



Release Notes for Management Center for Cisco Security Agents 5.1

Revision Date: April 6, 2009

These release notes are for use with Management Center for Cisco Security Agents (CSA MC) 5.1. The following information is provided:

- [Installation Overview, page 2](#)
- [Obtaining a License Key, page 2](#)
- [File Integrity Check Instructions, page 3](#)
- [Product Notes, page 4](#)
- [New Features, page 6](#)
- [System Requirements \(CSA MC\), page 8](#)
- [System Requirements \(Agent\), page 10](#)
- [Upgrade Support, page 13](#)
- [Internationalization Support, page 13](#)
- [VMware Environment Support, page 19](#)
- [Windows Firewall Disabled, page 21](#)
- [Cisco Security Agent Policies, page 22](#)



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

- [CSA MC System Default Policy](#), page 22
- [Cisco VPN Client Support](#), page 22
- [Known Issues](#), page 23
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#), page 31
- [Cisco Security Forum](#), page 32
- [Cisco Professional Services](#), page 33

Installation Overview



Caution

This Management Center for Cisco Security Agents V5.1 release is intended for new installations. You cannot upgrade to V5.1 from a previous version of the product.

You must have local administrator privileges on the system in question to perform the CSA MC installation. Once you've verified system requirements, you can begin the installation.



Caution

After you install CSA MC, you should not change the name of the MC system. Changing the system name after the product installation will cause agent/CSA MC communication problems.

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.

File Integrity Check Instructions

You can perform integrity checks on the files provided with Management Center for Cisco Security Agents 5.1. Use the `cisco_V(#)_verify_digests.exe` file posted to CCO to check the MD5 hashes of the files. The MD5 of the `cisco_V(#)_verify_digests.exe` file is posted on CCO to maintain a linked verification chain.

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 Management Center for Cisco Security Agents V5.1:



Note

The Management Center for Cisco Security Agents V5.1 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:** The default Unix policy having to do 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, 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:
 - 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.

Administrator LDAP Authentication

The CSA MC default authentication method for authenticating administrators to the system is local database configuration authentication. This is when administrator names and passwords are entered via CSA MC. Alternatively, you can configure CSA MC to authenticate administrators using LDAP. You must already have a configured LDAP server that can communicate with CSA MC to use this authentication type.

Administrator Role-based Configuration

Administrators can have different levels of CSA MC database access privileges. The initial administrator created by the CSA MC installation automatically has configure privileges. Edit or add administrator accounts on the MC from Maintenance>Administrators>Account Management.

Browser Support

The CSA MC V5.1 UI is no longer supported with Netscape Browsers. Support has been added for FireFox Version 1.5.0.x or higher.

MSDE Installation

If you selects to install MSDE as part of the CSA MC installation, the MSDE installation procedure is now “seamless.” You are no longer required to reboot the server after the MSDE installation and then restart the CSA MC install as in past releases. Now, the CSA MC installation automatically proceeds after the MSDE installation completes. Only a single reboot at the end of the both installations is required.

Report Integration

CSA MC V5.1 UI no longer supports integration with SecMon for reporting. Integration with MARS is now supported.

Server Platform Support

CSA MC V5.1 is only supported on Windows 2003 R2 Standard or Enterprise Editions, Service Pack 0 or 1.

Standalone Server

CSA MC V5.1 is not part of the CiscoWorks/VMS product. It is a standalone server intended for new customers. There is no upgrade path to CSA MC V5.1.

System Requirements (CSA MC)

Table 1 shows the minimum CSA MC server requirements for Windows 2003 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	<ul style="list-style-type: none"> IBM PC-compatible computer Color monitor with video card capable of 16-bit
Processor	1 GHz or faster Pentium processor
Operating System	Windows 2003 R2 Standard or Enterprise Editions Note To run terminal services on the CSA MC system, you must edit the MC policy.
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 4. 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 if 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	<ul style="list-style-type: none"> • 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 <p>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.)</p> <p>Supported language versions are as follows:</p> <ul style="list-style-type: none"> • 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.

System Component	Requirement
Memory	128 MB minimum—all supported Windows platforms
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 to CSA MC V5.1 from previous versions of CSA MC is not supported.

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 (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)
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)

	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	T	T
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	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

VMware GSX 3.2	Host OS (US English Only)
	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 System Default Policy

The CSA MC system itself requires a severely locked down policy to protect it. As a result, no Web browsing from the MC or running of mobile code of any kind is allowed. This includes automatic Windows update downloads. By default, Windows updates are not allowed on the CSA MC system.

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	<p>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.</p> <p>Conditions: Administrator performing maintenance tasks on CSA MC.</p> <p>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.</p>
CSCed17183	Cannot view ActiveX reports without using fully qualified CSA MC name	<p>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.</p> <p>Workaround:For proper viewing of CSA MC ActiveX reports, make sure to use the fully qualified name when browsing to the MC.</p>
CSCef16814	Unix non-root users should have access to UI	<p>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.</p> <p>Workaround: None at this time. Polls will continue to occur at regular intervals determined by the group parameter for polling.</p>

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.	<p>Symptom: It has been reported that the AFS (Andrew File System) is not compatible with the Cisco Security Agent on Solaris 2.8.</p> <p>Workaround: None at this time.</p>
CSCef22643	Request to have CSA alerts include the parent process with the child process.	<p>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.</p> <p>Workaround: None at this time.</p>
CSCef38271	Unicode characters are not supported for CSA MC reports.	<p>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.</p> <p>Workaround: There is no known workaround.</p>
CSCef69413	ASC query is displayed in the wrong session.	<p>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.</p> <p>Workaround: None at this time.</p>
CSCef96134	Behavior analysis creates incorrect rule modules at times.	<p>Symptom: Behavior analysis creates incorrect rule module when file/data streams are used.</p> <p>Workaround: Run the Behavior analysis job but manually delete all data/file stream references (the colon and all information after it).</p>
CSCeg30323	Analysis reports do not detect outlook express and media player.	<p>Symptom: Application Analysis fails to report windows components such as Outlook Express and MediaPlayer unless they are patched.</p> <p>Workaround: None at this time.</p>

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.	<p>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.</p> <p>Workaround:None at this time.</p>
CSCeg57681	Cannot navigate keyboard in Linux query challenge.	<p>Symptom:Unable to navigate using only the keyboard as input on the Linux query challenge dialog.</p> <p>Workaround:Cisco Security Agent on Linux must use a pointer device (mouse, etc) to direct input in the Linux query challenge dialog.</p>
CSCeg60208	False positive using Netmeeting directory on W2K.	<p>Symptom:The use of NetMeeting in a domain environment produced certain events. These events are not due to malicious behavior on the part of Net-Meeting.</p> <p>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.</p>

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCeg71633	Report engine design cannot support multiple administrators.	<p>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".</p> <p>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.</p> <p>Workaround:Exercise care in administering a system where more than one administrator could be running reports at one time.</p>
CSCeg76282	There is no way to enable security if agent UI is not present.	<p>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.</p> <p>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.</p>
CSCeg87069	Policies that ship with CSA MC for Linux interfere with automounter.	<p>Symptom:Default Linux policies interfere with the operation of the automounter.</p> <p>Workaround:A workaround is to create exceptions for /usr/sbin/automounter from Buffer overflow rule terminate actions in the Linux policies.</p>

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.	<p>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.</p> <p>Workaround:Use the wizard to tune the default policies to allow the Red Carpet daemon to run less noisily.</p>
CSCeg88921	Newly installed COM objects are not protected by the agent until the system is rebooted.	<p>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.</p> <p>Workaround: The system must be rebooted or the agent service stopped and restarted. At that time, the agent will register the new COM objects.</p>
CSCeh25293	Uninstalling CSA turns on Windows XP firewall automatically	<p>Symptom: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.</p> <p>Workaround: After CSA uninstall completes, set the Windows Firewall to the appropriate state manually.</p>
CSCeh36870	The multimedia client rule module is not attached to a policy.	<p>Symptom:The multimedia client rule module ship as “not attached” to a policy by default.</p> <p>Workaround:Attach the multimedia client rule module to the default desktop group policy if those particular rules are required.</p>

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.	<p>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.</p> <p>Workaround:Disable the "Pop-Up Blocker" on the browser when administering CSA MC.</p>
CSCin88933	When upgrading to CSA MC 4.5, the import root certificate tab is seen twice.	<p>Symptom:When upgrading to CSA MC 4.5 with CSAMC 4.0.x already installed, there are two entries for importing the root certificate.</p> <p>Workaround:The root certificate only needs to be imported once.</p>
CSCok06488	CSA MC event report exporting fails for a large numbers of events.	<p>Symptom:The generation of a CSA MC report, containing very large numbers of events, fails and produces only a truncated report.</p> <p>Workaround:When exporting event-based reports, keep the number of exported events to a manageable size.</p>
CSCsa60422	Crystal Reports 8 cannot export to Excel 2003.	<p>Symptom:Crystal Reports 8 can only be exported using Excel 5 (rtf 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.</p> <p>Workaround:The only available work around is to export as rtf and import to Excel 2003.</p>
CSCsa63154	When you Click the Purge log button on the agent GUI, events remain in the Messages window.	<p>Symptom:The agent GUI does not clear events from the Messages display when the "Purge log" button is clicked.</p> <p>Workaround:One can exit the agent GUI and then restart the GUI via the Windows Start menu to clear the display.</p>

Table 15 Known Issues in Cisco Security Agent 5.0

Bug ID	Summary	Explanation
CSCsb14859	Application SpeedCommander aborts when CSA is installed	<p>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.</p> <p>Workaround: The workaround is to add the SpeedCommander program to the application class for "Processes requiring Kernel Only Protection".</p>
CSCsc13217	CSA default policies do not support Webroot Spysweeper	<p>Symptom: Webroot Spysweeper triggers buffer overflow rules in CSA Feature Request: Add CSA support for Webroot products such as Spysweeper. (Conditions: CSA 5.x and Webroot Spysweeper (www.webroot.com))</p> <p>Workaround: Create appropriate policy exceptions.</p>
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.	<p>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.</p> <p>Workaround: None. This is considered additional functionality to be added in a future release.</p>
CSCsc30216	@removable does not work in an application class	<p>Symptom: @removable token does not work properly in the literal definition of a application class.</p> <p>Workaround: Use @removable in the file set definition.</p>

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.	<p>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.</p> <p>Workaround: None. Subsequent packets in the stream will be marked and the stream will benefit from the QoS markings.</p>
CSCsc40429	There is a repeatable system delay / non-responsiveness when accessing a file protected by a CSA File version rule.	<p>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.</p> <p>Workaround: Avoid using File Version rules on systems where virus scanners are deployed.</p>
CSCsb02296	CSA cannot distinguish a remote client accessing the registry as a read or a write operation	<p>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.)</p> <p>Workaround: None. This is considered addition functionality to be added in a future release.</p>

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

Related CSA Documentation

This section describes the types and location of documentation for Management Center for Cisco Security Agents. These locations are subject to change.

- *Installing Management Center for Cisco Security Agents 5.1* on Cisco.com at the following location:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_installation_guides_list.html.
- *Using Management Center for Cisco Security Agents 5.1* on Cisco.com at the following location:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_and_configuration_guides_list.html
- *Release Notes for Management Center for Cisco Security Agents 5.1* on Cisco.com at the following location:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_notes_list.html

Location of CSA Documents on Cisco.com

You can find the documentation for the Management Center for Cisco Security Agents here:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html

To navigate to the area represented by the link, follow these steps:

-
- Step 1** Browse to Cisco's home page, <http://www.cisco.com>.
 - Step 2** Mouse over the **Products & Services** menu and click **Security**.
 - Step 3** Scroll down to the **Product Portfolio** area.
 - Step 4** Find **Endpoint Security** and click **Cisco Security Agent**.
 - Step 5** Look for the **Support** box on the right side of the page.

Click **Cisco Security Agent**. This brings you to a linking page where you will find links to all CSA user documents.

Cisco Security Forum

If you would like to post questions or read what others are posting to the Cisco Security Forum concerning the Cisco Security Agent, go to the following location (You must have a valid CCO account to access this location):

http://forum.cisco.com/eforum/servlet/NetProf?page=Security_discussion

Cisco Professional Services

If you are interested in contracting Cisco professional services to assist you in the deployment of the Cisco Security Agent and in the writing of CSA MC policies, inquire at the following location:

http://www.cisco.com/en/US/products/svcs/services_area_root.html

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Copyright © 2009, Cisco Systems, Inc.
All rights reserved.

