supported in IPS MC.

Table 26 *User Interface (continued)***CSCsb04175—Target value ratings in groups not properly handled**

Description: After configuring a Target Value at the group level and the device level, the IPS MC deploys successfully. But when the configuration is imported into IPS MC, the TVR page displays values inherited from the group level. The deletion of values at the group level deletes the value at the group level, but the device level displays the values with Sensor as the source.

CSCsb04873—Editing IP address in EAF is not handled properly

Description: When the user commits Attacker Address Range and Victim Address Range without making any changes during “Edit” operation, the entry is removed from the list.]

CSCsb04945—IPS MC does not provide an option to move EAF to inactive lists

Description: IPS MC Event Action Filter does not support INACTIVE LIST supported by IPS 5.x.

CSCsb06188—VS config is not displayed after Query Interfaces

Description: Virtual Sensor Configuration is not displayed in Virtual Sensor page after “Query Interfaces” operation is done in “Edit Virtual Sensor” Page.

CSCsb07030—Network Admin does not have privilege to do Quick Deploy

Description: Network Administrator cannot do a Quick Deploy.

CSCsb07781—IOS IPS default value of max SDEE Subscriptions incorrect

Description: For IOS IPS devices added with a default configuration, IPS MC 2.1 will incorrectly show the value of Max Subscriptions (under Configuration > Settings > Communications > IOSIPS SDEE Properties) as 2 instead of 1.

CSCsb09966—Some configurations not listed when copying 4.x devices

Description: Under certain conditions, not all of the eligible configuration settings are displayed in the Copy Wizard.

CSCsb10641—Page disappears for special characters in EAF parameter fields

Description: IPS 5.0 Event Action Filters page throws exception when special characters are given in Add/Edit Event Action Filters page.

CSCsb10708—Latest signature version not properly displayed

Description: IPS MC does not display the latest signature version properly.

CSCsb12753—5.x Sig event action filters allow duplicate names when editing

Description: 5.x signature event action filters (EAFs) allow duplicate names when editing. On a 5.x sensor with two or more EAFs, if one of the EAFs is edited and renamed to an already existing EAF, it is allowed by IPS MC and an exception is thrown in the stderr log.

CSCsb14747—Query Interfaces page throws errors for IPS5.x devices

Description: After you delete the interface pair imported from a sensor and reuse one of the interfaces to create another pair, the interface pair configuration becomes inconsistent between IPS MC and the sensor. Querying interface after that causes an error: “An error occurred trying to get the interface information. Interface XXX is part of another Interface Pair pair PPP.”

CSCsb17129—Deploying filters to sensor fails if sensor name has “-” character

Description: Deployment fails when the following two conditions exist: 1) the sensor has a name with one or more '-' characters in the name and 2) event action rules are defined on the sensor using IDM or CLI.

CSCsb61455—IOS IPS errors not being communicated back to IPS MC

Description: If you configure IOS IPS Port Mapping for IOS devices, IPS MC does not provide adequate validation to prevent the TCP port or UDP port from being used more than once.

Table 26 *User Interface (continued)***CSCsb84851—Group-level signatures can be deleted at device level**

Description: Group-level mandatory and non-mandatory signatures are allowed to be deleted at the device level.

CSCsb91613—Override check box on signature edit page causes loss of action values

Description: While editing a signature, clicking override loses Action values if multiple actions were selected/configured (for example, the previously selected action values are no longer selected after you select the override check box).

CSCsb98285—Internet Explorer stops during durability testing

Description: Internet Explorer randomly stops. This happens randomly and infrequently.

CSCsb73168—Boundary check not done for ChokeThreshold and MinHits sig 1000

Description: IPS MC accepts incorrect value for ChokeThreshold and MinHit Tuning Parameter for IDS 4.x devices.

CSCsb73188—Override unset and OK in quick succession gives NullPointerException

Description: Override unset and OK in quick succession gives NullPointerException.

CSCsc57478—4.x Custom-Sig created through CLI not present in IPS MC

Description: A custom signature with a value of 50000 created through the CLI for a 4.x device is not present in IPS MC.

CSCsc61460—Undo pending changes does not undo the changes for IOS IPS

Description: IPS MC 2.2 does not undo SDF type in Configuration > Identification page when pending settings are deleted.

CSCsc62468—Object Selector is not present for 4.x and IOS IPS device

Description: Object Selector is not available in the Signature Summary screen for custom signatures.

CSCsc62527—SDF type not shown in Identification page

Description: After you import from IOS devices, the Cisco SDF release version on the device is not shown in the Identification page for that device in IPS MC.

CSCsc27577—Event variables are deleted when in use by SigEvent Action Filters

Description: IPS MC does not display any warning message when you try to delete Event Variables that are used by SigEvent Action Filters.

CSCsc41770—Switching off Override and Mandatory works only in one order

Description: When tuning an IPS 5.x signature at the group level, if the “Override” and “Mandatory” check boxes are selected, they can be deselected only by following a special series of steps.

CSCsc43277—Generate does not preserve config names provided by the user

Description: Generate does not preserve config file names provided by the user.

CSCsc43309—500 Error when NTP server link clicked when device reimport in progress

Description: IPS MC will throw “500 Error...” when you click on the NTP server TOC item when reimport is in progress.

CSCsc36458—Attempt to import unsupported device throws null error

Description: Importing an unsupported device generates the following error message: “Unable to import sensor: null”

CSCsc45435—Sig tuned user comments not shown at group level after Save

Description: Signature tuning values are not shown at the group level after Save pending.

CSCsc47083—Cannot import a 5.x sensor using HTTP

Description: Importing a 5.x sensor that is configured to use HTTP (tls disabled) into IPS MC fails.

Table 26 User Interface (continued)

CSCsc47654—Master Blocking Sensors are not imported for 4.x devices

Description: Master Blocking Sensors are not imported into IPS MC for IDS 4.x devices. To work around this problem, add Master Blocking Sensors through the GUI before generating and deploying the configuration to the device.

CSCsc71383—View All does not show rate limit actions after reimport at group level

Description: Event Action “request rate-limit” will not be shown at the group level if IPS 5.0 is imported/re-imported to IPS MC.

CSCsc71434—Configurable items not displayed on IOS General Properties page

Description: IPS MC 2.2 does not show the 'Shun Event Timeout' and 'Enable Deny Action' fields in IOS General Properties screen for IOS IPS phase 3 type (IOS IPS engine version: 2.002) devices.

CSCsc73182—5.x deploy fails when custom signature is created at device level

Description: Deployment fails when deploying a custom signature to a 5.x sensor with S205 or a non-CCO version of S206.

CSCsc79119—Mandatory check box loses setting when group has more than one context

Description: Mandatory check box settings are lost when multiple contexts exist at the group level for the selected signature.

Where To Go Next

If you want to:	Do this:
Install Security Manager server or client software	See <i>Installation Guide for Cisco Security Manager 3.0</i> at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/installation/guide/ig.html .
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	To get up and running most efficiently, work through the “ <i>Getting Started Checklist</i> ” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0.2/user/guide/wfplan.html#wp1035392 .
Define essential settings	See “ <i>Define These Settings First</i> ” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0.2/user/guide/defapset.html#wp1035126 .

If you want to:	Do this:
Manage user authentication and authorization	To define user roles and permissions, see “ <i>Setting Up User Permissions</i> ” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0.2/user/guide/defapset.html#wp1035153 . To integrate Security Manager with Cisco Secure ACS, see “ <i>Integrating Security Manager with Cisco Secure ACS</i> ” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0.2/user/guide/defapset.html#wp1036148 .
Bootstrap your devices	See “ <i>Preparing the Devices for Security Manager to Manage</i> ” at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0.2/user/guide/ivman.html#wp1035100 .
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. To understand which applications are available for installation and plan your installation, we strongly recommend you begin by reviewing the installation guide overview at http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.0/installation/guide/overview.html .

Related Documentation

Table 27 describes the product documentation that is available.

Table 27 Product Documentation

Document Title	Available Formats
<i>Installation Guide for Cisco Security Manager 3.0</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/3.0/installation/guide/ig.html
<i>User Guide for Cisco Security Manager 3.0</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/products/ps6498/products_user_guide_list.html
<i>Supported Devices and Software Versions for Cisco Security Manager 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

Table 27 Product Documentation (continued)

Document Title	Available Formats
<i>FAQs and Troubleshooting Guide for Cisco Security Manager 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/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>User Guide 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/auto_update_server/3.0/user/guide/ausrvr.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/auto_update_server/3.0/compatibility/information/aus_dev.html
<i>User Guide for Cisco IPS Manager 3.0</i>	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/ips_manager/3.0/user/guide/ipsmug.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 and Submitting a Service Request

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

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.

© 2006 Cisco Systems, Inc. All rights reserved.

