Release Notes for Management Center for Cisco Security Agents 4.5.1

Revision 1

These release notes are for use with Management Center for Cisco Security Agents (CSA MC) 4.5.1. The following information is provided:

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

Installation Information

This CSA 4.5.1 release is supported with VMS 2.3.

If you are upgrading from 4.x.x to 4.5.1 you already have VMS installed. If this is a new installation, 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 4.5.1. 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. (You should find that you have 410 files occupying about 650MB of space.)

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 V4.5.1:

Note The Management Center for Cisco Security Agents V4.5 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**: 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 in this module to query the user if your security policy permits the use of the application in question.

- **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**: Once a rootkit has been detected on a system, the rootkit system state is not removed until the system is rebooted.

  Solution: Reboot system to reset rootkit system state.
- **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**: 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.

New Features

This release contains the following new features:

Displaying Packet Information in Human-Readable Form

For any event that provides packet information as part of the event details, that packet information can be displayed in human-readable form provided that "Ethereal" software is installed on the same system as CSA MC.

See the User Guide for links to Ethereal and instructions on how to read packet information.

Internationalization and Localization for Windows Agents

The Cisco Security Agent now accepts and displays query text characters appropriately for the supported, selected language type. Supported languages are Chinese (Simplified), French, German, Italian, Japanese, Korean, and Spanish. It also displays events in non-ASCII characters so that internationalization of events is possible. See Internationalization Support, page 14 for details about language support.

Bulk Transfer of Hosts from Group to Group

This new feature allows you to search for all the hosts that meet a certain criteria and then act on the hosts found by that search. From the page displaying the search results you will be able to move or copy hosts from one group to another or delete hosts.

Update Groups Associated with Agent Kits

After an agent kit is made and deployed, new groups can be associated with the kit and existing groups can be removed from the kit.

One use for this feature is to prolong the life of installation images by requiring fewer changes to agent kits. For example, agent kits would most likely be deployed in test mode until all the rules, rule-modules, and policies are fine-tuned to meet the needs of your enterprise. An image installed on new desktops during the testing period would include an agent kit, which includes the Test Mode Systems group, which makes all other groups run in test mode.

Once the period of testing is over, the image deployed for new desktops would still include the Test Mode System group but it may no longer be needed because the rules and policies have been finalized and it is time to "go live" for some or all of your enterprise. This feature would allow you to remove the Test Mode System group from the agent kit that is currently included in the installation image for all desktops. When the agent on a new desktop registers with CSA MC for the first time, the Test Mode System group will be removed from the agent kit and the new desktop will not run in test mode.

Use Network Address Class Notation

You can now specify a range of IP addresses in network address sets using Network Address Class Notation. For example you can now specify a range using the syntax: `128.67.0.0/16`. This indicates the range of addresses:

`128.67.`**`0.0`** `- 128.67.`**`255.255`**

Cisco Trust Agent (CTA) Support

The Cisco Security Agent is a supported configuration for the Cisco Trust Agent feature for both CTA versions 1.0 and 2.0. For configuration details, please refer to the Cisco Trust Agent documentation.

CSA Supports the Distribution of a Wider Variety of CTA Installation Kits

After the installation of CSA MC you can copy additional CTA installer files to the system running CSA MC. When you create agent kits, you will be able to select from the different CTA installer kits. Some installer kits include the CTA supplicant, others do not.

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 VMS bundle server requirements for Windows 2000 systems.

Table 1 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

System Component	Requirement
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** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	• Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0 or 1 • Windows XP (Professional 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 • All Windows, Internet Explorer 4.0 or higher required. **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	15 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 20 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 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

System Component	Requirement
Hard Drive Space	15 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	Intel Pentium 500 MHz or higher **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	15 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 from versions earlier than Cisco Security Agent V4.0.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
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 (Installshield 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)
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	S	S	NA
Russian	S	S	NA
Spanish	L	L(S)	L(S)

	Professional	Server	Advanced Server
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
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	S	S
Portuguese	S	S
Russian	S	S
Spanish	L	L(S)

	Professional	Home
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
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	S	S	S
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 Agent, Revision 1 for the procedure to determine if language tokens are correct.

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.

Policy Changes from CSA 4.5 to CSA 4.5.1

Changes to rules in CSA 4.5.1 were made to increase security, be less restrictive, or be more efficient. After you upgrade from 4.5 to 4.5.1, look for evidence of a rule change in the rule module list page or policy list page in CSA MC. If a rule has changed you will see a 4.5.1 version of a rule module or policy alongside the rule modules and policies of previous versions.

You can easily compare the new policy to the old policy to see exactly what changed. See the "Using Security Management Center for Cisco Security Agent" manual for information about the Compare Tool.

Policies Changed for Security Reasons

Security changes were made to enforce stricter security where it was needed. These policies changed to provide greater security:

Cisco Trust Agent - Windows: One rule in the Network Admission Control Quarantine Module was changed so that it is now shipped as "disabled" rather than "enabled." The rule prevents all network access outside the system except by Cisco Trust Agent (CTA) and by anti-virus software. The rule protects networked assets but also prevents the local agent from being remediated. This rule was disabled, and not removed, because the rule could be used as a template for a rule which better suits your individual enterprise.

Microsoft SQL Server 2000 - Windows: Two rules were changed to provide proper access to .ndf files. So that Microsoft SQL Server 2000 could access its own .ndf file type, MS SQL Server Services and MS SQL user applications were explicitly allowed to read and write .ndf files. To prevent access to .ndf files from "vulnerable applications," these applications were explicitly denied write access to .ndf files.

Operating System - Base Permissions - Solaris: The System Hardening Module (Solaris) was changed to prevent a telnetted buffer overflow attack documented in the CERT (Computer Emergency Response Team) advisory, CA-2001-21.

Operating System - Base Protection - Solaris: The System Hardening Rule Module (Solaris) was changed to prevent known exploits against sadmin daemon. By default, the tool starts in a weak authentication mode and can be easily spoofed. The sadmin daemon is not necessary and the rule prevents it from being started.

MS Management Applications application class. A change to the MS Management Applications applications class changed rules in several policies. The application class was changed because it referred to any mmc.exe executable in any path. Now the application class references only the explicit path to mmc.exe. This change prevents Trojan Horse attacks. These policies were affected by this change:

- DHCP Servers - Windows
- DNS Servers - Windows
- Operating Systems - Base Permissions - Windows
- Web Server - Microsoft IIS - Windows
- Microsoft SQL Server 2000 - Windows

Policies Changed to Be Less Restrictive

Some changes were made to make rule modules and policies less restrictive. Often these changes were made by adding new rules, which allowed more behavior, to rule modules. These changes will help new customers during the pilot phase of CSA by reducing the number of denials that require investigation.

These policies were made less restrictive:

- Application Classification
- General Applications - Base Security - Windows
- General Applications - Multi-level Security - Windows
- Installation Applications - Solaris
- Installation Applications - Windows
- Operating System Base protection - Linux
- Web Server - Apache

Policies Changed for Efficiency Reasons

Efficiency changes were made by combining rules to reduce the overall number of rules, expanding application classes to include more commonly used text editors, and by enhancing rule descriptions. These changes do not change the security benefit of a rule.

These policies were made more efficient:

- E-mail Client - Basic Security - Windows
- E-mail Client - Multi Level Security - Windows
- Network Personal Firewall
- Operating System - Base Protection - Windows
- Web Browser - Linux
- Web Server - Apache

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 10 provides information on known issues found in this release.

Table 10 Known Issues in Cisco Security Agent 4.5

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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCed45830	CSA Certificate does not comply with RFC2396	**Symptom**:The Cisco Security Agent and the CSA Management Console share a certificate to insure trusted communication. It has been reported that the certificate does not "fully" comply with RFC 2396. **Workaround**:None at this time. It is considered an enhancement request to add support for third party certificates.
CSCee45283	There is no VMS policy for running VMS on Solaris.	**Symptom**:The Cisco Security Agent ships with a default policy to defend the VMS system that CSA MC is installed on. This policy is tuned to allow the normal operation of the CSA MC. VMS also supports running VMS components on Solaris systems. However, CSA MC does not run on a Solaris environment. **Conditions**:Customers with VMS installed on Solaris. **Workaround**:It is suggested that the Customer initially deploy the Solaris Servers kit in TESTMODE. This will allow the admin to tune the rules on this server without imposing unwarranted events from the Cisco Security Agent.
CSCee61396	Overlay agent install does not enable previously disabled csauser / shims.	**Symptom**:To solve specific customer issue, the CSA escalation team will, from time to time, ask the customer to disable various drivers in the CSA agent. This disable is not respected when the agent is upgraded from release to release. This will cause the previous issue to re-surface. **Conditions**:Agent upgrades occur. Previous resolved issue returns. **Workaround**:Manually re-apply the driver disable steps.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCee62597	The Solaris agent does not allow netbackup to backup agent files.	**Symptom**:Netbackup is not allowed to backup the agent files. **Workaround**:This situation is true of any backup application that attempts to archive the agent files and uses a "write flag" in their file operation. The workaround that has been presented to several customers is to configure the backup system not to archive the agent files. To enable the agent to permit the backup of its own files would be compromising the agent's built-in self protection.
CSCee82644	Detect agent UI disabled if uninstalling CSA MC	**Symptom**:If the Cisco Security Agent user interface is not present (not enabled for the user), then the user receives no popup query when attempting actions such as stopping the agent. **Workaround**:Warn user that the agent UI is disabled and they cannot stop the agent service if CSA MC is uninstalled. Or, you can enable the agent UI for the user. Then this issue does not arise.
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.
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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCef85937	Blue Bar for login screen on WinXP-sp2 corp IT image and SOE images	**Symptom**: After reboot, instead of a login screen, the user sees a blank screen with only a blue bar. This blue bar normally appears on the Windows logo screen, but instead of the logo screen, only the blue bar is displayed. This is indicative of the logon is being impeded by CSA. **Workaround**: It has been determined that this typically occurs on Windows XP systems with Service Pack 2 installed. The Cisco Security Agent engineering team has implemented a partial workaround that requires CSA v4.5.1. In CSA 4.5.1, the rules now control whether one of the Clipboard rule's hook is installed. If there are no Clipboard rules in effect, then this hook is not inserted during logon. This will resolve the blue bar problem in this case. In order to get the keyboard hook installed after adding a clipboard rule, you will need to reboot your system. Before the reboot, the PrtScrn key will not be hooked. And the user should be aware that after reboot with a clipboard rule, the system may again experience the blue bar issue. The Cisco Security Agent engineering team is continuing to trace the root of this issue.
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 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeg51694	For a forced reboot configuration, minutes and seconds are not translated.	**Symptom**:On the forced reboot message after installing an agent kit, it reads "5 minutes, 00 seconds" regardless of OS language type. **Workaround**:None at this time.
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 10 Known Issues in Cisco Security Agent 4.5

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.
CSCeg75348	Application control rule allows All applications in both application fields.	**Symptom**: Configuring an Application control rule allows "All Applications" to be selected for both application class fields. This results in the following warning: “Dangerous application class selection (might render the system unusable).” Although this warning does appear the user is still allowed to proceed and generate the rule. This could cause systems become inoperable. **Workaround**: Administrators should be aware of this condition and exercise care in creating an Application control rule that uses All applications in both fields.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
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.
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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeg90229	If the CTA installation fails, CSA refers to non existent CTA log file.	**Symptom**:The Cisco Trust Agent is optionally installed with the Cisco Security Agent on any Windows platform. On Windows NT, the CTA installer fails because it is not a supported platform. The error presented contains a path to a non-existent log file. **Workaround**:None at this time. Windows NT is an unsupported CTA platform. Windows NT is a supported CSA platform.
CSCeh03415	The agent requires stop/start to register after 3.2->4.0.3->4.5 upgrade.	**Symptom**:After Migrating from 3.2 to 4.0.3.760 and subsequently to version 4.5, the agent will not register properly with the MC. It requires a stop/start of the agent service in order to allow the agent to register. However, after registering, the agent is still not associated with any groups. **Workaround**:On the next poll or restart of the agent, it is allowed to register, as a NULL registration. Because of the NULL registration however, the administrator must then associate the agent with the desired groups in order for any rules to be enforced on the agent.
CSCeh06088	File access control Directory protection does not protect symlinks in path.	**Symptom**:If a File access control rule is created to deny <All applications> write directory actions upon a file literal whose path includes a symbolic link (/opt/sfw/bin/* for example, where /opt/sfw is a symbolic link to another directory) the symbolic link itself can still be renamed. **Workaround**:Protect the symbolic link itself by denying read/write permission to it literally. In the above example, the File access control rule would include the file literal "/opt/sfw".

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeh17492	File protection is still operative after the entry is deleted.	**Symptom**:If the local File protection feature on the agent is modified. The protection enforced takes a short period of time to synchronize the changes. **Workaround**:Waiting a short period of time will allow the change to register in the system.
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.
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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeh32788	Intermittently, logout and reboot causes a 30 second to 2 minute hang.	**Symptom**:An attempt to logout and restart the Linux machine will often result in a hang. **Workaround**:None at this time. It is best to wait for the system to recover to maintain system integrity.
CSCeh34232	Install as power user on W2k3 provides no failure feedback to user.	**Symptom**:When a non-administrator attempts to install a Cisco Security Agent kit, the installation will fail because administrator permissions are required. Agent kits can be created in silent or interactive modes. When an silent agent kit is installed by a non-administrator, it is silent and does not provide feedback to the screen. **Workaround**:Inspect the installation log created by the agent kit installer.
CSCeh35116	Microsoft AntiSpyware questions the CTA installer.	**Symptom**:Microsoft AntiSpyware Alert message appears as follows “An Unknown Windows Service Requires Approval.” Microsoft AntiSpyware has detected a Windows service trying to be added. This service is the Cisco Trust Agent (CTA). **Workaround**:This message, from the Microsoft AntiSpyware BETA, should be ignored.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
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.
CSCeh35616	An incorrect Network access control rule triggers when packets are sent to an alias IP address.	**Symptom**:When a single interface has several IP addresses assigned to it (e.g. alias IP addresses) and a Network access control rule is specified to control connections on one of these local addresses, the agent may fire an incorrect Network access control rule or no rule at all. This is because 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 which 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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeh37876	Turning off agent security is cached when this action should not be cached.	**Symptom**:When stopping the Cisco Security Agent service, the user must successfully answer a query challenge dialog. When the user then repeats this shutdown of the agent within a short time period after the last attempt, the previous response is cached and the cached result will be acted upon. In the negative case, the user will experience some level of frustration as the query challenge dialog will not be displayed for them to "try again". **Workaround**:Use the "Clear" action on the Cisco Security Agent GUI to clear the cached response.
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.
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.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCok05577	There is no removable media support for Solaris platforms.	**Symptom**:The specification of tokens such as @removable, @floppy, and @CD does not function correctly on the Solaris platforms. **Workaround**:None at this time.
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.
CSCsa71629	CSA MC host diagnostics output indicates that it cannot display all the diagnostic information available.	**Symptom**: At the end of the host diagnostics output, there is a statement that says that there is too much information to display. **Workaround**: We have doubled the amount of information that can be displayed. However there is still a limit to the amount of information that can be displayed and the administrator should be aware this message may appear. There is no additional workaround at this time.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeg69427	Turning security to Off from the agent UI does not disable the network shim.	**Symptom**:If the user turns security to Off from the agent UI and the host then receives malicious network traffic that is typically intercepted by the Network shield rule, the agent continues to prevent the network traffic. **Workaround**:To turn off all security, including the network shim, you must "net stop" the csagent service. Only administrators can do this.
CSCeh10008	CSA MC 4.5 to 4.5 upgrade does not upgrade auto-enrollment groups.	**Symptom**:The auto-enrollment group does not upgrade to the latest policies when upgrading the CSA MC. This works as designed but it should be noted that after the CSA MC upgrade, the auto-enrollment groups (i.e. <All Windows>) will continue to contain the old policies from the previous CSA MC 4.5 installation. **Workaround**:To upgrade policies for the auto-enrollment group. you must manually remove the old policies from the relevant auto-enrollment group and add the new policies contained in the versioned upgraded group (i.e. ALL Windows-v.4.5.0.557). The upgrade works this way so that any custom policies that have been added to the <All Windows> group will not be replaced or removed. Use the compare function to determine content differences. The compare function also provides the ability to add and remove compared content in a single screen.

Table 10 Known Issues in Cisco Security Agent 4.5

Bug ID	Summary	Explanation
CSCeh29189	Some items remain hidden when the "Always use Show All mode" Admin preference is selected.	**Symptom**:Some items marked as visible only in "Show All" mode are not displayed in the list page unless you select the right click "Show All" menu option. The Show all option from the select box is not related to the Admin preference of "Show All" mode. **Workaround**: Right click on the page in question and select Show all mode to ensure all items are displayed.
CSCsb14982	Redhat Linux: If /etc/issue file is modified then CSA reports that the platform is unsupported.	**Environment: CSA** 4.5.0.565 with Redhat Linux AS3 **Symptom**: If first line of /etc/issue file is modified, then CSA reports an "unsupported platform error". **Workaround**: Do not modify the first line of the /etc/issue file.
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.

Obtaining Documentation

These are documents included in this release:

- Installing Management Center for Cisco Security Agents 4.5.1
- Using Management Center for Cisco Security Agents 4.5.1
- Release Notes for Management Center for Cisco Security Agents 4.5.1

The CSA security policies are described in their own policy description papers. These papers are maintained and distributed separately from the CSA 4.5.1 documentation above. All policy descriptions are contained in the "CSA_Policy_Descriptions.zip" file which can be downloaded through CSA's Product Postings area on Cisco.com

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access CSA's Product Postings area at this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/csa

You can access CSA's Hot Fix Postings area at this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/csahf-crypto

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the Obtaining Documentation section.