Release Notes for Management Center for Cisco Security Agents 5.0

These release notes are for use with Management Center for Cisco Security Agents (CSA MC) 5.0. The following information is provided:

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

Installation Information

This CSA 5.0 release is supported with VMS 2.3.

It is recommended that you do not install other VMS products on the system to which are installing Management Center for Cisco Security Agents. Only install the "Common Services" needed for VMS in addition to CSA MC.

Caution When you install VMS 2.3, by default, checkboxes for several VMS products on the "Select Components" install screen are selected. You should click the Deselect button. Then select the "Common Services" checkbox and click Next to continue.

Obtaining a License Key

The Management Center for Cisco Security Agents CD contains a license key which is used to operate the MC itself. If you need further license keys, before deploying Cisco Security Agents, you should obtain a license key from Cisco. To receive your license key, you must use the Product Authorization Key (PAK) label affixed to the claim certificate for CSA MC located in the separate licensing envelope.

To obtain a production license, register your software at one of the following web sites.

If you are a registered user of Cisco.com, use this website:

http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl.

If you are not a registered user of Cisco.com, use this website:
http://www.cisco.com/pcgi-bin/Software/FormManager/formgenerator.pl.

After registration, the software license will be sent to the email address that you provided during the registration process. Retain this document with your VMS bundle product software records.

File Integrity Check Instructions

You can perform integrity checks on the files provided with Management Center for Cisco Security Agents 4.5. Use the verify_digests.exe file provided to check the MD5 hashes of the files.

When you run the verify_digests.exe file, you can enter the CD drive letter and check the files on the CD itself or you can copy the files to your system and check them from the directory to which they were copied.

The following output is displayed:

- The output displays "OK" if the hashes match and the files are valid.
- If the hashes do not match, "Failure" is displayed. Contact Cisco if this occurs.

How to install obtain and install VMS 2.3:

Step 1 If you have not received a CD containing VMS 2.3, you should download these four files: VMS-23-W2k-CD1-image-K9.z01, VMS-23-W2k-CD1-image-K9.z02, VMS-23-W2k-CD1-image-K9.z03, VMS-23-W2k-CD1-image-K9.zip from http://www.cisco.com/cgi-bin/tablebuild.pl/vms into a scratch directory

Step 2 Run winzip on the fourth file and unzip the entire contents into a temporary directory.

Step 3 Run **vmmc_verify_digest.exe** to ensure the integrity of your download.

Step 4 Run **autorun.exe** to begin the VMS 2.3 installation process. (When you install VMS 2.3, by default, checkboxes for several VMS products on the "Select Components" install screen are selected. You should click the **Deselect** button. Then select the **Common Services** checkbox and click **Next** to continue.)

Step 5 Complete the VMS 2.3 installation by rebooting your system when prompted.

How to install CSA MC V5.0:

Note The Management Center for Cisco Security Agents V5.0 kit is signed by Cisco Systems. This can be verified using Windows Explorer File ->Properties ->Digital Signatures.

Step 1 Open a command prompt window and cd into the product directory. Run **setup.exe**. Alternatively, you can use Windows Explorer to navigate to the product directory. Then, double-click the setup.exe file to begin the installation.

Step 2 You can now follow the standard installation directions provided in the Installation Guide. The Installation Guide appears as a PDF file in the Documentation directory at the top level.

Note The agent kits are provided in test mode in order to minimize any possible adverse impact of initial agent installation.

The provided policies are meant as a starting point to enterprise security. In general, you will want to run in test mode and create exceptions with the event

wizard to create a suitable rule set for your environment. At that point, you can remove your agents from the test mode group and allow them to operate in protect mode. Test mode is turned on in the **Auto-enrollment** groups for each OS type. From the **Group** page, expand the **Rule overrides** section and uncheck the **Test mode** checkbox to turn test mode off for that group. Then **Generate rules**.

Product Notes

The following are issues that exist with the product, but are not product bugs. Therefore, they are not in the bug list.

- **Issue:** When you install CSA MC 5.0 on the same system where a previous version of CSA MC is installed and then you uninstall the newer 5.0 version, the protecting system agent is also uninstalled. This leaves the previous, existing CSA MC without an agent.

  Solution: It is recommended that you install an agent on this CSA MC system.

- **Issue:** If you have performed a single system upgrade from CSA MC 4.0.x to CSA MC 5.0, and you select to backup your database when you then uninstall CSA MC 4.0.x, you may see an error in the uninstall log referring to the “Profiler” database. Because the name of this database is changed during the upgrade process, the backup program, will not be able to locate it.

  Solution: The majority of the backup does succeed despite the message that appears about the profiler database. There is no solution at this time.

- **Issue**: The default Unix policy having to with rpatch or package installation and system management may cause the following issue. Some package or patch installations will attempt to write to agent-protected system files and will, by default, will be denied.

  Solution: Administrators can perform maintenance, configuration or installation of packages using one of the following methods:

  1. Locally in a trusted session such as Single User mode (init level 1) on Solaris or from a VTY session (Ctrl-Alt-F1) on Linux.
  2. Remotely via SSH from a trusted host. In this case, the trusted host's IP address must be added to the list of trusted hosts on CSA MC.
  3. Local Login via serial port.

- **Issue**: In some environments, the shipped installation policy may not allow non-standard installations. It is recommended that you tune the policy accordingly or stop the agent service to allow the installation.

  Solution: You may change the File access control rule from the previous version of CSA MC in this module to query the user if your security policy permits the use of the application in question.

- **Issue**: The pre-built reports configured for Analysis Deployment Investigation are meant as samples. You will likely have to edit or add to the existing report configurations to gather comprehensive information.

- **Issue**: Linux Agent UI: For gnome desktop environments, the install script will only modify the default session config file for launching the agent UI automatically every time a user starts a gnome desktop session. But if a user already has their own session file (~/.gnome2/session), the default session file (/usr/share/gnome/default.session) will not be effective. Therefore, the agent UI will not automatically start when the user logs in. In such a case, the user must add the agent UI (/opt/CSCOsca/bin/ciscosecui) manually (using "gnome-session-properties" utility) to make the agent UI auto-start. The user may also need to add a panel notification area applet to the control panel.

- **Issue**: Data access control rules for iPlanet running on Solaris systems are untested and unsupported. CSA ships with a data filter that you must manually install to use Data access control rules for iPlanet applications on Solaris. If you use this functionality, be aware that it is unsupported and that this filter may be removed in a future release.

- **Issue**: There have been issues with Compaq/HP Teaming and the Cisco Security agent (CSA). Symptoms include the NICs not being enabled automatically after an agent installation. This has to do with issues between Compaq/HP Teaming software and the agent's network shim. This is an example of the behavior: Installing CSA on an HP DL380G2 server with an HP-NC3163 Ethernet card disables the ethernet card. After CSA is installed, and before the PC is rebooted to complete the installation, the ethernet adapter is disabled.

  Solutions: There are several different solutions to this issue:

  - Do not install the network shim; it is an optional product.
  - Reboot the system immediately after CSA is installed.

- Dissolve the team before installing CSA. Then, re-create the team after CSA has been installed.

  There may be other issues between CSA's network shim and Compaq/HP Teaming and thus we highly recommend dissolving the team prior to installing CSA if you plan to install the network shim.

– **Issue**: The “Desktop interface applications, client HTTP protocol” rule in the Windows System Hardening module prevents Windows Find Files/Folders functionality from accessing sa.windows.com. When the rule is applied, the event text reads like this:

  “The process 'C:\WINDOWS\explorer.exe' (as user HostName\Administrator) attempted to communicate with 10.123.124.125 on TCP port 80. The attempted access was to initiate a connection as a client (operation = CONNECT). The operation was denied.” The Windows search function is vulnerable to a redirection attack and the rule is designed to prevent just such an attack.

– **Issue**: If the Local File Protection feature of the Cisco Security Agent UI is modified, the protection enforced continues to be enforced on previously opened files.

  Solution: Note that once a File has been opened and marked as protected, that instance of the file will remain protected even if you remove it from the File Lock list. Only unchecking the enable box on the agent turns off the File Lock entirely. You can then re-enable the File Lock to continue to protect other files on the list.

New Features

This release contains the following new features:

Action Name Changes

Although the functionality and general precedence of action types has not changed, the names have been altered. The “High priority” actions are now named “Priority”.

CTA 2.0 Plug-in Support

The CTA 2.0 plug-in to support NAC Phase 2 is packaged with the Cisco Security Agent for optional deployment in this release.

Differentiated Service

By using the Set action available from certain rule types, you can specify Differentiated Service for a traffic flow by setting a QoS marking which is a recognizable value in an IP packet. This allows routers and switches to identify and take action on QoS-marked traffic, providing finer granularity of control in forwarding traffic.

Detected Access Protection

By using the Set action available from certain rule types, you can configure the MC to notify you (via the event log) and optionally take action (via a system state) when an application or service, or other system component that is marked as “detected access” Unprotected does not have a corresponding “detected access” Protected rule and is therefore not being protected by the agent.

Event Aggregation and Suppression

When first deploying rules to agents, it is not unusual to have an overwhelming flurry of events appearing in the event log. In some cases, most of these events are similar events or simply "noisy", not useful events to view. If this is the case, the event log provides two mechanisms for paring down the number of events that appear. *Event Filtering*: When event filtering is enabled, the event log displays an aggregation of events. This aggregation means that one representative event is displayed for all events that are considered similar on the MC. *Event Suppression*: When event suppression is enabled, all chosen events are no longer displayed in the event log. Event suppression is best used when you have a reoccurring event that is more noisy than useful to you.

Host Managing Tasks

The configuration options on this new page let you add, move, and remove hosts from selected groups at set times so that the action occurs automatically. Using a configured, automatic, management task could be useful in various recommended scenarios. For example, you’re conducting a pilot of the product and you want all newly registered hosts to remain in a group that has test mode enabled for certain period of time before those hosts move to a group that is not in test mode. Having this group movement occur automatically can reduce the administrative burden of having to manually do this. Especially, if it is your policy to have all new hosts start off in test mode. This same scenario can also applied to the learn mode feature.

Host Operations Box

From the Hosts Search page, you can perform certain operations on found hosts. When you the click the Operations button from the Hosts Search page, a new pop-up window appears from which you can move a host to the recycle bin, attach/detach a host from a group.

Hosts Recycle Bin

A recycle bin window is now available from the Hosts list page. To manually move hosts to the recycle bin, you must select the checkbox beside the host in question and click the Move to Recycle Bin button. This is how you remove an inactive or irrelevant host from the Hosts list. If you do not perform this task manually, as mentioned earlier, hosts that have been inactive for 30 days are automatically moved the recycle bin.

IP Address Quarantining

Addresses can be added to the quarantine list by using the Set action - Host address - Untrusted - locally or globally - in a System API rule type.

Learn Mode

Learn mode is intended to localize policies on individual systems, eliminating the initial flurry of pop-up queries that users may experience when the agent is first installed on a system. The learn mode feature should be enabled for a temporary period of time. Learn mode directs the agent not to display query pop-ups, and to instead take an immediate *Allow* query response when a query rule is triggered, and to persistently save the allow response. Once query responses are taken, and Learn mode is turned off, the majority of queries no longer appear and system security provided by the agent is normalized to the individual system. At this point, users should only see query pop-ups for unusual or suspicious system behavior.

Network Access Control Rules take Source Ports into Account

This is useful when the destination port is ephemerally allocated, but the source port is a well-known port. For example, most network connections are keyed off of well-known destination ports. Applications that only have well-known source ports, such a multimedia applications or Active FTP data connections, must be controlled off the source port. Therefore, if you are specifying a differentiated service marking for a multimedia connection, you would key off the source port.

Platform Support

In this V5.0 release, there is now agent support for the following platforms: Solaris 9, Windows XP Tablet PC Edition 2005, VMware.

Query Logging Granularity

In addition to deciding which query actions (Allow, Deny, Terminate) are available to the user for query pop-up, you can also configure the query response to log only when a particular query action is selected by the user. Using the multi-select box available from the Logged query responses section, you can select one or more response types to produce a log message. For example, if all query actions are being made available for the query, you can configure only a Terminate response to produce a log message. (By default, all query responses are logged.)

Reset Options Added

The MC lets you centrally reset agent settings back to their original states and clears all user-configured settings. When you click the Reset Cisco Security Agents link, a pop-up window appears displaying various checkboxes that let you to reset various specific agents settings or to reset all settings. You can reset the following agent settings: Cached Responses and Logging, Local Firewall Settings, Learned Information, System Security, System State, Untrusted Applications, and User Query Responses.

Secure Boot Mode

Use the Set detected boot attribute to detect when a previous system boot occurred in a non-standard manner. For example, the system was booted from a peripheral device (CD ROM) rather than from the hard drive. This type of boot can be considered non-standard and therefore possibly suspicious. (This is one way of introducing a Trojan to a system.) This type of peripheral device insecure boot detection works in conjunction with a particular type of compatible BIOS on compliant systems.

Note At this time, the following systems have a BIOS that is compatible with the Secure Boot Mode feature: ThinkCentre (R) M52 Desktop PCs by Lenovo (tm).

Set Action

A Set action is available for certain rule types. Set is a singular configuration action that causes a particular, one-time, configuration item to occur when the criteria configured in the rule triggers on a system. For example, when a rule with “Set” configured triggers, a specific action occurs, such as the security level being set to low.

The Set action functionality is now used to perform some of the Add/Remove built-in application process tagging that was available in previous releases. The following built-in applications that were available in previous releases have been removed for V5.0 and although the functionality is the same, they are now implemented using the Set function: Authorized rootkit, Unauthorized rootkit, Processes communicating with Untrusted Hosts, Processes requiring Security Level <High, Medium, Low>, Processes Copying Untrusted Content, Processes Writing Untrusted Content.

You use Set in a rule to perform the following one-time actions: detected access, detected boot, detected rootkit, Differentiated Service (QoS), file trust markings, and host address trust markings. See the User Guide for details.

Status Summary - Host History

There is one item in the Network Status section that is configurable. *Host history collection* is a feature that you enable and disable from this page. You optionally, globally enable Host history collection for all hosts if you want to maintain individual host histories of the following types of information: host registration, test mode setting changes, learn mode setting changes, IP address changes, CTA posture changes, CSA version changes, host active/inactive status changes.

Status Summary - Most Active

Use the links available in the Most Active section to view the Hosts, Rules, Applications, or Rule/Application pairs that have been the most active or triggered the most (logged the most events to the MC). This information is useful to help you tune your policies for rules that are being tripped too often. This can also alert you to common unwanted occurrences that may be triggering across your enterprise. Additionally, you can purge the events that appear in these lists.

Third Party Certificates

Third party certificates have been qualified with CSA MC.

Wizard Changes

You can use the Wizard to suppress an event from the event log. (This is one way to make use of the new Event Aggregation and Suppression feature.) Event suppression is configured using the Rule ID of the event and the application (including file path) as the criteria for suppressing the event in question and all similar events.

System Requirements (CSA MC)

CSA MC is a component of the VPN/Security Management Solution (VMS).

For information on all bundle features and their requirements, see *CiscoWorks2000 VPN/Security Management Solution Quick Start Guide*.

Table 1 shows the minimum VMS bundle server requirements for Windows 2000 systems. These requirements are sufficient if you are running a pilot of the product or for deployments up to 500 agents. If you are planning to deploy CSA MC with more than 500 agents, these requirements are insufficient. See the Installation Guide for more detailed system requirements.

Table 1 Minimum Server Requirements

System Component	Requirement
Hardware	• IBM PC-compatible computer • Color monitor with video card capable of 16-bit
Processor	1 GHz or faster Pentium processor
Operating System	Windows 2000 Server or Advanced Server (Service Pack 4) **Note** Terminal services are not supported on Server and Advanced Server running CSA MC.
File System	NTFS
Memory	1 GB minimum memory
Virtual Memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space **Note** The actual amount of hard drive space required depends upon the number of CiscoWorks Common Services client applications you are installing and the number of devices you are managing with the client applications.

- Pager alerts require a Hayes Compatible Modem.
- For optimal viewing of the CSA MC UI, you should set your display to a resolution of 1024 x 768 or higher.
- On a system where CSA MC has never been installed, the CSA MC setup program first installs MSDE with Service Pack 3a. If the CSA MC installation detects any other database type attached to an existing installation of MSDE, the installation will abort. This database configuration is not supported.
- If MSDE Service Pack 2 or earlier is present on the system, you must uninstall that version of MSDE or upgrade it before proceeding further.

SQL Server Desktop Engine Installation

As part of the installation process on a system where CSA MC has not previously been installed, the setup program first installs Microsoft SQL Server Desktop Engine (MSDE). You can use the included Microsoft SQL Server Desktop Engine (provided with the product) if you are planning to deploy no more than 500 agents. When the MSDE installation completes, it may prompt you to reboot the system. In that case, you must reboot the system before restarting the CSA MC setup program. If the MSDE installation does not prompt you to reboot the system, you may restart the setup program without rebooting the system.

Caution If the CSA MC installation detects any other database type attached to an existing installation of MSDE, the CSA MC installation will abort. This database configuration is not supported by Cisco. (Installation process aborts if any databases other than those listed here are found: master, tempdb, model, msdb, pubs, Northwind, profiler and AnalyzerLog.)

For a local database configuration, you also have the option of installing Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Desktop Engine that is provided. Microsoft SQL Server Desktop Engine has a 2 GB limit. In this case, you can have CSA MC and Microsoft SQL Server 2000 on the same system if you are planning to deploy no more than 5,000 agents. Note that of you are using SQL Server 2000, it must be licensed separately and it must be installed on the system before you begin the CSA MC installation. (See the *Installation Guide* for details on installation options.)

We also recommend that you format the disk to which you are installing CSA MC as NTFS. FAT32 limits all file sizes to 4 GB.

System Requirements (Agent)

To run Cisco Security Agent on your Windows XP, Windows Server 2003, Windows 2000 or Windows NT 4.0 servers and desktop systems, the requirements are as follows:

Table 2 Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher **Note** Up to eight physical processors are supported.
Operating Systems	• Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0 or 1 • Windows XP (Professional, Tablet PC Edition 2005, or Home Edition) Service Pack 0, 1, or 2 • Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4 • Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a **Note** Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000. (Terminal Services are not supported on Windows NT.) Supported language versions are as follows: • For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported. • For Windows NT, US English is the only supported language version.
Memory	128 MB minimum—all supported Windows platforms

System Component	Requirement
Hard Drive Space	25 MB or higher **Note** This includes program and data.
Network	Ethernet or Dial up **Note** Maximum of 64 IP addresses supported on a system.

Note Cisco Security Agent uses approximately 30 MB of memory. This applies to agents running on all supported Microsoft and UNIX platforms.

To run Cisco Security Agent on your Solaris server systems, the requirements are as follows:

Table 3 Agent Requirements (Solaris)

System Component	Requirement
Processor	UltraSPARC 400 MHz or higher **Note** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	Solaris 9, 64 bit, patch version 111711-11 or higher, and 111712-11 or higher installed. Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.) **Note** If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disc (1 of 2) in the /Solaris_8/Product directory. Install using the **pkgadd -d . SUNWlibCx** command.
Memory	256 MB minimum
Hard Drive Space	25 MB or higher **Note** This includes program and data.
Network	Ethernet **Note** Maximum of 64 IP addresses supported on a system.

Caution On Solaris systems running Cisco Security Agents, if you add a new type of Ethernet interface to the system, you must reboot that system twice for the agent to detect it and apply rules to it accordingly.

To run the Cisco Security Agent on your Linux systems, the requirements are as follows:

Table 4 Agent Requirements (Linux)

System Component	Requirement
Processor	500 MHz or faster x86 processor (32 bits only) **Note** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	RedHat Enterprise Linux 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	25 MB or higher **Note** This includes program and data.
Network	Ethernet **Note** Maximum of 64 IP addresses supported on a system.

Upgrade Support

Upgrading CSA versions earlier than Cisco Security Agent V4.X is not supported.

See “Installing Management Center for Cisco Security Agents” provided as a PDF file in Documentation directory on the product CD for product installation instructions.

Duplicate Configuration Naming Convention

Configuration items shipped with CSA MC and provided by Cisco contain a version column with a version number. Administrator-created items have no version number.

When you import configuration items provided by Cisco, if it is found that there is already an existing exact match for an item, the new configuration data is not copied over. Instead, the existing item will be reused and the name will reflect the new versioning.

If the import process finds that there is an existing item with the same name, the same version number, and different configuration components (variables, etc.), the newly imported item is changed by appending the name of the export file. The new item is always the item that the export file name appended to it. Existing items are not renamed or reversioned if there is a collision.

Also note that CSA MC automatically appends the name of the export file to any administrator configured item collision it finds during administrator imports. The imported item is given a different name and both new and old items can co-exist in the database.

Internationalization Support

All Cisco Security Agent kits contain localized support for English, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish language desktops. This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system will appear in the language of the end user's desktop.

The following table lists CSA localized support and qualification for various OS types.

Table 5 CSA Localizations

Language	Operating System	Localized	Qualified
Chinese (Simplified)	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes

Language	Operating System	Localized	Qualified
French	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
German	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Italian	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Japanese	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Korean	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Spanish	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes

Explanation of terms:

Localized: Cisco Security Agent kits contain localized support for the languages identified in Table 5. This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system will appear in the language of the end user's desktop. All localized languages are agent qualified and supported. (CSA MC is not localized.)

Qualified: The Cisco Security Agent was tested on these language platforms. Cisco security agent drivers are able to handle the local characters in file paths and registry paths. All qualified languages are supported.

Supported: The Cisco Security Agent is suitable to run on these language platforms. The localized characters are supported by all agent functions.

Refer to the following tables.

Internationalization Support Tables

The following tables detail the level of support for each localized version of Windows operating systems. **Note that support for a localized operating system is different from localized agent.** A localized operating system may be supported even though the corresponding language is not translated in the agent. In this case, the dialogs will appear in English. The tables below define the operating system support, not agent language support. Note, for Multilingual User Interface (MUI) supported languages, installs are **always** in English (Install shield does not support MUI), and the UI/dialogs are in English unless the desktop is Chinese (Simplified), French, German, Italian, Japanese, Korean, or Spanish.

Any Windows 2000, Windows XP or Windows 2003 platforms/versions not mentioned in the tables below should be treated as not supported.

The following letter combinations are used to describe the level of support:

Table 6 Support Level Key

L	Agent localized, supported and qualified. (**Note:** L(S) – Localized and supported only)
T	Supported and qualified.
S	Supported but not qualified – Bugs will be fixed when reported by customers, but the exact configuration was not tested.
NA	Not applicable – Microsoft does not ship this combination.
NS	Not supported.

Table 7 Windows 2000 Support

	Professional	Server	Advanced Server
MUI	T	S	S
Arabic	NS	NA	NA
Chinese (Simplified)	L	L(S)	L(S)

	Professional	Server	Advanced Server
Chinese (Traditional)	T	S	S
Czech	S	S	NA
Danish	T	NA	NA
Dutch	S	S	NA
English	L	L	L
Finnish	S	NA	NA
French	L	L(S)	L(S)
German	L	L(S)	L(S)
Greek	S	NA	NA
Hebrew	NS	NA	NA
Hungarian	S	S	NA
Italian	L	L(S)	NA
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)
Norwegian	S	NA	NA
Polish	S	S	NA
Portuguese	T	T	NA
Russian	S	S	NA
Spanish	L	L(S)	L(S)
Swedish	S	S	NA
Turkish	S	S	NA

Table 8 Windows XP Support

	Professional	Home
Arabic	NS	NS
Chinese (Simplified)	L	L(S)
Chinese (Traditional)	T	S

	Professional	Home
Chinese (Hong Kong)	S	S
Czech	S	S
Danish	T	S
Dutch	S	S
English	L	L
Finnish	S	S
French	L	L(S)
German	L	L(S)
Greek	S	S
Hebrew	NS	NS
Hungarian	S	S
Italian	L	L(S)
Japanese	L	L(S)
Korean	L	L(S)
Norwegian	S	S
Polish	T	T
Portuguese	S	S
Russian	S	S
Spanish	L	L(S)
Swedish	S	S
Turkish	S	S

Table 9 Windows 2003 Support

	Standard	Web	Enterprise
Chinese (Simplified)	L	L(S)	L(S)
Chinese (Traditional)	T	S	S
Chinese (Hong Kong)	S	S	S
Czech	S	S	S

	Standard	Web	Enterprise
Dutch	S	NA	NA
English	L	L	L
French	L	L(S)	L(S)
German	L	L(S)	L(S)
Hungarian	S	S	S
Italian	L	L(S)	L(S)
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)
Polish	T	T	T
Portuguese	S	S	S
Russian	S	S	S
Spanish	L	L(S)	L(S)
Swedish	S	S	S
Turkish	S	S	S

On non-localized but tested and supported language platforms, the administrator is responsible for policy changes arising from directory naming variations between languages.

If the previous operating system tables do not indicate that CSA is localized (L), then the system administrator is responsible for checking to ensure that the tokens are in the language they expect and the directory path is the one they intend to protect. See *Installing Management Center for Cisco Security Agents* for the procedure to determine if language tokens are correct. Also note that if you are upgrading to V5.0 from a version earlier than 4.5, and you are carrying policies forward, you will want to change literal string system path references to token paths for localization purposes.

VMware Environment Support

The following tables provide support details for the Cisco Security Agents running in a VMware environment for host and guest operating systems.

Table 10 VMware Support Overview

VMware Product	Host Operating System	Guest Operating System	Supported
VMware WS 5.0 (workstation)	Various	All agent supported operating systems	Yes
VMware GSX 3.2 (enterprise)	Various	All agent supported operating systems	Yes
VMware ESX 2.5 (workstation)	N/A	not supported	No

Note that the table above assumes that the VMware virtualization layer between the guest operating system and the host operating system isolates it from underlying differences. The following tables list the specific host and guest operating systems that this capability is qualified on. While other operating systems may work, only those listed here have been verified.

Table 11 VMware WS 5.0 Host OS Support

VMware WS 5.0	Host OS (US English Only)
	Windows 2000 Professional/Server/Advanced Server SP4
	Windows 2003 Server/Enterprise Server/Web Edition SP1
	Windows XP Professional/Home Edition SP2
	Windows 2003 Server 64 bit SP1 *CSA protection not supported
	Windows XP Professional 64 bit SP0 *CSA protection not supported
	Red Hat AS/ES/WS 3.0

Table 12 VMware WS 5.0 Guest OS Support

VMware WS 5.0	Guest OS (US English Only)
	Windows NT 4.0 Workstation/Server SP6a
	Windows 2000 Professional/Server/Advanced Server SP4
	Windows 2003 Server/Enterprise Server/Web Edition/Small Business Server SP1
	Windows XP Professional/Home Edition SP2
	Red Hat AS/ES/WS 3.0

Table 13 VMware GSX 3.2 Host OS Support

VMware GSX 3.2	Host OS (US English Only)
	Windows 2000 Server/Advanced Server SP4
	Windows 2003 Server/Enterprise Server/Web Edition SP1
	Windows 2003 Server/Enterprise Server 64 bit SP1 *CSA protection not supported
	Red Hat AS/ES/WS 3.0

Table 14 VMware GSX 3.2 Guest OS Support

VMware GSX 3.2	Guest OS (US English Only)
	Windows NT 4.0 Workstation/Server SP6a
	Windows 2000 Professional/Server/Advanced Server SP4
	Windows 2003 Server/Enterprise Server/Web Edition/Small Business Server SP1
	Windows XP Professional/Home Edition SP2
	Red Hat AS/ES/WS 3.0

Windows Firewall Disabled

The Cisco Security Agent automatically disables the Windows XP and Windows 2003 firewall. This is done per recommendation of Microsoft in their HELP guide for their firewall. If you want to read this recommendation, you can access the "Windows Security Center" console from a Windows XP or Windows 2003 installation, click on "Windows Firewall", and select "on." The firewall status will warn you as follows: "Two or more firewalls running at the same time can conflict with each other. For more information see Why you should only use one firewall."

Because the Cisco Security Agent, in part, utilizes firewall-like components, the agent disables the Windows firewall per the recommendation from Microsoft.

Cisco Security Agent Policies

CSA MC default agent kits, groups, policies, rule modules, and configuration variables provide a high level of security coverage for desktops and servers. These default agent kits, groups, policies, rule modules, and configuration variables cannot anticipate all possible local security policy requirements specified by your organization's management, nor can they anticipate all local combinations of application usage patterns. We recommend deploying agents using the default configurations and then monitoring for possible tuning to your environment.

CSA MC Local Agent and Policies

When you install CSA MC, an agent containing the policies necessary to protect a system only running CSA MC and Security Monitor as part of your VMS bundle on the CiscoWorks system (the recommended configuration) is automatically installed as well. The policy in question contains a “restrictive” rule module which puts tighter restrictions on the system because it does not have to account for other VMS bundle products that might be running on the system.

If you are running additional products as part of your VMS bundle on the CiscoWorks system, you must remove the CiscoWorks Restrictive VMS Module from the CiscoWorks VMS Systems policy in order to allow this additional software to operate.

To do this, navigate to **Configuration>Policies** and locate “VMS CiscoWorks - Windows” in the list of policies. Click on the “VMS CiscoWorks - Windows” policy. This takes you to the main policy page with the list of rule module associations. Click the **Modify rule module associations** link. Locate the “CiscoWorks Restrictive VMS Module” in the right-side Attached rule modules swap box. Select this module and click the **Remove** button. Then **Generate rules**. (Note that this is not the recommended deployment.)

Caution If you are installing or uninstalling various VMS components, and you have a Cisco Security Agent protecting the VMS bundle, you should disable the agent service before you install or uninstall of any other VMS component. (You do not have to do this when installing or uninstalling CSA MC.) To disable the agent service, from a command prompt type: net stop “Cisco Security Agent”. (You may receive a prompt asking if you want to stop the agent service. You should click Yes.) To enable the service, type: net start “Cisco Security Agent”.

If you do not disable the agent service and you attempt to alter a CiscoWorks system configuration, the agent may disallow the action or it may display multiple queries to which you must respond.

RME Gatekeeper Remote Access Issue

It is recommended that you do not install other VMS products on the system to which are installing Management Center for Cisco Security Agents. However, if you do not follow this recommendation, you should be aware of the following.

Remote access to the CiscoWorks RME Gatekeeper daemon is not required for correct operation of any of the components in the VMS bundle. Therefore, remote client access to this daemon is normally disabled through a deny rule in the "CiscoWorks VMS Module" within the CiscoWorks VMS Policy.

If other products that require the RME Gatekeeper daemon to be accessed remotely, such as Campus Manager or ACLM, are installed on the same system as the VMS bundle, the CSAMC "CiscoWorks VMS Module" protecting the VMS system should be modified as follows:

Step 1 Login to CSAMC and navigate to the "CiscoWorks VMS Module" in the VMS CiscoWorks Policy. The module is accessible from **Configuration>Rule Modules [Windows]** in the menu bar.

Step 2 Once you locate the module, you don't have to click on the module name. You can click the **<#> rules** link to access the rules list directly.

Step 3 From the "CiscoWorks VMS Module" rule list, change the Allow rule "CiscoWorks RME Gatekeeper daemon, server for TCP and UDP services" from Disabled to Enabled. (Select the checkbox beside the rule and click the Enable button in the footer frame of CSAMC. Remember to save your changes.)

Step 4 Generate rules.

Step 5 Optionally, force polling on the agent to download the rule change.

Cisco VPN Client Support

Cisco Security Agent is a supported configuration for the "Are You There?" feature of the Cisco VPN Client, Release 4.0. For configuration details, please refer to Chapter 1 of the *Cisco VPN Client Administrator Guide*, in the section entitled "Configuring VPN Client Firewall Policy—Windows Only."

Known Issues

Table 15 provides information on known issues found in this release.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCec61813	CSAMC authentication fails when spawned from explorer.exe	**Symptom**:The Cisco Security Agent Management Console is typically accessed through a web browser. In the case of Internet Explorer, one can place a URL string in the address bar of the Windows file explorer and it will start to act like a limited functionality browser. **Conditions**:Administrator performing maintenance tasks on CSA MC. **Workaround**:Do not invoke a session to browse to an external site such as CSA MC. A supported web browser must be used. Consult the Installation Guide for these requirements.
CSCed17183	Cannot view ActiveX reports without using fully qualified CSA MC name	**Symptom**:Browsing to CSA MC without using the "full" MC name (e.g. "machine" instead of "machine.mycompany.com") will result in the inability to view ActiveX reports on the MC. **Workaround**:For proper viewing of CSA MC ActiveX reports, make sure to use the fully qualified name when browsing to the MC.
CSCef16814	Unix non-root users should have access to UI	**Symptom**:Currently non-root users on Solaris do not have access to the agent ./csactl utility. Therefore they cannot poll for new rules or perform software updates. **Workaround**: None at this time. Polls will continue to occur at regular intervals determined by the group parameter for polling.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCef17103	CSA and AFS (Andrew File System) are incompatible on Solaris 2.8.	**Symptom**: It has been reported that the AFS (Andrew File System) is not compatible with the Cisco Security Agent on Solaris 2.8. **Workaround**: None at this time.
CSCef22643	Request to have CSA alerts include the parent process with the child process.	**Symptom**: When a descendent of a process is blocked, it would be useful to also list the parent process in the alert. For example, if one program is prevented from writing executable files and it is a dependent of another program, the alert displays the child program but does not mention the parent process. This makes the alerts harder to understand. **Workaround**: None at this time.
CSCef38271	Unicode characters are not supported for CSA MC reports.	**Symptom**:Because CSA MC generated reports do not support Unicode characters, some report fields (e.g. filename) may contain nonsense characters on internationalized versions of CSA. **Workaround**:There is no known workaround.
CSCef69413	ASC query is displayed in the wrong session.	**Symptom**:When running in a multiple display environment (Terminal Services or Citrix), the Cisco Security Agent makes every attempt to locate the user triggering the security query and display the query dialog in the session the local user in. **Workaround**: None at this time.
CSCef96134	Behavior analysis creates incorrect rule modules at times.	**Symptom:**Behavior analysis creates incorrect rule module when file/data streams are used. **Workaround**: Run the Behavior analysis job but manually delete all data/file stream references (the colon and all information after it).
CSCeg30323	Analysis reports do not detect outlook express and media player.	**Symptom**:Application Analysis fails to report windows components such as Outlook Express and Mediaplayer unless they are patched. **Workaround**:None at this time.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCeg56326	Test mode does not apply to the service restart rule.	**Symptom**:Service restart rules do not switch to TESTMODE. TESTMODE is the agent state where rules log "what would have happened" but do not enforce any policies on the system. The Service restart rule will restart the service it was monitoring regardless of the agent state. **Workaround**:None at this time.
CSCeg57681	Cannot navigate keyboard in Linux query challenge.	**Symptom**:Unable to navigate using only the keyboard as input on the Linux query challenge dialog. **Workaround**:Cisco Security Agent on Linux must use a pointer device (mouse, etc) to direct input in the Linux query challenge dialog.
CSCeg60208	False positive using Netmeeting directory on W2K.	**Symptom**:The use of NetMeeting in a domain environment produced certain events. These events are not due to malicious behavior on the part of NetMeeting. **Workaround**: It is advisable for the administrator to use the event wizard to tune the default desktop group's policies to allow NetMeeting to operate in the network environment.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCeg71633	Report engine design cannot support multiple administrators.	**Symptom**:Two administrators log into CSA MC from different systems and they both proceed to the same report (e.g.default report that is currently unmodified). The first administrator changes the parameters of the report and selects "View Report". The second administrator accesses the same report and selects "View Report". The second administrator believes he/she is viewing the default report. But this administrator is actually viewing the report that the first administrator is configuring despite the fact that the first administrator never "Saved" the changes. Further, there is no way to revert. **Workaround**:Exercise care in administering a system where more than one administrator could be running reports at one time.
CSCeg76282	There is no way to enable security if agent UI is not present.	**Symptom**:If the administrator disables the display of the agent UI after agent kits are deployed, there exists a rare condition that a host with security suspended during the disable of the UI display will not be able to restore the security level to the agent once the UI disappears. **Workaround**:There are two methods to correct this situation - Use the Reset feature from local host's Start menu - Or use the Reset feature from the CSA MC to remotely reset the agent.
CSCeg87069	Policies that ship with CSA MC for Linux interfere with automounter.	**Symptom**:Default Linux policies interfere with the operation of the automounter. **Workaround**:A workaround is to create exceptions for /usr/sbin/automounter from Buffer overflow rule terminate actions in the Linux policies.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCeg87071	Policies that ship with CSA MC for Linux interfere with RedHat RedCarpet Daemon.	**Symptom**:An optional Red Hat Linux utility that automatically patches the operating system - the Red Carpet daemon - when run in the presence of default Linux policies, generates events. **Workaround**:Use the wizard to tune the default policies to allow the Red Carpet daemon to run less noisily.
CSCeg88921	Newly installed COM objects are not protected by the agent until the system is rebooted.	**Symptom**: With an agent already installed and running on a Windows host, if a new MS Office application is installed, the COM objects it installs are not recognized by the agent and therefore are not protected by COM component access rules. **Workaround**: The system must be rebooted or the agent service stopped and restarted. At that time, the agent will register the new COM objects.
CSCeh25293	Uninstalling CSA turns on Windows XP firewall automatically	**Sympton**:Windows XP SP2 offers firewall functionality to those who install Service pack 2. The firewall is disabled but after installing and uninstalling CSA the firewall is automatically turned on. The state of the firewall should be the same as before you installed the agent. **Workaround**: After CSA uninstall completes, set the Windows Firewall to the appropriate state manually.
CSCeh29382	An agent running on Windows NT is unable to resolve MC hostname after upgrade.	**Symptom**:If DNS is not configured properly and the agent is installed on a Windows NT machine, the agent may not be able to resolve CSA MC properly. We require that CSA MC be resolvable via DNS or WINS but in some cases, the NT 6a system tries to resolved via netbios. **Workaround**:Make sure DNS is properly configured and the machine name of CSA MC can be resolved via DNS.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCeh31986	The Behavior analysis progress status for log file size does not work on Solaris.	**Symptom**:While your Application behavior analysis is in-progress, the progress status for log file size resets to zero. This happened to both Unix platforms (Solaris and Linux). **Workaround**:If your Application behavior analysis relies on log size as a criteria, there is no status available. Using other criteria, such as number of invocations, will provide progress status.
CSCeh35360	Network access control rules trigger incorrectly with alias IP address & same netmask.	**Symptom**:Network access control rules trigger incorrectly with alias IP addresses and similar netmask addresses(UNIX) in the presence of a Network access control rule specified to control connections on one of these local addresses. The agent may trigger an incorrect Network access control rule or no rule at all. This is because the TCP/IP layer doesn't report the local IP address on which the packet was received and the agent attempts to select a correct local IP address that matches the address specified in the rule. The agent selection logic may return an incorrect local IP address and thus apply a wrong rule or no rule at all. **Workaround**:None at this time.
CSCeh36870	The multimedia client rule module is not attached to a policy.	**Symptom**:The multimedia client rule module ship as “not attached” to a policy by default. **Workaround**:Attach the multimedia client rule module to the default desktop group policy if those particular rules are required.
CSCeh39645	The Network access control rule for Telnet takes the default action before the user can respond.	**Symptom**:Use of this rule type should be done after the administrator has carefully reviewed the documentation for the rule type. **Workaround**:Refer to the User's Guide - Page 4-71 - the second Note: on the page is of particular relevance.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCeh40327	A pop-up blocker prevents launching the Crystal Reports Viewer.	**Symptom**:When a "Pop-Up Blocker" is enabled in the browser administering CSA MC, there are a number of functions that will appear not to be functioning correctly. These include (but are not limited to): Display of reports, pop-up creation of objects such as Application classes, File sets, and, from within the context of configuring a rule, the quick help syntax. **Workaround**:Disable the "Pop-Up Blocker" on the browser when administering CSA MC.
CSCin88933	When upgrading to CSA MC 4.5, the import root certificate tab is seen twice.	**Symptom**:When upgrading to CSA MC 4.5 with CSAMC 4.0.x already installed, there are two entries for importing the root certificate. **Workaround**:The root certificate only needs to be imported once.
CSCok06488	CSA MC event report exporting fails for a large numbers of events.	**Symptom**:The generation of a CSA MC report, containing very large numbers of events, fails and produces only a truncated report. **Workaround**:When exporting event-based reports, keep the number of exported events to a manageable size.
CSCsa60422	Crystal Reports 8 cannot export to Excel 2003.	**Symptom**:Crystal Reports 8 can only be exported using Excel 5 (rft that support only 16,384 lines). If you export trying to use the xls format, the 16K line limit is imposed and the blank lines are inserted. **Workaround**:The only available work around is to export as rtf and import to Excel 2003.
CSCsa63154	When you Click the Purge log button on the agent GUI, events remain in the Messages window.	**Symptom**:The agent GUI does not clear events from the Messages display when the "Purge log" button is clicked. **Workaround**:One can exit the agent GUI and then restart the GUI via the Windows Start menu to clear the display.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCsb15517	CSA-MC does not provide any audit info to common services	**Symptom**: Common Services "Audit Log" is not updated by audit events from CSA-MC. **Workaround**: None at this time.
CSCsb14859	Application SpeedCommander aborts when CSA is installed	**Symptom**: When CSA is installed on a PC running the SpeedCommander application, the application will no longer function correctly. The SpeedCommander application aborts immediately after execution. **Workaround**: The workaround is to add the SpeedCommander program to the application class for "Processes requiring Kernel Only Protection".
CSCsc13217	CSA default policies do not support Webroot Spysweeper	**Symptom**: Webroot Spysweeper triggers buffer overflow rules in CSA Feature Request: Add CSA support for Webroot products such as Spysweeper. (Conditions: CSA 4.x and Webroot Spysweeper (www.webroot.com) **Workaround**: Create appropriate policy exceptions.
CSCsc04336	Many events occur where any application will attempt to inject code into a single target. Administrators cannot create an exception for this without the exception being too broad.	**Symptom**: The System API rule allows administrators to specify what source application is allowed to inject code. There is no second selection for the target application into which the code is injected. **Workaround**: None. This is considered additional functionality to be added in a future release.
CSCsc30216	@removable does not work in an application class	**Symptom**: @removable token does not work properly in the literal definition of a application class. **Workaround**: Use @removable in the file set definition.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCsc37818	ACK packet is not getting marked when the Solaris or Linux agent acts as a Server and the protocol is TCP.	**Symptom**: The ACK in question is not marked due to a timing issue. The local stack is acking receive traffic before the accept system call returns. CSA doesn't provision the QoS marking until the accept system call returns. **Workaround**: None. Subsequent packets in the stream will be marked and the stream will benefit from the QoS markings.
CSCsc40429	There is a repeatable system delay / non-responsiveness when accessing a file protected by a CSA File version rule.	**Symptom**: A circular logic exists when CSA is installed on a system with a virus scanner in a certain scenario. When the file is open, CSA traps the open and tries to read the file's version by opening the file itself. The CSA process that attempts to open the file is interrupted by the installed virus scanner. Which in turn looks like the original file open and the cycle begins again. Note that the virus scanner gives up after 16 attempts to scan the file and the system responsiveness returns. **Workaround**: Avoid using File Version rules on systems where virus scanners are deployed.

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCsb02296	CSA cannot distinguish a remote client accessing the registry as a read or a write operation	**Symptom**: If a Registry access control rule is used to control the registry access from a remote client, CSA cannot distinguish between a read operation and a write operation. CSA treats a remote client registry read operation as a remote client registry write operation. (Condition: This affects users running CSA V4.5.0.565 and deploying the Registry access control rules with remote Clients.) **Workaround**: None. This is considered addition functionality to be added in a future release.
CSC sc08032	Too many license files causes the CSA MC License information page to hang.	**Symptom**: Too many license files will hang the License Information page, returning an "Internal Server Error" to the user. Significant slowdown is seen around 100 license files. License files in addition to 100 results in a significant decrease in the ability to access the License page. **Workaround**: Consolidate the number of license files, making sure that none of the consolidated files is greater than 4KB in size.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order

documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help

solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the Table 15 provides information on known issues found in this release. section.