



Release Notes for Management Center for Cisco Security Agents 5.2

These release notes are for use with Management Center for Cisco Security Agents (CSA MC) 5.2. 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 14](#)
- [Internationalization Support, page 15](#)
- [VMware Environment Support, page 20](#)
- [Windows Firewall Disabled, page 22](#)
- [Cisco Security Agent Policies, page 22](#)
- [CSA MC System Default Policy, page 23](#)
- [Cisco VPN Client Support, page 23](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Cisco Security Forum, page 23](#)
- [Cisco Professional Services, page 23](#)
- [Known Issues, page 24](#)
- [Obtaining Documentation, page 48](#)
- [Documentation Feedback, page 50](#)
- [Cisco Product Security Overview, page 50](#)
- [Obtaining Technical Assistance, page 51](#)
- [Obtaining Additional Publications and Information, page 54](#)

Installation Overview

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 the following web site.

<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>

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 5.2. 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 `cisco_V(#)_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 V5.2:



Note

The Management Center for Cisco Security Agents V5.2 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 Cisco Trust Agent (CTA) and its bundled components do not include upgrade support.

Solution: The CSA MC Agent Kits page lets you install a CTA kit, if present, with the CSA kit. Because CTA does not include upgrade support, before you install a new CTA kit, you must manually uninstall an existing installation of CTA on the end hosts in question.

- **Issue:** When generating reports on CSA MC, you should not that the font Jasper reports uses to generate PDF reports does not support the complete extended Japanese and Chinese character sets.

Solution: Use an HTML format. HTML reports use the Arial Unicode font from Microsoft which supports most extended language types.

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

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

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

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

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

- **Issue:** The pre-built reports configured for Analysis Deployment Investigation are meant as samples. You will likely have to edit or add to the existing report configurations to gather comprehensive information.
- **Issue:** Linux Agent UI: For gnome desktop environments, the install script will only modify the default session config file for launching the agent UI automatically every time a user starts a gnome desktop session. But if a user already has their own session file (`~/.gnome2/session`), the default session file (`/usr/share/gnome/default.session`) will not be effective. Therefore, the agent UI will not automatically start when the user logs in. In such a case, the user must add the agent UI (`/opt/CSCOsca/bin/ciscosecui`) manually (using "gnome-session-properties" utility) to make the agent UI auto-start. The user may also need to add a panel notification area applet to the control panel.
- **Issue:** 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.

Connection Rate Limit Rule

This rule type now has another pulldown option. The *Communicating with* field allows you to select all, different, or specific hosts for the rule. When the rate limit is reached, you can use this field to determine whether all subsequent service requests are dropped or only those received or sent by a specific host. If you select a “specific” host, this indicates that the host in question exceeded the rate limit. If you select all hosts, this indicates that the sum total of to and from all hosts exceeds the limit and all hosts are blocked. Selecting the “different” hosts option would be beneficial for controlling outgoing connections.

CSAAPI - The Scripting Interface

The Management Center for Cisco Security Agents provides administrators with the ability to use scripts for performing some very specific functions locally on the MC or from a remote system. This scripting interface is called CSAAPI and it allows you to write your scripts in any language and run your scripts on any operating system. The CSA MC scripting interface lets you execute a variety of functions, which include manipulating hosts and retrieving host information.

Discovery of other CSA Nodes

This new *Set* attribute is available for certain rule types. It is intended to determine if a host IP address has an active Cisco Security Agent associated with it. If so, a list of active agent systems is maintained and can be used in rules, via a cookie (@csanode) to restrict or allow communication and resource availability based on the presence of an active agent.

Full-Text Searches

The CSA MC Database Maintenance page provides an optional *Event full-text search* function. This feature allows you to utilize the SQL Server full-text search function. Full-text searching is an optional component of SQL Server. When installed, it offers additional string querying abilities such as string comparisons similar to internet search engines, returning both results and a matching score or weight.

Jasper Reports

CSA MC now uses Jasper Reports to generate MC reports. CSA MC requires and installs Sun JRE (Java Runtime Environment) to generate reports using the Jasper reporting tool. Note that if you don't want the Java Runtime Environment on your MC system, and you remove the Java directory from the system, you cannot generate reports. Available report format types are PDF and HTML.

Microsoft SQL Server 2005 Support

CSA MC now supports local and remote database installations using Microsoft SQL Server 2005 with Service Pack 0 or Service Pack 1. You should note that if you install a SQL Server 2005 build that is lower than build number 2153 (released after SP1), the service "SQL Server Integration Services" will fail upon system reboot. You can manually start the service or you can upgrade to Microsoft SQL Server 2005 SP1 build number 2153 or higher.

System API Control Rule

This rule type now has a "targeting" feature that applies to the *Inject code into other applications* and *Write memory owned by other applications* checkboxes. A targeting option is available for these items because these actions (injecting code and writing memory) involve two or more parties. These parties include the one that is initiating the action and the process(es)

being affected. Providing an optional targeting selection in these cases for choosing particular application classes allows for further configuration granularity.

Wireless Support

You can now select network interface types (Wired, WiFi, Bluetooth, IrDA, Virtual, Dial-up) to control connections on your network. The interface types apply only to your local network and do not apply to remote connections. You can use this feature to control connectivity based on the manner in which a machine is talking on the network. For example, if a type of WiFi network interface detected by CSA, you can configure and apply rules that deny wireless connections on your internal network. Configure this feature using System States and Network Interface Set variable types in rules. Note that CSA only deals with IP networks. Therefore, the provided list of interface types only pertains to those connection types running over IP.

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 1,000 agents. If you are planning to deploy CSA MC with more than 1,000 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, Service Pack 0 , 1, or 2 Note To run terminal services on the CSA MC system, you must edit the MC policy.
File System	NTFS

System Component	Requirement
Memory	1 GB minimum memory
Virtual Memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space

- CSA MC qualification and first level support for operation on Japanese OS (JOS) platforms is provided by Cisco Japan.
- 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 Microsoft SQL Server Express Edition. If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express Edition, the installation will abort. This database configuration is not supported.

SQL Server Express Edition

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 Express Edition and the required .NET environment. You can use the included Microsoft SQL Server Express Edition (provided with the product) if you are planning to deploy no more than 1,000 agents.



Caution

If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express Edition, 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 2005 or 2000 instead of using the Microsoft SQL Server Express Edition that is provided. Microsoft SQL Server Express Edition has a 4 GB limit. In this case, you can have CSA MC and Microsoft SQL Server 2005 on the same system if you are planning to deploy no more than 5,000 agents. Note that if you are using SQL Server 2005 or 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 R2 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0 , 1, or 2 • Windows XP (Professional, Tablet PC Edition 2005, or Home Edition) Service Pack 0, 1, or 2 • Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4 • Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a Note Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000. (Terminal Services are not supported on Windows NT.) Supported language versions are as follows: <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.
Memory	128 MB minimum—all supported Windows platforms

System Component	Requirement
Hard Drive Space	50 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	50 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 4.0 WS, ES, or AS - minimum supported kernel is 2.6.9-11 RedHat Enterprise Linux 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	50 MB or higher Note This includes program and data.
Network	Ethernet Note Maximum of 64 IP addresses supported on a system.

Upgrade Support

There are several upgrade paths to CSA MC V5.2 from previous versions of CSA MC. Please refer to the Installation Guide for details.

Internationalization Support

All Cisco Security Agent kits contain localized support for various language desktops as shown 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.

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
Polish	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes

Language	Operating System	Localized	Qualified
	Windows 2003	Yes	Yes
Portuguese (Brazilian)	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
Language Interface Pack (LIP)	Windows XP	Yes	No

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
Brazilian Portuguese	L	L	L
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)

	Professional	Server	Advanced Server
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	L	L	L
Portuguese	L	L	L
Russian	S	S	NA
Spanish	L	L(S)	L(S)
Swedish	S	S	NA
Turkish	S	S	NA

Table 8 *Windows XP Support*

	Professional	Home
Arabic	NS	NS
Chinese (Simplified)	L	L(S)
Chinese (Traditional)	T	S
Chinese (Hong Kong)	S	S
Czech	S	S
Danish	T	S
Dutch	S	S
English	L	L
Finnish	S	S
French	L	L(S)

	Professional	Home
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	L	L
Portuguese	L	L
Russian	S	S
Spanish	L	L(S)
Swedish	S	S
Turkish	S	S

Table 9 *Windows 2003 Support*

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

	Standard	Web	Enterprise
Korean	L	L(S)	L(S)
Polish	L	L	L
Portuguese	L	L	L
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 V5.2 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.x (workstation)	Various	All agent supported operating systems	Yes
VMware GSX 3.2 (enterprise)	Various	All agent supported operating systems	Yes
VMware ESX 3.0 and 2.5 (enterprise)	Various	All agent supported operating systems	Yes
(free) VMware Player	Various	All agent supported operating systems	Yes
(free) VMware Server	Various	All agent supported operating systems	Yes

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.

Also note, the Cisco Security Agent has not been fully qualified during the use of VMware Virtual Center's virtualization-based distributed services such as VMware DRS, VMware High Availability (HA) and VMware VMotion.

The following table lists 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 Host OS and Guest OS Support**

VMware/All supported versions	Host OS and Guest OS (US English Only)
	Windows 2003 Server/Enterprise Server/Web Edition/Small Business Server SP1
	Windows 2000 Professional/Server/Advanced Server SP4
	Windows XP Professional/Home Edition SP2
	Windows NT 4.0 Workstation/Server SP6a

VMware/All supported versions	Host OS and Guest OS (US English Only)
	Windows 2003 Server. Enterprise Server 64 bit *CSA protection not supported
	Windows XP Professional 64 bit *CSA protection not supported
	Red Hat AS/ES/WS 4.0
	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."

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

Known Issues

[Table 12](#) provides information on known issues found in this release.

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsi29597	Upgraded systems are not allowed to login after reboot.	<p>Symptom:Upgraded systems are not allowed to login after reboot.</p> <p>Events seen on CSA MC Event Log are of the form: The process '/usr/bin/fam' (as user root(0) group nobody(99)) attempted to access '/tmp/.fam_socket'. The attempted access was a write (operation = DELETE). The operation was denied.</p> <p>Conditions:CSA 5.0 Agents deployed with default rules on Red Hat 3.0 systems that are migrated directly to a CSA 5.2 MC without group re-association to CSA 5.2 policies.</p> <p>Workaround:To address the issue stated in this defect, there was a change applied to System Hardening Module (Linux) [5.2.0 r 203] The 'fam utility (Linux) [V5.2 r203]'application class was excluded from File Access Control rule for All dot files, deny creation and modification in tmp directories (Linux)</p> <p>For earlier releases of CSAMC upgraded to V5.2 r203 we recommend to exclude 'fam utility (Linux) [V5.2 r203]'application class manually.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsa84415	CSA blocks Video-on-Demand re-sumption after pausing.	<p>Symptom:If the user pauses a UDP video stream viewed through IE 6.0 with Windows Media Player (v9.0) for some amount of time (more than one minute), CSA prevents resuming viewing with the following message:</p> <p>4/11/2005 11:50:11 AM: The process 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user domainname\username) attempted to communicate with "10.11.12.13" on UDP port 2334. The attempted access was to accept a connection as a server (operation =@ ACCEPT). The operation was denied.</p> <p>Workaround:Stop the agent if the video fails to resume. Then resume the video and restart the agent. You could also use TCP rather than UDP.</p>
CSCsa88291	The agent queries the user during a Windows XP SP2 search.	<p>Symptom:When performing a Windows search from the Start Menu for all the OCX files on a Windows XP2 machine, the following agent query is seen:</p> <p>The process 'C:\WINDOWS\explorer.exe' (as user ADMIN\Administrator) attempted to access 'C:\WINDOWS\system32\macromed\flash\Fflash.ocx'. The attempted access was a write (operation = OPEN/WRITE).</p> <p>Workaround:Answer “Yes” when queried.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsb83811	There have been requests to allow particular IP addresses to access a remote registry.	<p>Symptom: You cannot control access to a remote registry using the network access control rules or otherwise. There have been requests to be able to control which hosts can access a remote registry of a system running the CSA agent without having to allow ALL hosts to connect. This is because there is no way to tie in an application class for remote registry access to a network set.</p> <p>Conditions: Remote registry access of a CSA protected host.</p> <p>Workaround: Using an IP address to authenticate a remote access is not advisable. Please use a User State for the authenticated remote user.</p>
CSCsc54472	Installing CSA over a remote desktop connection with terminal services, corrupts the agent installation.	<p>Symptom: If CSA is installed over RDP/WTS, and the Windows RDP server is configured to "End" broken connections, it will cause a partial installation of the agent and cause the network card to be left disabled.</p> <p>Workaround: Do not install the agent via Terminal Services with the end broken connections feature ENABLED.</p>
CSCsd03508	When applying Microsoft updates on a system, the agent displays multiple query pop-ups.	<p>Symptom: When attempting to apply Microsoft updates on a system, the agent displays numerous pop-ups related to the download and installation of MS patches or the MS update fails due to lack of permissions.</p> <p>Workaround: Add an exception rule to the rule module in question to allow the Microsoft updates to be applied.</p>
CSCsd21748	A Skype video call freezes when CSA is installed.	<p>Symptom: When a user chooses "No" to a query popped by CSA for system API resources, an in-progress Skype video call will freeze.</p> <p>Workaround: None.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsd55061	Blue Screen On windows XP and Windows 2003 Vmware GSX 3.2	<p>Symptom:A blue screen occurs on Windows XP and Windows 2003 under Vmware Gsx 3.2 with the agent installed when a driver verifier for CSA drivers is executed.</p> <p>Workaround:None.</p>
CSCsh14142	Include unblock function in CSA MC for disabled accounts.	<p>Symptom:CU must open a TAC service request when an admin account needs unblocking after excessive invalid logins (within 24 hours)/</p> <p>Conditions:CSAMC login without local server access.</p> <p>Workaround:See CSA MC User Guide for “webmgr” command line usage.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh71171	The Linux up2date rule should be a Query deny, not a Priority deny.	<p>Symptom:Up2date is terminated without feedback while the csagent is in enforcement mode.</p> <p>Conditions:Using the default Linux groups, up2date is terminated with no output to the user as to why.</p> <p>Workaround:Make the rule 'Redhat Network Update Applications, client/server TCP Services' in the System Hardening Module (Linux) a Query Deny rather than a High Priority Deny. Use the query popup to give the user a warning as to the dangers of updating the kernel.</p> <p>Further Explanation:It is expected that the user, upon seeing that up2date is terminated by the agent, is likely to either put the agent into test mode or simply turn it off to run up2date, not understanding why it is denied. A Query Deny with an appropriate popup warning would be much more informative. The following warning is suggested:</p> <p>Do not use up2date to update kernel while the agent is running. If updating kernel, stop the agent, rebuild the adaptation layer if required, reinstall the csaadapt kernel module, and restart the agent.</p>
CSCsi03931	On Red Hat 4 machines, turning agent security off and rebooting, can cause the system to hang after reboot when security is enabled.	<p>Symptom:If a system is rebooted with agent security turned off, Red Hat 4 machines can hang when agent security is enabled after the reboot.</p> <p>Workaround:None.</p>
CSCsi22075	Data access control rules do not work for Apache 2.2 on Windows systems.	<p>Symptom:Data access control rules do not trigger on Windows systems for Apache 2.2.</p> <p>Workaround:None.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsb06370	CSA agent installation on Solaris does not provide an install log.	<p>Symptom:If an agent install on Solaris 8 fails, there is no install log to explain what failed.</p> <p>Conditions:Failed csagent install on Solaris 8.</p> <p>Workaround:Save the output of the pkgadd command issued to install the CSA agent.</p>
CSCsb17414	There is a request to be able to update CTA from within CSA MC.	<p>Symptom:Enhancement request is made to add the ability to update CTA software from the CSAMC in the same fashion that CSA updates are deployed.</p> <p>Conditions:Customer would have deployed CTA along with CSA and wishes to update CTA and not CSA.</p> <p>Workaround:None</p>
CSCsb31648	Windows cleanmgr continually triggers rule.	<p>Symptom:Windows cleanmgr.exe continually triggers rules even after checking "Don't ask again."</p> <p>Conditions:CSA agents deployed on Windows hosts. But not all Windows hosts are configured to run cleanmgr.exe on a schedule basis. Exceptions are not made in the sample policies.</p> <p>Workaround:Create policy exceptions for cleanmgr.exe that conform to the deployed environment.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsb55146	Administrators cannot make reports from audit log.	<p>Symptom:The CSA Audit Trail cannot be saved in report format. This DDTs is a request to enhance the functionality of CSA by providing audit reports.</p> <p>Conditions:All CSAMC installs have audit log enabled by default. It cannot be disabled.</p> <p>Workaround:The ability to display all changes on a single page has been added. Filter Changes --> Changes per page - Select <All> Cut and paste the output to a file to capture output.</p>
CSCse87201	You cannot disable logging for Registry access control alert on 'REGISTRY\MACHINE'.	<p>Symptom:Can't stop logging only of alerts for access to \REGISTRY\MACHINE or other hive roots. Here is an example of such an alert:</p> <p>TESTMODE: The process '<remote application>' (as user COMPUTER\Administrator) attempted to access the registry key '\REGISTRY\MACHINE' and value ". The attempted access was an open (operation = OPEN/KEY). The operation would have been denied.</p> <p>Workaround:It is possible to disable logging for this key by disabling logging to all subkeys as well. Create an exception rule that does not log, and matches on HKLM**. Be careful not to make this an allow rule, or you will allow access to the whole branch of the registry.</p> <p>Also, the alert above usually does not effect application access to the registry, so it is usually safe to ignore it.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCse93386	There is popup/banner during login to the CSA MC.	<p>Symptom:Support is implemented for displaying a notice/warning popup before login (after the user clicks Login). The user needs to acknowledge this popup to be able to login.</p> <p>Conditions:CSA MC administrators require additional security measures for accessing CSAMC to meet internal standards.</p> <p>Further Explanation:To enable the notice popup: webmgr enable_login_notice "notice_filepath" admin_name password notice_filepath = file containing the notice text (truncated to 1000 chars). Credentials of a Configure admin are required.</p>
CSCsf24202	Turn off agent flag waving from the CSA MC.	<p>Symptom:The ability to disable the flag waving in the Windows system tray was added by an agent side configuration change. How to configure the agent side is detailed in CSCeg87151.</p> <p>Conditions:CSA MC administrators desiring the ability to disable the flag waving centrally from the CSA MC.</p> <p>Workaround:This enhancement request will be considered in a future release.</p>
CSCsg20120	UNIX QoS TCP Server the ACK packet is not getting marked and remarked.	<p>Symptom:On Linux and Solaris, the ACK packet is not getting marked or remarked when the CSA agent machine acts as a SERVER. All other packets are getting marked and remarked.</p> <p>Conditions:Cisco Security Agent deployed on Unix systems with rules that enforce QoS marking and remarking of traffic.</p> <p>Workaround:None.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsg70010	Cisco IPS needs a constant URL for the SDEE server connectivity.	<p>Symptom: Cisco IPS needs a constant URL for the SDEE server connectivity.</p> <p>Conditions: The following was implemented:</p> <ul style="list-style-type: none"> - For 5.0, 5.1 hotfixes add the URL <code>https://csa-hostname/csamc/sdee-server</code> to apache config. - For 5.2 add the URL <code>https://csa-hostname/csamc/sdee-server</code> to apache config, and implement auto-switch of this URL during migration from the old to new MC. <p>Workaround: Upgrade to current CSAMC versions CSAMC 5.0.0 --> Upgrade to version 5.0.0.210 or higher</p> <p>CSAMC 5.1.0 --> Upgrade to version 5.1.0.95 or higher</p> <p>CSAMC 5.2.0 --> The FCS release contains this code correction.</p> <p>For additional details, see the release note published on www.cisco.com for this defect.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsg77327	Incorrect selection of interface for outgoing and incoming connections.	<p>Symptom:The interface displayed in a log message for a TCP or UDP connection is not the expected interface or is Unknown.</p> <p>Conditions:There are cases where it is not possible to determine which interface is being used for a particular 'connection'. These include cases where more than one interface is being used for a single connection (such as when asymmetric routing is in place). In these cases, one of the interfaces will be used as the interface in the log message (and controlled in the rules).</p> <p>Workaround:In some cases, this problem is triggered when the routing metrics for (say) the ethernet adapter and the wireless adapter are set to the same value. In this case, adjust the wireless adapter to have a higher metric to favor the ethernet adapter when it is available.</p> <p>It is intended to provide a comprehensive fix in a later version of the product which would cause these multi-adapter connections to be checked by the rule system once for each adapter.</p>
CSCsg89393	CSA MC upgrade fails when files in DB directory have NTFS compression attribute.	<p>Symptom:CSA MC upgrade fails.</p> <p>Conditions:If the SQL database files have the NTFS compression attribute set, then upgrade of the MC fails with a log message complaining that the DB files are compressed.</p> <p>Workaround:Detect compression attribute and unset it in DB directory and files before upgrading.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsg98329	Many unusual system calls made on agent systems.	<p>Symptom:Events seen on the CSAMC with the format of: 12/6/2006 4:06:24 AM some-host.cisco.com Notice The process 'E:\icm\bin\dumplog.exe' (as user NT AUTHORITY\SYSTEM) attempted to call the function OpenKeyedEvent. This is unusual, as calls to this function are seldom made. The operation was allowed by a rule (rule defaults).</p> <p>Conditions:Unusual systems calls being made on deployed CSA agent systems.</p> <p>Workaround:These are diagnostic messages aimed at detecting changes in the system calls offer by the operating system. They are only monitoring the system call. Please report these events to TAC at your earliest convenience.</p>
CSCsh44023	Putting extended ascii set characters into Contact Info crashes Linux agent UI.	<p>Symptom:On Red Hat Linux -v4 and -v3, putting extended ascii set chars into agent Contact Info crashes the agent UI. The v4 popup message is "The application ciscosecui has quit unexpectedly." The v3 popup message is " Application "ciscosecui" has crashed due to a fatal error (segmentation fault).</p> <p>Conditions:CSA agents system running on Red Hat Linux. Use of extended characters is not considered typical for users to input into the CSA agent GUI.</p> <p>Workaround:None at this time. Avoid the use of extended character sets in this data. Restart the CSA agent GUI if the process exits.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh45706	W2k3-sp1: File access control query triggers twice on one write operation.	<p>Symptom:Common mis-perception of Windows file operations making multiple attempts to operate on a file when only one user action was take.</p> <p>Conditions:When you right click to create a new document on a Windows 2003 system with the Cisco Security Agent installed, it appears that explorer.exe tries to create a document with the default name first, and then, if it fails, it tries with the (2) name. Happily, it stops there.</p> <p>We correctly prevent both attempts to create the file, and since they are different file names, the cached answer from the first query is not used for the second query.</p> <p>Windows does have a habit of appending suffixes to filenames to find one that works, and it might be an enhancement request to treat (for cached answer purposes) file.txt and file(2).txt as the same name.</p> <p>Workaround:None. This is how the operating system behaves and the Cisco Security Agent identifies all operations correctly. Careful observation will allow the user to draw the same conclusions.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh51376	Data access control rule not installing / working on RHEL4 with SELinux enforced.	<p>Symptom:Red Hat v4 systems with the SELinux kernel parameter set to enforced will fail to load data filter into the system's web server.</p> <p>Conditions:CSA 5.2 agent on Red Hat Linux V4 installing data filter.</p> <p>Workaround:CSA 5.2 prints a warning message that tells the user at data filter installation time if the SELinux is enforced on the RHLE4 machine. The user then can add a SELinux policy that allows httpd to perform ioctl on /dev/csacenter, or put the SELinux to permissive or disabled state if they want use CSA data filter function.</p>
CSCsh56306	Remove CTA 2.0.x default installers from CSA MC.	<p>Symptom:Cisco Trust Agent has updated to version 2.1.103-0. Older versions currently shipped with the Cisco Security Agent Management Center should be replaced.</p> <p>Conditions:Recent hotfixes to CSA MC 5.0.0 and CSA MC 5.1.0 remove all versions of the CTA installer. The admin needs to obtain the current CTA package and load it into the CSA MC.</p> <p>CSA 5.2 ships without any CTA packages. It is up to the administrator to obtain current CTA packages and rebuild CSA agent kits.</p> <p>Workaround:</p> <ul style="list-style-type: none"> - Remove all obsolete CTA packages from CSA MC directories. - Obtain current CTA package from www.cisco.com. - Copy current CTA packages to CSA MC directories. - Rebuild CSA agent kits before deployment.

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh64974	Remove CTA 1.0 from CSA 5.0 and 5.1.	<p>Symptom: Cisco Trust Agent has updated to version 2.1.103-0. Older versions currently shipped with the Cisco Security Agent Management Center should be replaced.</p> <p>Conditions: Recent hotfixes to CSA MC 5.0.0 and CSA MC 5.1.0 remove all versions of the CTA installer. The admin needs to obtain the current CTA package and load it into the CSA MC.</p> <p>CSA 5.2 ships without any CTA packages. It is up to the administrator to obtain current CTA packages and rebuild CSA agent kits.</p> <p>Workaround:</p> <ul style="list-style-type: none"> - Remove all obsolete CTA packages from CSA MC directories. - Obtain current CTA package from www.cisco.com. - Copy current CTA packages to CSA MC directories. - Rebuild CSA agent kits before deployment.

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh66575	CSA MC csalog contains a large amount of false positive portscan messages.	<p>Symptom:Each Network access control deny rule is observed to be accompanied with a corresponding possible syn flood message in csalog.txt. The messages appear to be false positives and therefore should not appear in csalog.txt.</p> <p>Conditions:The feature design is to catch an attacker scanning a range of ports on a single machine and to catch an attacker that scans a specific port on multiple machines. Global correlation determines when a port scanning message is logged to the MC.</p> <p>All Network access control rule denies are not, in fact, followed up with a corresponding syn flood message. The MC policy is restrictive. The nacl denies are for blocked inbound netbios traffic. These messages just appear to be linked because the only network activity is netbios.</p> <p>Workaround:Disable logging on the rule producing events.</p>
CSCsh79059	SMB NULL SESSION and @(smb-null-session) do not work on Windows NT.	<p>Symptom:Using service as either \$SMB NULL SESSION or @(smb-null-session) special token doesn't work on Windows NT. It does work on other Windows platforms. This is a known limitation.</p> <p>Conditions:In Windows NT SMB runs on top of NBT (NetBIOS over TCP/IP), which used the ports 137, 138 (UDP) and 139 (TCP). In Windows 2000 onwards, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra layer of NBT. For this the operating system use TCP port 445.</p> <p>Workaround:None</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh79424	CSA failed to start after clean install RH4.	<p>Symptom:Error messages seen in /var/adm/messages on REd Hat 4.0 systems, such as: Feb 15 09:50:15 client57 kernel: insmod: page allocation failure. order:5, mode:0xd0 Feb 15 09:50:15 client57 kernel: [<c0145f77>] 0x298<br="" __alloc_pages+0x28b=""></c0145f77>]> Feb 15 09:50:15 client57 kernel: [<c0145f9c>] 0x24<br="" __get_free_pages+0x18=""></c0145f9c>]> Feb 15 09:50:15 client57 kernel: [<c014940e>] 0x94<br="" kmem_getpages+0x15=""></c014940e>]> Feb 15 09:50:15 client57 kernel: [<c014a0ce>] 0x236<br="" cache_grow+0x10a=""></c014a0ce>]> Feb 15 09:50:15 client57 kernel: [<c014a3f1>] 0x227<="" cache_alloc_refill+0x1f7="" p=""> <p>Conditions:The problem caused by the kernel memory being badly fragmented when we try to allocate a big block of contiguous memory at csaadapt loading time. A warning message in the startup script will inform the user to reboot the system if the problem happens.</p> <p>Workaround:None</p> </c014a3f1>]></p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh86078	CSA prevents CTAPSD from writing logfiles/directory	<p>Symptom:Error messages seen for the Cisco Trust Agent process CTAPSD writing to log files.</p> <p>Conditions:Message seen on the CSA MC event log will be of the form:</p> <p>The process 'D:\Program Files\Cisco Systems\CiscoTrustAgent\ctapsd.exe' (as user NT AUTHORITY\SYSTEM) attempted to access 'D:\Documents and Settings\All Users\Application Data\Cisco Systems'. The attempted access was a write (operation = OPEN/CREATE). The operation was denied.</p> <p>Workaround:CTA 2.1 does not use the application data directory for logging, rather a logging directory under program files\...\CTA\logging, that is created at install time.</p> <p>Cisco Trust Agent 2.1 is the currently supported version. Administrators should update to this package.</p>
CSCsh94476	Some Japanese characters are missing in PDF reports.	<p>Symptom:Some japanese characters are missing in PDF report. In HTML reports, all Japanese characters are shown correctly.</p> <p>Conditions:The current font used by Jasper to generate PDF reports does not support the extended Japanese and extended Chinese character sets. HTML reports use the Arial Unicode font from Microsoft which supports most of these extended languages. This is a known limitation.</p> <p>Workaround:No workaround at this time. Scheduled to be addressed in a future release.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsi00271	There is no logging in Agent UI for IIS Server policy kit.	<p>Symptom: Administrators and users are not clear as to why some CSA events are not seen on CSA agent GUI and are only logged to the CSA MC.</p> <p>Conditions: Logging is controlled by a variety of criteria. Logging may occur on MC or agent or both. UI messages are filtered by event and may not appear when logged.</p> <p>Workaround: None</p> <p>For additional details, see the release note published on www.cisco.com for this defect.</p>
CSCsi01550	RHEL-3: Kernel panic with Kernel/rootkit rule.	<p>Symptom: Kernel panic error on Red Hat 3.0 systems with CSA installed.</p> <p>Conditions: The problem happens only on RHEL3 when you install (build) csagent on a single cpu configuration and then reboot using a multi cpu configuration.</p> <p>Note1: If you install(build) on multi-cpu and reboot using single cpu configuration, you will not have this problem.</p> <p>Note2: In RHEL4 this is not an issue because you cannot load the csa drivers that do not match the kernel on which they were built - this is controlled by the OS itself and not CSA.</p> <p>Therefore the problem case is a corner case where the user is configured with the two configurations. It is not considered typical for a system to physically have multiple processors and run a version of RHEL3 that does not take advantage of all hardware.</p> <p>Workaround: Configure and boot to the version of RHEL3 that best matches the physical system. Install CSA when booted to that configuration.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsi13689	Page error occurs after unchecking reminder visibility.	<p>Symptom:The next page after unchecking the login reminders visibility checkbox throws the following error:</p> <pre>[2007-03-15 10:14:25.921] [PID=7376] [webadmin]: LoadPage: Error processing htl_page 'group_list'. err=invalid command name "db-String" while executing"dbString show_reminder" (procedure "hf_handle_reminders" line 6) invoked from within"hf_handle_reminders" (procedure "header" line 103) invoked from within"header \$title { } { } {" ("eval" body line 1) invoked from within "eval {header \$title} \$args" (procedure "common_header" line 135) invoked from within "common_header \$path "" \$onload \$onunload" (procedure "dirview" line 56) invoked from within "dirview view"</pre> <p>Conditions:This error will only display once and later visits to the same page will not produce the error.</p> <p>Workaround:Administrators can safely ignore the error after the first occurrence. Or the version of CSA MC can be upgraded to pick up the code corrections.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
CSCsh10786	How can we identify the related hosts generating these alerts?	<p>Symptom:When a file is quarantined globally as a result of AntiVirus software detecting an infected file on 2 or more CSA protected hosts on the network, the events listed in the Global Event Correlation page on the CSA MC do not indicate what hosts the infected files were detected on.</p> <p>This information would be useful to the administrator in order to find and inspect the potentially infected machines.</p> <p>Workaround:By default, the NT Event Log rules that gather the AntiVirus software events are set to log a message in the event log when these events occur.</p> <p>By looking at the Global Event Correlation and Quarantine events, the administrator should be able to decipher the time frame within which the AntiVirus detections occurred, and then use the event log messages to find the potentially infected hosts.</p>
CSCsh95492	The Wizard window does not stay in the foreground when using Firefox 2.0.	<p>Symptom:There exists a bug in Firefox 2.0 (fixed in Firefox 2.0.0.1 and beyond) that can prevent the CSA MC event wizard from remaining in the foreground at all times.</p> <p>Workaround:From the Firefox menu bar, select Tools->Options. Select the Content tab and click the "Advanced" button across from "Enable JavaScript". Next, click on the box that says "Raise or lower windows". Then press OK on the open Dialogs.</p>

Table 12 Known Issues in Cisco Security Agent 5.2

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>
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>
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>
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>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
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>
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>
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>

Table 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
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>
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 12 Known Issues in Cisco Security Agent 5.2

Bug ID	Summary	Explanation
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>
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>

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco

service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

<http://www.cisco.com/techsupport>

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

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



Note

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [Table 12 provides information on known issues found in this release](#) section.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Copyright © 2007, Cisco Systems, Inc.
All rights reserved.

