Release Notes for Cisco Security Manager 4.0.1

Published: September 17, 2010

Revised: September 30, 2011

These release notes are for use with Cisco Security Manager 4.0.1.

Release 4.0.1 is now available. Registered SMARTnet users can obtain release 4.0.1 from the Cisco support website by going to http://www.cisco.com/go/csmanager and clicking **Download Software** in the Support box.

This chapter contains the following topics:

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

Introduction

Note Use this document in conjunction with the documents identified in Product Documentation, page 20. The online versions of the user documentation are also occasionally updated after the initial release. As a result, the information contained in the Cisco Security Manager end-user guides on Cisco.com supersedes any information contained in the context-sensitive help included with the product. For more information about specific changes, please see Where to Go Next, page 20.

This document contains release note information for the following:

- **Cisco Security Manager 4.0.1 (Including Service Packs 1 and 2)**—Cisco Security Manager (Security Manager) enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of firewall, VPN, and IPS services across IOS routers, PIX and ASA security appliances, IPS sensors and modules, and some services modules for Catalyst 6500 switches and some routers. (You can find complete device support information under Cisco Security Manager Compatibility Information on Cisco.com.) Security Manager also supports provisioning of many platform-specific settings, for example, interfaces, routing, identity, QoS, logging, and so on.

  Security Manager efficiently manages a wide range of networks, from small networks consisting of a few devices to large networks with thousands of devices. Scalability is achieved through a rich feature set of device grouping capabilities and objects and policies that can be shared.

- **Auto Update Server 4.0.1**—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. Security appliances with dynamic IP addresses that use the auto update feature connect to AUS periodically to upgrade device configuration files and to pass device and status information.

- **Performance Monitor 4.0.1**—Performance Monitor is a browser-based tool that monitors and troubleshoots the health and performance of services that contribute to network security. It helps you to isolate, analyze, and troubleshoot events in your network as they occur, so that you can increase service availability. Supported service types are remote-access VPN, site-to-site VPN, firewall, Web server load-balancing, and proxied SSL.

Note Before using Cisco Security Manager 4.0.1, we recommend that you read this entire document. In addition, it is critical that you read the Important Notes, page 7, the Installation Notes, page 4, and the *Installation Guide for Cisco Security Manager 4.0.1* before installing or upgrading to Cisco Security Manager 4.0.1.

This document lists the ID numbers and headlines for issues that may affect your operation of the product. 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.

Supported Component Versions and Related Software

The Cisco Security Management Suite of applications includes several component applications plus a group of related applications that you can use in conjunction with them. The following table lists the components and related applications, and the versions of those applications that you can use together for this release of the suite. For a description of these applications, see the *Installation Guide for Cisco Security Manager 4.0.1*.

Note For information on the supported software and hardware that you can manage with Cisco Security Manager, see the *Supported Devices and Software Versions for Cisco Security Manager* online document under Cisco Security Manager Compatibility Information on Cisco.com.

Table 1 Supported Versions for Components and Related Applications

Application	Support Releases
Component Applications	
Cisco Security Manager	4.0.1
Auto Update Server	4.0.1
Performance Monitor	4.0.1
CiscoWorks Common Services	3.3
Resource Manager Essentials (RME)	4.3
Cisco Security Agent	5.2
Related Applications	
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	6.0.5, 6.0.6
Cisco Secure Access Control Server (ACS) for Windows **Note** Cisco Secure ACS Solution Engine 4.1(4) is also supported.	4.1(3, 4), 4.2(0)
Cisco Configuration Engine	3.0

What's New

Cisco Security Manager 4.0.1 Service Pack 2

Security Manager 4.0.1 Service Pack 2 provides fixes for various problems. For more information, see Resolved Caveats—Release 4.0.1 Service Pack 2, page 17.

Cisco Security Manager 4.0.1 Service Pack 1

Security Manager 4.0.1 Service Pack 1 enables support for ASA Software Release 8.2(3) on all ASA platforms.

Security Manager 4.0.1 Service Pack 1 also provides fixes for various problems. For more information, see Resolved Caveats—Release 4.0.1 Service Pack 1, page 17.

Cisco Security Manager 4.0.1

In addition to resolved caveats, this release includes the following new features and enhancements:

- Support for these new Cisco ASA-5500 Series Adaptive Security Appliance models: 5585-X, all models.
- Support for ASA Software release 8.2(3) on the ASA 5585-X platform.

Note Security Manager 4.0.1 Service Pack 1 enables support for ASA Software Release 8.2(3) on all ASA platforms.

- Support for these Cisco 3800 Series Integrated Services Routers: 3825 NOVPN, 3845 NOVPN. You cannot configure VPN policies or other policies that require encryption on these devices.
- Support for these Cisco 3900 Series Integrated Services Routers: 3925E, 3945E.
- Support for Cisco IOS Software release 15.1(1)T.
- Support for Cisco IOS XE Software releases 2.5 and 2.6. These releases are known as 12.2(33)XNE and 12.2(33)XNF, respectively, in Security Manager. The only new feature supported in these releases is for DMVPN phase 3, which allows direct communication between spokes. Otherwise, software support is equivalent to release 2.4 (known as 12.2(33)XND).
- Support for Cisco ASA 5585 IPS Security Services Processor.
- Support for changes to the mechanism used for downloading sensor and signature updates from Cisco.com.
- You can now configure AAA access control using a RADIUS server for IPS devices running IPS Software release 7.0(4).
- A new device property, License Supports Failover, for ASA 5505 and 5510 devices that indicates whether an optional failover license is available on the device. The property is set when you discover device policies, or you can manually set the property. Failover policies are deployed to these devices only if the property indicates that the device has a failover license installed. This helps eliminate deployment failures due to failover licensing issues.
- Performance Monitor adds support for Cisco ASA-5500 Series Adaptive Security Appliance model 5585-X, and Cisco 3900 Series Integrated Services Routers 3925E and 3945E.
- IPS signature tuning has been enhanced. If you modify a signature policy with more than one tuning contexts, Security Manager can copy the policy to other contexts when appropriate and with your permission.

Installation Notes

Do not modify casuser (the default service account) or directory permissions that are established during the installation of the product. Doing so can lead to problems with your being able to do the following:

- Logging in to the web server
- Logging in to the client
- Performing successful backups of all databases

Internet Explorer 8 is supported, but only in Compatibility View. To use Compatibility View, open Internet Explorer 8, go to Tools > Compatibility View Settings, and add the Security Manager server as a “website to be displayed in Compatibility View.”

You can install Security Manager server software directly, or you can upgrade the software on a server where Security Manager is installed. The *Installation Guide for Cisco Security Manager* for this release of the product explains which previous Security Manager releases are supported for upgrade and provides important information regarding server requirements, server configuration, and post-installation tasks.

Before you can successfully upgrade to Security Manager 4.0.1 from a prior version of Security Manager, you must make sure that the Security Manager database does not contain any pending data, in other words, data that has not been committed to the database. If the Security Manager database contains pending data, you must commit or discard all uncommitted changes, then back up your database before you perform the upgrade. The *Installation Guide for Cisco Security Manager* for this release contains complete instructions on the steps required for preparing the database for upgrade.

We do not support installation of Security Manager on a server that is running any other web server or database server (for example, IIS or MS-SQL). Doing so might cause unexpected problems that may prevent you from logging into or using Cisco Security Manager.

For the *Installation Guide for Cisco Security Manager 4.0.1*, go to the list of Cisco Security Manager installation and upgrade guides on Cisco.com.

Be aware of the following important points before you upgrade:

- Ensure that all applications that you are upgrading are currently functioning correctly, and that you can create valid backups (that is, the backup process completes without error). If an application is not functioning correctly before an upgrade, the upgrade process might not result in a correctly functioning application.

  Note It has come to Cisco's attention that some users make undocumented and unsupported modifications to the system so that the backup process does not back up all installed CiscoWorks applications. The upgrade process documented in the installation guide assumes that you have not subverted the intended functioning of the system. If you are creating backups that back up less than all of the data, you are responsible for ensuring you have all backup data that you require before performing an update. We strongly suggest that you undo these unsupported modifications. Otherwise, you should probably not attempt to do an inline upgrade, where you install the product on the same server as the older version; instead, install the updated applications on a new, clean server and restore your database backups.

- If you install RME on the same server as Security Manager, do not apply the MDF.zip file available with the RME IDU patch. Applying this file will damage the device support files in Security Manager, and you will need to contact Cisco Technical Support to correct the problem. If you install RME on a server separate from Cisco Security Manager, this restriction does not apply.
- Security Manager 3.x users cannot upgrade directly to Security Manager 4.0.1. They must first upgrade to 4.0 and then to 4.0.1.

Service Pack 2 Download and Installation Instructions

Service pack 2 is a cumulative update that also includes the updates that were found in service pack 1. You can apply Cisco Security Manager 4.0.1 Service Pack 2 to a Cisco Security Manager 4.0.1 installation whether that installation has an earlier service pack installed or not.

To download and install service pack 2, follow these steps:

Note You must install the Cisco Security Manager 4.0.1 FCS build on your server before you can apply this service pack.

Step 1 Go to http://www.cisco.com/go/csmanager, and then click **Download Software** under the Support heading on the right side of the screen.

Step 2 Enter your user name and password to log in to Cisco.com.

Step 3 Click **Security Manager (CSM) Software**, expand the **4.0** folder under All Releases, and then click **4.0.1sp2**.

Step 4 Download the file fcs-csm-401-sp2-win-k9.exe.

Step 5 To install the service pack, close all open applications, including the Cisco Security Manager Client.

Step 6 If Cisco Security Agent is installed on your server, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 7 Run the fcs-csm-401-sp2-win-k9.exe file that you previously downloaded.

Step 8 In the Install Cisco Security Manager 4.0.1 Service Pack 2 dialog box, click **Next** and then click **Install** in the next screen.

Step 9 After the updated files have been installed, click **Finish** to complete the installation.

Step 10 On each client machine that is used to connect to the Security Manager server, you must perform the following steps to apply the service pack before you can connect to the server using that client:

a. If Cisco Security Agent is installed on the client, manually stop the Cisco Security Agent service from **Start > Settings > Control Panel > Administrative Tools > Services**.

b. Launch the Security Manager client.

   You will be prompted to “Download Service Pack”.

c. Download the service pack and then launch the downloaded file to apply the service pack.

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

Important Notes

The following notes apply to the Security Manager 4.0.1 release:

- You can use IPv4 addresses only in Security Manager. Although some of the device software Security Manager supports allows you to use IPv6 addresses on commands, Security Manager does not support IPv6 addresses directly. If you want to configure IPv6 features using Security Manager, you can use FlexConfig policies.
- You cannot use Security Manager to manage an ASA 8.3+ device if you enable password encryption using the **password encryption aes** command. You must turn off password encryption before you can add the device to the Security Manager inventory.
- ASA 8.3 ACLs use the real IP address of a device, rather than the translated (NAT) address. During upgrade, rules are converted to use the real IP address. All other device types, and older ASA versions, used the NAT address in ACLs.
- The device memory requirements for ASA 8.3 are higher than for older ASA releases. Ensure that the device meets the minimum memory requirement, as explained in the ASA documentation, before upgrade. Security Manager blocks deployment to devices that do not meet the minimum requirement.
- If you have a device that uses commands that were unsupported in previous versions of Security Manager, these commands are not automatically populated into Security Manager as part of the upgrade to this version of Security Manager. If you deploy back to the device, these commands are removed from the device because they are not part of the target policies configured in Security Manager. We recommend that you set the correct values for the newly added attributes in Security Manager so that the next deployment will correctly provision these commands. You can also rediscover the platform settings from the device; however, you will need to take necessary steps to save and restore any shared Security Manager policies that are assigned to the device.
- 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.
- Do not connect 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.
- Cisco Secure ACS 5.0 is not supported by Security Manager 4.0.1, even though ACS 5.0 is supported by Common Services 3.3.
- If you do not manage IPS devices, consider taking the following performance tuning step. In *$NMSROOT*\MDC\ips\etc\sensorupdate.properties, change the value of packageMonitorInterval from its initial default value of 30,000 milliseconds to a less-frequent value of 600,000 milliseconds. Taking this step will improve performance somewhat. [*$NMSROOT* is the full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).]

Caveats

This section describes the open and resolved caveats with respect to this release.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:
http://www.cisco.com/support/bugtools
To become a registered cisco.com user, go to the following website:
http://tools.cisco.com/RPF/register/register.do

This section contains the following topics:

Open Caveats—Release 4.0.1

The following caveats affect this release and are part of Security Manager 4.0.1.

Note In some instances, a known problem might apply to more than one area, for example, a PIX device might encounter a problem during deployment. If you are unable to locate a particular problem within a table, expand your search to include other tables. In the example provided, the known problem could be listed in either the Deployment table or the PIX/ASA/FWSM Configuration table.

Table 2 ASA, PIX, and FWSM Firewall Devices Caveats

Reference Number	Description
CSCse51450	OSPF validations are not adequate
CSCsh20731	FAILOVER - Active/Active deploys to Standby unit and returns errors
CSCsi24397	SLA: Interface roles assigned to an SLA Monitor not validated
CSCsi34972	OSPF Discovery: Deployment of incomplete OSPF policy invalid
CSCsi44546	RIP configuration commands in PIX/ASA 7.2(1) cannot be fully managed
CSCsl51451	Enable DHCPD auto configuration with interface option not discovered

Table 2 ASA, PIX, and FWSM Firewall Devices Caveats (Continued)

Reference Number	Description
CSCsm82107	Discovery of a multi-mode ASA added to CSM as a new device fails
CSCsr17662	Deployment of ips command truncated if containing class map is changed
CSCtd60804	CSM managing A/A FWSM will not use configured management ip of context
CSCth74557	Error deleting tenGig sub-interface in system context

Table 3 CSM Client and Server Install Caveats

Reference Number	Description
CSCte49471	CSM installer should check for supported SP during install
CSCte56524	Not able to launch the CSM client after upgrade (CSM3.3SP1 to CSM4.0)
CSCtf78013	CS patch install fails when CSM is installed on Japanese windows
CSCtg58541	CSM coexistence problem with Symantec Event Manager startup sequence
CSCti37345	Diagnostics collector doesn't zip up SP pack install logs
CSCti79240	Not able to install incremental device license in CSM 4.0

Table 4 Cisco Catalyst 6000 Device Support Caveats

Reference Number	Description
CSCsi17608	Deployment fails when allowed VLAN ID is modified on IDSM capture port
CSCsi24091	Deploy fails if you change access to trunk mode & enable DTP negotiation

Table 5 Cisco IOS Router Devices Caveats

Reference Number	Description
CSCsf09088	PPP policy does not support if-needed and local-case keywords for AAA
CSCsh18926	NetFlow deployment fails on subinterfaces
CSCsi20458	802.1x-Number of retries command not generated correctly
CSCsi25845	PPP-No validation for multilink support on device
CSCsi45142	AAA - source intf disc from global cmd instead of aaa subcommand
CSCsi45204	QoS policy not discovered when WRED is enabled
CSCsr14267	Discovery failure with target os 12.3(9) does not exist
CSCsr45265	Negation is not getting generated for policies using nonexistent ACL
CSCsz79334	Deployment fails on changing VTY authentication method frm AAA to local.
CSCta73192	NTP Authentication key is not negated for 3945 router
CSCta84886	RIP-Deployments fails for RIP policy but CLI are pushed into the device
CSCta84894	BGP-Unassign bgp pol+Deploy,Deployment fails for 861 Router for 15.0 ima
CSCta84907	Deployment fails after unassigning BGP policy

Table 5 Cisco IOS Router Devices Caveats (Continued)

Reference Number	Description
CSCth57536	Filters not working in QOS->Control Plane and Interfaces->settings->CEF
CSCth66433	no auto-summary in EIGRP discovered as auto-summary for infusion device
CSCth79839	ASR: Advanced Interface Settings: MOP needs to be enabled by default
CSCth94343	HTTP-Radius Retransmit on Dev-Key Not Disc & Retransmit Removed on Deploy
CSCth94684	Static: No Cli Generated when Null0 Interface is selected
CSCth94764	RIP: “Chain” is Masked instead of Key Chain Name
CSCth94840	XNE: Syslog: Both Standard and XML Syslog Buffers are Allowed on Device
CSCth94895	XE:MemoryThreshold Notification can be configure only for Free Processor
CSCth95357	XE: Deploy Fails when Memory Critical Notifications are Changed
CSCti02291	EIGRP Removed if Network is Changed
CSCti02324	ASR - BGP - redistribute static - clns does not appear on device
CSCti02438	Dialer Profile - Named Acl is Created During Discovery
CSCti02504	PVC - UI Issues
CSCti02548	ASR - PVC/OAM - Unsupported Cli
CSCti02928	Cannot Rollback Either from Config Archive or Deployment Manager
CSCti15944	CLI: “dot1x pae authenticator” generated after deployment of 802.1x
CSCti22798	Infusion: RAVPN Checkbox should be disabled in Bulk Re-discovery Panel

Table 6 Cisco IPS and IOS IPS Devices Caveats

Reference Number	Description
CSCse95933	IPS related policies should be listed in device properties page
CSCsg25899	IPS 6.x pol. should not be listed for 5.x devices in copy & share policy
CSCsg38052	VLAN groups need to display “unassigned” VLANS
CSCsg51052	After Abort, progress bar continues to 100% and Status remains = Started
CSCsg78129	Copy policies between devices with VS as source only shows VS's as destn
CSCsg80289	Warning message is displayed during blocking policy deployment.
CSCsh02407	Autoupdate setting value for a device should be same in device tree.
CSCsh36604	IPS EAO: After editing a row, the ed. row is displayed as the last row
CSCsh52484	IPS Licensing Date varies between sensor CLI and sensor
CSCsh53265	On IPS Update page, checkbox for shared sig. policy can be incorrect
CSCsh67506	Dynamic IP address IOS router imported by CNS cannot be discovered
CSCsh77105	During deployment, signatures removed from current.xml
CSCsh86189	Sig update fails when using HTTP if console logging is on
CSCsi01650	EAF: Show content option in context menu for victim addr is not working
CSCsi26525	OOB OPACL changes not resynced after successful deploy

Table 6 Cisco IPS and IOS IPS Devices Caveats (Continued)

Reference Number	Description
CSCsi39380	Deployment of NTP policy with policy objects sometimes fails
CSCsi44605	IPS variable names cannot contain special characters.
CSCsi47289	Policy object overridden at VS level is not deployed correctly
CSCsj60530	Inventory alone discovery fails for IPS 6.x device for submit operation
CSCsl70245	Licensing: Repeated clicking of refresh button shows duplicate entries
CSCsm32616	CSM - Needs a way to remove old IPS metadata
CSCsm72033	Deployment Failed error on Event Action Rules
CSCso11145	CSM daily autodownload every 2 days should start from the present date
CSCso11482	MultiContext not handled in ApplyIPSUpdate wizard upon SigEditParams
CSCso17575	Intf Policy copy betn same IPS models but diff interface cards fails
CSCsr19163	OS Id.'s ->Restrict to these IP address field should not map to pol. obj
CSCsr31140	Err loading pg if NTP policy from 6.1 dev is copied to 6.0/5.1 dev
CSCsv44809	Rules and AD profile name changes with multiple vs profile config
CSCsv85664	Security Manager swaps names of policies while deploying to device
CSCsv91055	Security Manager Deployment UI shows OOB for unsupported commands
CSCsx72883	Link for Interface help for SSC is redirected to Product Overview
CSCsx98868	IOS IPS: Cannot deploy custom signature for "normalizer" engine
CSCsy03168	IOS IPS: SDEE properties cannot be discovered if SDEE is disabled
CSCsy47123	Unable to unshare a shared policy for un-supported platform in dev view
CSCsy51377	Package download fails with error msg Download not enough space on disk
CSCsy56978	IOS IPS version should be updated with changes in IOS version
CSCsy60393	Security Manager does not push "category ios_ips basic" command properly
CSCsy89865	Not able to do signature update on IPS-4260 running 5.1(8)E2.9S342.0
CSCsz33707	Licenses are not shown in IPS tab post ACS Integration without refresh
CSCsz35545	Pre-ACS integrated devices are shown in IPS updates page
CSCta90115	Cannot deploy service module policy in IOS
CSCtb16577	on applying sig pkg to the device, New sig(s) is not listed on sig page
CSCtb40828	Signature deploy failed with "category ios_ips default" command
CSCtb55176	Sensor update fails on applying sensor pkg manually with OOB change
CSCtc57010	No validation for incorrect speed/duplex setting for 10G Interface
CSCtc81519	IPS Validation warnings still show up after unassigning shared policies
CSCte61977	Delta shown for user profiles(no conf chng)after remote upgrade (3.3.1)
CSCtf08622	CSM will not recognize new AAA syntax from IOS 12.4(22)T
CSCtf40838	Licence Refresh functionality is broken when navigating between tabs
CSCtg23806	CSM discovery fail when Signature ID 50000 or later is modified
CSCtg47573	Event Action Filter variable problem

Table 6 Cisco IPS and IOS IPS Devices Caveats (Continued)

Reference Number	Description
CSCtg49034	Migration log: IPS backward compatible devices are not reported
CSCtg86699	Fails to apply a license to IPS
CSCth02638	sig 2158.0 remains enabled when updated from CSM
CSCth14454	CSM Policy view does not save settings when DNS servers are added.
CSCth80671	CSM: Corrupted IPS signature registration prevents re-registration
CSCti00195	reference context copy overrides the non-reference context local tuning
CSCti22345	CSM fails to deploy scheduled sig auto-update for IPS, and doesn't skip
CSCti23458	AAA policy managed as backward compatible throws wrong error post upgrade
CSCti35244	Validation error when sharing the new engine with older signature device
CSCti50519	After inline CSM upgrade, IPS database table is missing a column
CSCti56328	Discovery issue in CSM 3.3 SP2
CSCti73913	CSM: Checksum failed when downloading IPS signature S511
CSCti78774	sig tunings are not stored in csm for Multi-string engine signature

Table 7 Device Management, Discovery, and Deployment Caveats

Reference Number	Description
CSCsg29287	Not able to discover device if the banner has > or #
CSCsh63248	Add field in DM to specify whether device is Admin Context or not
CSCsi18673	Security Manager deployment may trigger ObjectGroup name warnings.
CSCsi18678	Security Manager deployment may trigger interface name warnings
CSCsk59843	DCS to monitor the Admin context CLI
CSCsq32343	HitCount -- Internal Failure
CSCsy98103	Config-diff shows diff between two configs though they are exactly same.
CSCta39358	Rollback is not working properly with ASA
CSCtb31451	In 3.2.2, database corruption in device_dirty_status table
CSCtc77997	Missing information in the FQ logic.
CSCte65524	Failover: Deployment takes a long time
CSCtf32208	Deployment fails with ACE edit in ACL BB
CSCtf51909	CSM does not deploy crypto related configuration to AUS
CSCtf78036	Deployment summary shows successful though deployment not done.
CSCtg87338	CSM 3.3.1 SP1 wrong deployment of ACLs to ISR running 12.4(24)T code
CSCth16062	Changes to shared credentials policy does not sync with CSM inventory
CSCth32152	CSM doesn't allow to deploy to a device that's part of a pending job
CSCth57997	One time deployment job shown as recurring in deploy manager
CSCth77654	Failover License Checkbox not updated after re-discovery

Table 7 Device Management, Discovery, and Deployment Caveats (Continued)

Reference Number	Description
CSCti36267	CSM: Remote Access VPN 'send FQDN to client' checkbox doesn't function
CSCti42824	Error Message Popup when deployment manager is opened in CSM 4.0.1

Table 8 Event Viewer Caveats

Reference Number	Description
CSCtd27974	Floating view minimized by default.
CSCtd33930	Real-time event row selection not retaining
CSCtd49651	Select all in custom filter with filter criteria not correct.
CSCtd59852	Custom filter does not remember values when some filter is applied.
CSCtd71393	Event Viewer must provide the ability to filter in a signature ID
CSCtd74239	"Backplane" & "physical" interface fields are always blank for events
CSCtd80726	Time slider doesn't show correct trend for view with long duration.
CSCte18239	Continue showing 'Navigating to.' dialog even if crosslaunch is canceled
CSCte37331	Internal error thrown on opening view having BB which is deleted.
CSCte37802	Custom filters using BB should have view option to see BB contents.
CSCte90167	[SSL VPN] Explanation and recommended action not displayed correctly.
CSCte92834	Need to modify format of "IP Log Id" values under "Displayed Fields" tab
CSCtf07664	No warning if event data store size is reduced than actual stored events
CSCtf21124	Some of the old event data folder is not getting deleted
CSCtf44733	EPS statistics not correct for ASA and IPS in Time-slider.
CSCtf61897	Unselecting a sigId should unselect it under all Signature Categories
CSCtf79977	Setting log level to SEVERE for Event management logs debug messages
CSCtg17154	Floating window goes invisible on clicking Cancel Close
CSCtg17383	Real time events with sort on non-default columns shows empty rows
CSCtg34811	View creation fails though view with same name not present.
CSCtg35646	Closing pre-defined view with filter changes should ask for save as.
CSCtg45140	Custom Filter shows Empty Categories for Syslog and Signature
CSCtg46517	ASA Eventing: Incorrect event names for some syslogs
CSCtg54222	Eventing Restore: Restore failing or partially succeeding in some cases
CSCtg57676	Internal error thrown when port list is used in service object filter.
CSCtg57745	Filtering does not work when only protocol name is used in service obj.
CSCtg57839	Results not correct when network obj with non-contiguous mask is used.
CSCtg75129	VmsEventServer doesn't come up after CSM DB restore.
CSCtg78128	Save required after device/BB is deleted and custom view is launched.
CSCth04745	Event Data Store Location change is not working

Table 9 Firewall Services Caveats

Reference Number	Description
CSCsc22934	ACL limitations for Layer 2 interfaces on IOS ISR devices
CSCsh68101	Activity Report: Issues with access rules table change report
CSCsh94210	Problems matching interface name when reusing AAA policy objects
CSCsi18871	Inspect Map: PIX 7.1 gtp-map subcommand order is not preserved
CSCsk33350	Discovery of PAM Mappings with Inspection Rules is incorrect
CSCsk46057	Changes to csm.properties files lost during Security Manager upgrade
CSCsr25786	AAA server object: no error issued when interface not specified
CSCsz53354	MAC Exempt list cannot be ordered
CSCtb00116	Wrong error message after sorting the Access control by ACL name
CSCtb03821	Failover: Deployment fails with subinterface as failover Interface
CSCtb51491	Delta generated for Object-groups
CSCtc44562	DES: Unmanaged policy-map configs removed after discovery
CSCtc56731	Cannot edit device overrides in nested ACL objects
CSCtc77998	SNMP Policy: Port field is applicable to only the admin context.
CSCtd46245	Security Level changes when name of interface changed
CSCtd71241	Unassign of translation rules should remove object nat rules also
CSCte08355	Auto NAT: Ordering of Auto NAT rules is not correct.
CSCte44602	Bottom align single row column headers if other headers are on 2 rows
CSCtf08441	ZBF:No validation message for protocols unsupported with IOS versions
CSCtf32103	ACL BB renames if remark is used
CSCtf68128	Proposed Performance optimization in NAT (translation and simplified)
CSCtf86613	Generates the duplicate port-map commands with ZBF port-map config
CSCtg08943	Deployment fails because of duplicate entries in the NAT address pool.
CSCtg21437	Discovery fails if IOS config contains OGs with name larger than 64 char
CSCtg48075	Simplified NAT: Additional validation required in Activity Validation
CSCtg60293	<NAT Rule> select Edit Source, not displaying BB selector Dialog
CSCtg64802	Edit BB throws Exception, After select OK button,If same name BB present
CSCtg73323	Add Singleton network object (host/network) takes more time than groups
CSCtg77573	Section feature supporting in NAT on ASA 8.3 and above
CSCtg80500	Manual-NAT: need validation for “neq” operator in static NAT
CSCtg84393	Fail to Removing un-reference object-groups leads to deployment fails
CSCtg89541	Discovery of asr-group in ASA 8.3.1 on CSM is not displayed
CSCtg91677	CLI for object generated even when it was not referred
CSCth01039	BV-NAT: Unable to delete last NAT rule with disable/enable operation
CSCth52454	CSM is altering manually deployed ACL/tcp-map names after deployment
CSCth62038	ASA: Error with more then 2 net-flow collector configuration in CSM

Table 9 Firewall Services Caveats (Continued)

Reference Number	Description
CSCti05438	CSM deploys dhcpd enable <nameif> if interface was removed in deployment
CSCti42271	Unable to deploy with large config due to Java.lang.NullPointerException
CSCti58861	CSM 4.0 discovers ASA 8.3 interfaces with uppercase fails deployment
CSCti62242	CSM: redundant mgmt int config delta sent to ASA in transparent mode
CSCti64353	CSM re-orders rules wrongly, and it causes rules deleted wrongly

Table 10 FlexConfig Caveats

Reference Number	Description
CSCti37583	CSM 4.0 Move Up and Move Down buttons delete FlexConfig lines

Table 11 Miscellaneous Caveats

Reference Number	Description
CSCsk11268	A User Can Open Multiple Sessions in Non-Workflow Mode
CSCsk78778	Error not shown for unavailable ACE during MARS events lookup
CSCsk94278	Read-only policy page in MARS is blank after starting Security Manager
CSCsm50836	MARS credentials retained in cache after changing authentication option
CSCsm68564	Disabled rules not shown as inactive in read-only policy page in MARS
CSCsy30953	CSM 3.2.2 does not release feature locks on a discarded activity
CSCsz81607	Last run entry not seen in Deployment Schedule on page refresh.
CSCta17924	MCP: Tunnel packet counters not updated for P2P S2S VPN on VSPA.
CSCtb81848	Security Manager - Server does not start - regdaemon.xml corrupted
CSCtc59526	Security Manager client performance upgrade
CSCtd87603	Performance Monitor not generating e-mail alerts
CSCte37778	Manual NAT: Incomplete display of menu bar
CSCte54843	MCP - cannot import VPN in HSRP configuration
CSCtg10817	CSM with ACS integration with WF db loaded takes 15 mins to login
CSCtg35295	failed login attempts don’t get logged in the audit log
CSCth07721	CSM is not prompting for license again when invalid license is given
CSCth10625	Pro- Time Bound license is behaving like pro- permanent license
CSCth15163	MCP:Packet In and Out Counters not updated for device in DMVPN topology
CSCth41026	Importing ACL rules w/ object-groups in CSM fail
CSCth66666	CSM CLient session hangs around when user is logged out
CSCth66680	CSM Client policy configuration is not exclusive to a user
CSCth92479	MCP/PM sometimes misses Event/Notifications
CSCti05502	Additional Interfaces like Null0 and Backplane are shown for Informers

Table 12 Policy Management Caveats

Reference Number	Description
CSCth79407	Deleted object still exists in DB and causes new device import failure.
CSCti17452	Object deletion of large number of objects leads to Sybase jConnect err
CSCti66531	Edit device overrides dialog takes unduly long to load if many overrides

Table 13 VPN Device and Configuration Support Caveats

Reference Number	Description
CSCse94752	Support for IOS version 12.2(33)SRA on 7600 devices
CSCsg70526	EzVPN - default tunnel-groups are not handled by Security Manager
CSCsh14709	Deployment fails on ASA 5505/PIX 6.3 Easy VPN remote client
CSCsh79282	Cat6k-SPA GRE+Multicast - unsupported
CSCso63006	IPSEC VPN import failed when crypto ACL contains intf in source/dest
CSCsq66815	Side-effects due to missing Protected Network's assignment usage info
CSCsr23893	Remote Access VPN - Activity validation reports error for http-form
CSCsy83931	VPN policy discovery fails when tunnel source defined with IP address.
CSCsz79453	CS Mgr discovery fails when NAT IP address is configured with LPIT.
CSCta92510	Regular ipsec discovery - Preshared key Aggressive mode not discovered
CSCtc18700	CS Mgr 3.3 not showing modified DfltGrpPolicy in RA VPN
CSCtd71798	CSM: ASA VPN creation/discovery failure if interface ip is not static
CSCtg26926	CSM - add incomplete smart-tunnel CLI
CSCtg98391	Lan-to-lan cannot be discovered if RA VPN was already discovered
CSCtg98419	Discovering RA VPN causes discovered Lan-to-Lan config to be removed
CSCth05090	VPN on ASA cannot be discovered when infinite keyword is used for DPD
CSCti37498	CSM deploys crypto enroll after importing device with existing cert
CSCti55212	Unable to remove password management from tunnel group
CSCti69683	CSM 3.3.1 SP1: IKE PKI Warning if trustpoint is configured for SSL

Resolved Caveats—Release 4.0.1 Service Pack 2

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.0.1 Service Pack 2.

Reference Number	Description
CSCto81899	CSM removed some ACLs that resulted in network outage
CSCtq63992	CSM - Arbitrary command execution vulnerability.
CSCtr28607	CSC 4.0.1 SP1 Preview fails for ASA 8.3.2 config
CSCtr79564	Bundle defect for known vulnerabilities in CiscoWorks Common Services.

Resolved Caveats—Release 4.0.1 Service Pack 1

The following customer found or previously release-noted caveats have been resolved in Cisco Security Manager 4.0.1 Service Pack 1.

Reference Number	Description
CSCsr23976	"ip local pool" DDP doesn't translate name assigned to ip addr ranges
CSCsv01908	CSM 3.2.1 SP 1 unable to use local user password of length 17-31 charact
CSCsz43023	ZBF: Activity validation does not consider BB override
CSCtd44879	CSM Deploy fails if removing web-type ACL that is applied to mult DAPs
CSCtd49734	Network/Service BB objects should retain the order
CSCte77128	UE: Deployment Devices Dialog - provide option to expand nodes
CSCtf08622	CSM will not recognize new AAA syntax from IOS 12.4(22)T
CSCtf21124	Some of the old event data folder is not getting deleted
CSCtg34811	View creation fails though view with same name not present
CSCti17452	Object deletion of large number of objects leads to Sybase jConnect err
CSCti37498	CSM deploys crypto enroll after importing device with existing cert
CSCti58861	CSM 4.0 discovers ASA 8.3 interfaces with uppercase fails deployment
CSCti64353	CSM re-orders rules wrongly, and it causes rules deleted wrongly
CSCti70139	Move section up/down is not working
CSCti80866	Re-Deploy w/o changes - set peer cli negated on ASA
CSCti95311	CSM - Query window pop-up is not appearing
CSCtj01008	CSM - selected object does not expand completely
CSCtj03660	CSM - switching back to access rule is very slow if filter is applied
CSCtj07173	users are allowed to create duplicate static routes
CSCtj14016	RAVPN:CSM needs to support CSD 3.5.1077
CSCtj24757	RAVPN: Need support for 'Windows 7' OS version in DAP entry
CSCtj25820	CSM: IPS signature registration fails with out of memory errors
CSCtj28155	BB caching is shutdown causing performance degradation
CSCtj33069	Object NAT: intf name with non lowercase does not show up in Object NAT

Reference Number	Description
CSCtj48666	8.2.3 validation check disabling
CSCtj59121	CSM: IPS event viewer doesn't display events when connection is stuck
CSCtj63343	CSM pushes incorrect config for DAP Policy for Symantec personal FW
CSCtj68043	Static NAT and PAT rules are not always added back to the configuration
CSCtj68560	CSM generates incorrect DAP LUA expressions for Process checks
CSCtj70266	Preview Fails --> Deployment failed due to an internal error in plugin
CSCtj71755	CSM: 8.3 destination nat displayed incorrectly
CSCtj72334	Save in predefined view not working
CSCtj75056	CSM does not generate LUA expression for Device category attributes
CSCtj77768	VPN config - ASANAT configuration causes deployment error
CSCtj78669	CSM 4.0 LDAP attribute map customer map value does not support space
CSCtj81252	CSM 3.3(1) - variables in FlexConfig script not correcty populated
CSCtj84306	DAP-Logical operation 'Match-All' for Personal FW are not saved properly
CSCtj86328	auto update failing for IPS
CSCtj92430	Beta: Error populating time slider for some of the historical queries
CSCtk12417	Eventing: 'idx' folder not Getting Deleted
CSCtk36374	Net Admin not able to deploy even if deployment approval is disabled.
CSCtk58951	CSM dirties system defined service obj when created frm within ruletable
CSCtk63681	CSM policy object manager content sorting not working
CSCtk64596	IPS download: Unnecessary URL conn made before checking MD5 and closed
CSCtk66798	CSM removes existing NAT0 ACL and creates new one per interface
CSCtk83060	Group Policy, Cert Map, DAP , Address Pool Discovery
CSCtk94944	Unable to view all the Events in EV after a query + navigation operation
CSCtl12521	CSM pushes incorrect DAP type for Device criteria-OS service pack
CSCtl53112	Detect/notify if server patch is not matching with client patch after CP
CSCtl58341	CSM ignore the first device in 2,3,.. N jobs of autodownload
CSCtl82415	CSM creating multiple deployment job at a same time.
CSCtl92187	CSM use wrong cmd syntax when disabling "log with interval" option
CSCtl94142	Change report shows passwords in clear text
CSCtn07096	While enabling Do not translate vpn traffic delta seen after deployment
CSCto41702	LDAP attribute maps not editable after migration to 4.1

Resolved Caveats—Release 4.0.1

The following customer found or previously release-noted caveats have been resolved in this release.

Reference Number	Description
CSCtc43031	preview configuration failing network object non-contiguous mask
CSCtc43845	Failover: ASA license-related deployment failure
CSCte60495	AUS 3.3SP1 'no monitor-interface' ASA base license auto-update failure
CSCtf32502	Deployment changes IPS WEBPORT setting to Default
CSCtf71882	Deployment failure when Static Route policy uses "all interfaces" role
CSCtg33456	Inspection rule with HTTP map - Deploy fails
CSCtg67869	DNS cli not generated for 2nd row onwards and double negation cli
CSCtg80784	Shared signature policies are not visible after signature update
CSCth13856	CSM doesn't deploy "no management-only" to management interfaces
CSCth19929	CSM 3.3.1: No option for bypass mode configuration for AIP-SSM module.
CSCth55266	Diagnostic Zip not put in specified folder with windows CLI prompt
CSCth61349	Performance Monitor does not show throughput data

Resolved Caveats—Releases Prior to 4.0.1

For the list of caveats resolved in releases prior to this one, see the following documents:

- http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html

Where to Go Next

If you want to:	Do this:
Install Security Manager server or client software.	See *Installation Guide for Cisco Security Manager 4.0.1*.
Understand the basics.	See the interactive JumpStart guide that opens automatically when you start Security Manager.
Get up and running with the product quickly.	See "Getting Started with Security Manager" in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager 4.0.1*.
Complete the product configuration.	See "Completing the Initial Security Manager Configuration" in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager 4.0.1*.
Manage user authentication and authorization.	See the following topics in the online help, or see Chapter 2 of *User Guide for Cisco Security Manager 4.0.1*. • Setting Up User Permissions • Integrating Security Manager with Cisco Secure ACS
Bootstrap your devices.	See "Preparing Devices for Management" in the online help, or see Chapter 5 of *User Guide for Cisco Security Manager 4.0.1*.
Install entitlement applications.	Your Security Manager license grants you the right to install certain other applications—including specific releases of RME and Performance Monitor—that are not installed when you install Security Manager. You can install these applications at any time. See the Introduction to Component Applications section in Chapter 1 of *Installation Guide for Cisco Security Manager 4.0.1*.

Product Documentation

For the complete list of documents supporting this release, see the release-specific document roadmap:

- *Guide to User Documentation for Cisco Security Manager*

  http://www.cisco.com/en/US/products/ps6498/products_documentation_roadmaps_list.html

  Lists document set that supports the Security Manager release and summarizes contents of each document.

- For general product information, see:

  http://www.cisco.com/go/csmanager

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:

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.