



Release Notes for Management Center for Cisco Security Agents 6.0

Updated: April 2, 2010

These release notes are for use with Management Center for Cisco Security Agents (CSA MC) 6.0. The following information is provided:

- [Installation Overview, page 3](#)
- [Obtaining a License Key, page 3](#)
- [License Types, page 4](#)
- [File Integrity Check Instructions, page 4](#)
- [Installing Management Center for Cisco Security Agents V6.0, page 5](#)
- [Documentation Location Information, page 6](#)
- [Product Notes, page 6](#)
- [New Features, page 9](#)
 - [Improved CSA MC Interface, page 9](#)
 - [Shortened Deployment Time, page 12](#)
 - [AntiVirus Integration, page 12](#)
 - [Automatic Signature Generation, page 13](#)



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

© 2010 Cisco Systems, Inc. All rights reserved.

- Data Loss Prevention, page 14
- Vista, WEPOS and IPv6 Support, page 15
- Additional Language Support, page 15
- Audit Mode, page 15
- Application Trust levels, page 16
- Event Analysis, page 16
- Notify User Rule Actions, page 16
- User Justifications, page 17
- Printer Access Control Rule, page 17
- PCI Policies, page 17
- Read Only Mode, page 17
- System Requirements (CSA MC), page 18
- System Requirements (Agent), page 20
- Upgrade Support, page 23
- Internationalization and Localization Support, page 23
- VMware Environment Support, page 32
- Windows Firewall Disabled, page 33
- Windows Safe Mode, page 34
- Cisco Security Agent Policies, page 34
- CSA MC System Default Policy, page 34
- Cisco VPN Client Support, page 34
- Cisco Security Forum, page 35
- Cisco Professional Services, page 35
- Known Issues, page 35
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 51

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

Management Center for Cisco Security Agents (CSA MC) ships with a preliminary license (csamc.lic) that is automatically imported during the CSA MC installation process. (Note that this is not the formal product license that you will eventually use.) This license is for the CSA MC itself; it allows the CSA MC to be installed, regardless of additional licenses, with at least one agent to protect it. 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. (While you are waiting to receive the combination of PAK information and licensing information from Cisco Systems, you can install the product with this initial license, intending to copy the formal license at a later time.) See the section on **PAK certificates** in *Installing Management Center for Cisco Security Agent, 6.0* for more information.

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.

License Types

There are several separate and distinct licenses for the CSA product:

- A license for the **Management Console (CSA MC)**. This license enables signature-based and behavior-based AntiVirus functionality and content-scanning functionality along with the core functionality of CSA MC.
- A license for **server platforms** (this includes all Windows servers such as Windows 2000 Server, Advanced Server, Windows 2003 Server family, Solaris, and Linux AS and ES)
- A license for **workstation platforms** (this includes Windows 2000 Professional, Windows XP Professional, XP Home, Windows Vista, and Linux WS)
- A license for the **Cisco Security Agent Analysis** (formerly known as “Profiler”). For more information on CSA Analysis, see the chapter on **CSA Analysis** in the *Using Management Center for Cisco Security Agents 6.0*.
- A license for **Data Loss Prevention**. The Data Loss Prevention (DLP) feature is available for Windows desktop platforms only. In order for data scanning rules to be distributed to a host, CSA requires a DLP license key in addition to the standard CSA desktop host key.

DLP licensees are named **DLP Desktop Agent Upgrade** and are available in bundles between 25 and 10,000 seats.

See the section on **Uploading a Licence** in *Installing Management Center for Cisco Security Agent, 6.0* for more information about uploading licenses. See the **Data Loss Prevention** chapter in the *Using Management Center for Cisco Security Agents 6.0* manual for more information about this feature.

File Integrity Check Instructions

You can perform integrity checks on the files provided with Management Center for Cisco Security Agents 6.0. 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.

Installing Management Center for Cisco Security Agents V6.0

**Note**

The Management Center for Cisco Security Agents V6.0 kit is signed by Cisco Systems. This can be verified using Windows Explorer File ->Properties ->Digital Signatures.

- Step 1** Open a command prompt window and `cd` into the product directory. Run **setup.exe**. Alternatively, you can use Windows Explorer to navigate to the product directory. Then, double-click the `setup.exe` file to begin the installation.
- Step 2** You can now follow the standard installation directions provided in the Installation Guide. The Installation Guide appears as a PDF file in the Documentation directory at the top level.

**Note**

The agent kits are provided in protect mode and their rules will be enforced as soon as they are deployed.

Before deploying Cisco Security Agents (CSA) on a large scale, it is worthwhile to run a manageable and modest initial pilot of the product. Even in a CSA upgrade situation, a short pilot program will be beneficial.

CSA 6.0 ships with many security policies that you should be able to run in your enterprise as they are or with only minimal tuning. This tuning is best done on a small sample of systems that are representative of the whole.

Once the pilot is operating satisfactorily, with CSA protecting systems using properly tuned policies, you can turn your pilot into a larger deployment.

Documentation Location Information

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 6.0* on Cisco.com at the following location:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_install_and_upgrade.html.
- *Using Management Center for Cisco Security Agents 6.0* 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 6.0* on Cisco.com at the following location:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_notes_list.html

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:** Windows NT will no longer be supported, starting with this release of CSA.
- **Issue:** When generating reports on CSA MC, you should note 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 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.

For operating system updates especially, it is recommended that you stop the agent to perform the update.

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 Application 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:** 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.

- **Issue: In the releases of CSA before version 6.0.0.214**, if the current securitylog.txt file is 1MB but CSA had created a new securitylog.txt file within the past hour, CSA does not create a new securitylog.txt file and stops logging. CSA interprets the excessive logging as an attack intended to deplete CSA's logging resources. CSA resumes logging to securitylog.txt after an hour has passed from the time it created the previous securitylog.txt file.

In CSA 6.0.0.214 and subsequent builds of CSA, this behavior is different: CSA continues to create new securitylog.txt files whenever the existing securitylog.txt file reaches 1MB. CSA saves up to four of the past securitylog.txt files depending on the configuration of the **esl_file_limit** parameter in the **sysvars.cf** file.

Solution: If you are running a version of CSA 6.0 built prior to version 6.0.0.214 but you prefer the logging behavior of CSA in version 6.0.0.214, upgrade your version of CSA to build 6.0.0.214 or later.

New Features

This release contains the following new features.

Improved CSA MC Interface

There are many additions and improvements to the CSA MC interface. Now administrators have a CSA MC Home page which provides them with central location for the information they need. Throughout the CSA MC interface, the interface has been changed to allow administrators to perform more tasks with less navigation of the CSA MC interface.

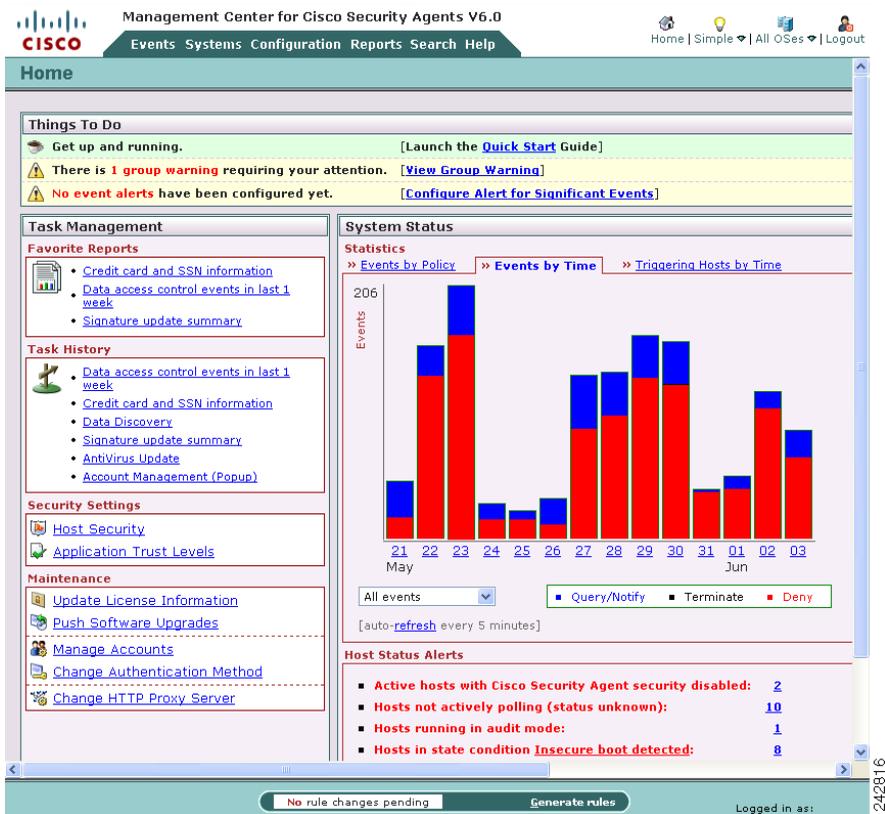
Administrator's Home Page

Upon first logging in, administrators are directed to CSA MC's Home page. The Home page facilitates CSA Administrators' work by pointing out and prioritizing problem areas, summarizing recent security events, and providing convenient links to common tasks and reports. From the Home page users can also launch a short Quick Start Guide to get their deployment up and running.

The Home page is available to both Advanced Mode and Simple Mode users. Administrators can reach the Home page from anywhere in the CSA MC interface by clicking the Home button.

Figure 1

CSA MC Home Page



Simple Mode and Advanced Mode of CSA MC

When users first login to CSA MC, the administrator created during the installation process has a simplified view of CSA MC. This “Simple Mode” view provides everything you need to deploy and administer the product. Default groups are pre-configured and shipped with the MC to provide out-of-the-box security policies for servers and desktops. Through the use of a wizard, you can refine the policies to match the security needs of your site and of the applications that run on your network. Many of the configuration pages are hidden in the Simple Mode view of the CSA MC to allow users to focus on the tools they use most often.

For advanced users there is the “Advanced Mode” view. This view exposes all CSA MC menus and pages to administrators. This gives the administrator the ability to create or configure any component, view all possible reports, and have access to the full range of analytical and maintenance utilities. Advanced view is best for administrators who need to create customized policies for their enterprise or who want more granular control of the system.

Host Security Page

For Windows deployments, the Host Security page allows you to associate policies with groups, put groups and policies in Audit Mode, create agent kits and groups using a wizard. You can view the agent kits associated with a group by clicking the number of agent kits listed in the group row. If there are hosts associated with a group, you can view them by clicking the number of hosts listed in the group row.

Global Command Buttons

The command buttons at the top right of the CSA MC user interface provide quick access to the Home page, the ability to toggle between Simple Mode and Advanced Mode, a way to filter information by operating system, and a logout button. These command buttons are displayed on every page.

Figure 2 *Global Command Buttons*



Configuration Tasks Menus

In the configuration view for many configurable items, there is a Tasks menu in the upper right corner of the page. Clicking the down arrow, expands the menu. This menu provides quick links to common tasks that are relevant to the item being configured. Advanced Mode users are more likely to see and use these menus.

Shortened Deployment Time

CSA 6.0 ships with many security policies that you should be able to run in your enterprise as they are or with only minimal tuning. As a result, you can use the agent kits that accompany the pre-configured desktop and server groups as a good starting off point for your enterprise.

Although every site is different, it would not be unusual to run a pilot program for only one or two weeks after you feel you have tuned your policies to your satisfaction.

AntiVirus Integration

The AntiVirus feature provides protection from computer viruses that have been identified by a signature and malware that has been identified by its suspicious or dangerous behavior.

Signature-based AntiVirus

The signature-based AntiVirus function protects the endpoint by identifying infected files. Once identified, CSA tags these files as infected and then security policies limit the actions of, or the access to, these files.

Virus signatures and the signature-matching infrastructure are supplied by Clam AntiVirus (<http://www.clamav.org>). Clam AntiVirus, or ClamAV™, is an open-source antivirus toolkit. A community of users submit files, infected with viruses to ClamAV, ClamAV creates a signature for the virus and then distributes signature updates to back to its user community.

Incorporating a traditional antivirus scanner in CSA provides fast and efficient defense against known viruses along with a low rate of false positives. This feature compliments CSA's ability to defeat unknown, day-zero attacks based on identifying malicious behavior.

The signature-matching infrastructure supplied by ClamAV and the CSA policies to restrict infected files are only available for Windows platforms.

Behavior-based AntiVirus

The behavior-based AntiVirus function protects the endpoint by examining an untrusted application's behavior. If an application acts in such a way that is suspicious, malicious, or dangerous, the application receives a behavior-based AntiVirus tag and the application is placed in an application class that reflects its behavior.

Behavior-based AntiVirus policies are available for Linux, Unix, and Windows platforms.

AntiVirus Integration in Agent

The end-user can perform a virus scan on demand, quarantine files, delete quarantined files, restore quarantined files, and download the latest available virus definitions through the Cisco Security Agent interface.

AntiVirus Reporting

There are several pre-configured reports administrators can use to learn about the most prevalent infection types, the most infected hosts, and the age of deployed virus-definitions.

Automatic Signature Generation

The automatic signature generation feature provides several new functions for hosts running on Windows platforms:

- Automatically generated signatures
- Denial of Service attack protection
- Process stack recovery

The Cisco Security Agent now responds to certain attacks by identifying malicious payloads used in an attack, dynamically creating a signature that represents those payloads, and then using the signature to prevent further attacks from similar payloads.

These automatically generated signatures are intended to catch a variety of attacks, primarily buffer overflows, including highly specific, targeted, and polymorphic ones. Currently, the automatic signature generation feature focuses on protecting LPC and MSRPC interfaces.

There are also several preconfigured reports that administrators can use to learn about the number of prevented denial of service attacks, the number of times CSA acted as a result of matching an attack payload to an existing signature, and the number of times CSA correlated a signature.

Data Loss Prevention

Data on network endpoints is increasingly subject to internal policies and external regulations concerning proprietary and confidential information. The process of data classification assists network data security by helping track the existence of sensitive data, its location in the enterprise, how that data is being accessed, and how it must be protected to meet legal and regulatory requirements.

Cisco Security Agent's new Data Loss Prevention (DLP) feature includes these capabilities:

- Classification and tagging of a file based on the result of a content scan or its location on the host system.
- Classification and tagging of a file based on what applications attempt to read or write it.
- User notification when users are working with content that is considered sensitive. Raising awareness of the presence of sensitive data will help prevent accidental data loss.
- Pre-configured reports that provide information on what kinds of data are discovered and on the movement of sensitive data.

The DLP feature enables CSA to tag files based on several types of file content, including specific characters or phrases. CSA also provides optimized pattern matching for credit card numbers and Social Security numbers, which are especially sensitive and subject to government regulatory control.

Identification of sensitive data and control over sensitive data can be customized on the CSA MC to assist in the implementation of Data Loss Prevention controls for use of data in compliance with your organization's policies.

The Data Loss Prevention feature is available for desktops only and requires an additional license.

Vista, WEPOS and IPv6 Support

Cisco Security Agent now supports 32bit Windows Vista for agent installation. On the CSA MC, rule modules can be configured specifically for Windows Vista.

The CSA MC now supports and manages IPv6 addresses. Network Address Sets and Network Access Control rules that specify IPv6 addresses can only be associated with a Vista Rule module.

Windows Embedded Point of Service (WEPOS) 1.1 is also supported in this release.

Additional Language Support

CSA now supports Russian. See [Internationalization and Localization Support, page 23](#) for a full list of supported languages and levels of support.

Audit Mode

Audit Mode is the new name for what was called Test Mode in previous releases. Now, in CSA 6.0, you can also place policies in Audit Mode.

When a group, policy, or rule module is running in audit mode, the agent will not deny any action or operation even if an associated rule which indicates that it should be denied. Instead, the agent will allow the action but log an event (if logging is enabled for the rule). This helps administrators understand the impact of deploying a policy or rule module to a host before enforcing it. If examining the logs proves that the policy or rule module is working as intended, administrators can remove the audit mode designation.

Application Trust levels

Application trust levels refer to an application's placement on a "White List," "Grey List," or "Black List." After an application is placed on one of these lists, there are different rules provided in this release that permit or restrict the application from acting.

Applications in the White List are generally trusted and allowed to run, however, they are continuously monitored and if they commit a severe violation, they are immediately restricted.

Applications in the Black List are not trusted and are prevented from running. If they are running, they are terminated. If a user needs to use a black-listed application, then the application must be added to the white list. In such a case, it is recommended that the user adds rules that restrict the application to the minimum set of privileges required.

Event Analysis

The Event Analysis tool shows you the applications that are producing the most events and the hosts on which those applications are running.

Notify User Rule Actions

When you configure various rule types, you can now notify users when one of their actions triggers a rule. Users can then acknowledge the notification and enter a justification for the action in question. The Notification Settings configuration window lets you choose an OK button or a combination of Yes and No radio buttons to add to the notification pop-up window.

Below is an example of a notification text provided in this release:

The application <Application Name> has read Regulatory Data and attempted to print. Please acknowledge if you are in compliance with Corporate Data Security Policy. If you are not in compliance, provide a justification.

User Justifications

Many different rule types can prompt users to justify their actions. Users receive a justification request in a pop-up window. They enter their justifications in a free form editable text box.

The justifications, or lack of justifications, are included in the text of the event if the rule logs events. Administrators can then analyze events in the context of these justifications.

The previous section, [Notify User Rule Actions](#), provided one example of a justification. Here is another example of requiring users to justify their actions when disabling security:

An attempt is being made to disable security for the Cisco Security Agent. Do you wish to allow this? Please provide a justification.

Printer Access Control Rule

Use this rule type to control which applications are allowed to send data to the printer. For example, you can use this rule to prevent applications categorized as “sensitive data applications” from printing.

PCI Policies

Cisco has created a series of Cisco Security Agent policies that map to PCI requirements. These policies can be used with any Cisco Security Agent, whether installed on servers, desktops, laptops, or point of service terminals.

Contact your Cisco Partner or Cisco Sales Engineer to obtain these policies.

Read Only Mode

Many components, such as variables, application classes, rule modules and policies can be configured as read-only. Read-only objects can not be edited or deleted. Read-only configuration prevents such components from being accidentally modified and it preserves the original configurations of components shipped with this release.

If the need arises, administrator accounts with configure privileges can be changed to permit them to modify read-only components.

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 *Installing Management Center for Cisco Security Agents 6.0* for more detailed information about scalable deployments.

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
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.
- The minimum recommended screen resolution for viewing the CSA MC UI is 1024x768. For optimal viewing of the CSA MC UI, you should set your display to a resolution of 1280x600 or higher.

- On a system where CSA MC has never been installed, the CSA MC setup program first installs Microsoft SQL Server Express and the required .NET environment. If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express, 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 servers and desktop systems, the requirements are as follows:

Table 1-2 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 Vista Business and Enterprise editions with service pack 0 or 1. Windows Server 2003 (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, 2, or 3. Windows Embedded Point of Service (WEPOS) 1.1 Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4 <p>Note Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000.</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. See Internationalization and Localization Support, page 23 for a full explanation of language support.
Memory	256 MB minimum—all supported Windows 2003, Windows XP, and Windows 2000 platforms 512 MB minimum—for Windows Vista.

System Component	Requirement
Hard Drive Space	60 MB or higher Note This includes program and data.
Network	Ethernet 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 1-3 Agent Requirements (Solaris)

System Component	Requirement
Processor	UltraSPARC 400 MHz or higher Note Uni-processor, dual processor, and quad processor systems are supported.

System Component	Requirement
Operating Systems	<p>Solaris 9, 64 bit, patch version 111712-11 or higher installed.</p> <p>Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.)</p> <p>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.</p>
Memory	256 MB minimum
Hard Drive Space	<p>50 MB or higher</p> <p>Note This includes program and data.</p>
Network	<p>Ethernet</p> <p>Note Maximum of 64 IP addresses supported on a system.</p>



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 1-4 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 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 V6.0 from previous versions of CSA MC. Please refer to the Installation Guide for details.

Internationalization and Localization Support

This section describes the localization of Cisco Security Agent on various Windows operating systems and the compatibility of Cisco Security Agent with various Windows operating systems running in different languages.

Localization Support for Cisco Security Agents

All Cisco Security Agent kits contain **localized** support for English, French, German, Italian, Japanese, Korean, Simplified Chinese, Spanish, Polish, Brazilian Portuguese and Russian language native desktops and Multilingual User Interface (MUI) desktops. This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and agent help system will appear in the language of the end user's native operating system language or MUI language desktop.

The localized languages above have been **tested**, and are **supported** on these operating systems:

- Windows 2000 Professional, SP4
- Windows XP Professional, SP3
- Windows 2003 Server, SP3
- Vista Enterprise, SP1

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 having a localized agent. Support for a localized operating system means that Cisco Security Agent can run on that localized version of an operating system even though CSA is not presented in the same language as the localized operating system. In this case, the dialogs will appear in U.S. English.**

The tables below define the operating system support, not agent language support.



Note

For Multilingual User Interface (MUI) systems, installation screens, the CSA MC user interface, and dialog boxes can be displayed in any of the MUI languages we support: Chinese (Simplified), French, German, Italian, Japanese, Korean, Polish, Brazilian Portuguese, Spanish, or Russian.

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

The following terms are used to describe the level of support:

- **Localized (L):** Cisco Security Agent kits contain localized support for the languages identified. This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system appear in the language of the end user's desktop.
- **Tested (T):** The Cisco Security Agent was tested on these language platforms. Cisco Security Agent drivers are able to interpret the local characters in file paths and registry paths.
- **Supported (S):** The English version interface of Cisco Security Agent is suitable to run on these language platforms. The localized characters are supported by all agent functions.
- **Not applicable (NA):** Microsoft does not ship this combination
- **Not supported (NS):** Not supported

Look at the entry for Chinese (Simplified) in [Table 1-5](#). For Windows 2000 Professional with Service Pack 4, Cisco Security Agent has been localized (L) for Simplified Chinese, Cisco Security Agent has been tested (T) on the operating system, and Cisco Security Agent is supported (S) for use with the operating system.

Table 1-5 Windows 2000 Support

	Professional, SP4	Server	Advanced Server
Arabic	NS	NA	NA
Chinese (Simplified)	L, T, S	L, S	L, S
Chinese (Simplified) (MUI)			
Chinese (Traditional)	T, S	S	S
Chinese (Traditional) (MUI)			
Czech	S	S	NA
Danish (Native OS)	T, S	NA	NA
Danish (MUI)			
Dutch	S	S	NA
English (Canadian)	T, S	S	S
English (UK)	T, S	S	S

	Professional, SP4	Server	Advanced Server
English (US)	L, T, S	L, S	L, S
Finnish	S	NA	NA
French	L, T, S	L, S	L, S
French (MUI)			
French (Canadian)	T, S	S	S
French (Canadian) (MUI)			
German	L, T, S	L, S	L, S
German (MUI)			
Greek	S	NA	NA
Hebrew	T, S	NA	NA
Hebrew (MUI)			
Hungarian	S	S	NA
Italian	L, T, S	L, S	NA
Italian (MUI)			
Japanese	L, T, S	L, S	L, S
Japanese (MUI)			
Korean	L, T, S	L, S	L, S
Korean (MUI)			
Norwegian	S	NA	NA
Polish	L, T, S	L, S	NA
Polish (MUI)			
Portuguese (Brazilian)	L, T, S	L, S	NA
Portuguese (Brazilian) (MUI)			
Russian	L, T, S	L, S	NA
Russian (MUI)			
Spanish	L, T, S	L, S	L, S
Spanish (MUI)			

	Professional, SP4	Server	Advanced Server
Swedish	S	S	NA
Turkish	S	S	NA

Table 1-6 Windows XP Support

	Professional, SP3	Home
Arabic	NS	NS
Chinese (Simplified)	L, T, S	L, S
Chinese (Simplified) (MUI)		
Chinese (Traditional)	T, S	S
Chinese (Traditional) (MUI)		
Chinese (Hong Kong)	S	S
Czech	S	S
Danish	T, S	S
Danish (MUI)		
Dutch	S	S
English (Canadian)	T, S	S
English (UK)	T, S	S
English (US)	L, T, S	L, S
Finnish	S	S
French	L, T, S	L, S
French (MUI)		
French (Canadian)	T, S	S
French (Canadian) (MUI)		
German	L, T, S	L, S
German (MUI)		
Greek	S	S

	Professional, SP3	Home
Hebrew	T, S	NS
Hebrew (MUI)		
Hungarian	S	S
Italian	L, T, S	L, S
Italian (MUI)		
Japanese	L, T, S	L, S
Japanese (MUI)		
Korean	L, T, S	L, S
Korean (MUI)		
Norwegian	S	S
Polish	L, T, S	L, S
Polish (MUI)		
Portuguese (Brazilian)	L, T, S	L, S
Portuguese (Brazilian) (MUI)		
Russian	L, T, S	L, S
Russian (MUI)		
Spanish	L, T, S	L, S
Spanish (MUI)		
Swedish	S	S
Turkish	S	S

Table 1-7 Windows 2003 Support

	Standard, SP2	Web	Enterprise
Chinese (Simplified)	L, T, S	L, S	L, S
Chinese (Simplified) (MUI)			
Chinese (Traditional)	T, S	S	S
Chinese (Traditional) (MUI)			
Chinese (Hong Kong)	S	S	S

	Standard, SP2	Web	Enterprise
Czech	S	S	S
Danish	T, S	S	S
Danish (MUI)			
Dutch	S	NA	NA
English (Canadian)	T, S	S	S
English (UK)	T, S	S	S
English (US)	L, T, S	L, S	L, S
French	L, T, S	L, S	L, S
French (MUI)			
French (Canadian)	T, S	S	S
French (Canadian) (MUI)			
German	L, T, S	L, S	L, S
German (MUI)			
Hebrew (Native)	T, S	S	S
Hebrew (MUI)			
Hungarian	S	S	S
Italian	L, T, S	L, S	L, S
Italian (MUI)			
Japanese	L, T, S	L, S	L, S
Japanese (MUI)			
Korean	L, T, S	L, S	L, S
Korean (MUI)			
Norwegian	S	S	S
Polish	L, T, S	L, S	L, S
Polish (MUI)			
Portuguese (Brazilian)	L, T, S	L, S	L, S
Portuguese (Brazilian) (MUI)			

	Standard, SP2	Web	Enterprise
Russian	L, T, S	L, S	L, S
Russian (MUI)			
Spanish	L, T, S	L, S	L, S
Spanish (MUI)			
Swedish	S	S	S
Turkish	S	S	S

Table 1-8 Windows Vista Support

	Standard	Web	Enterprise, SP1
Chinese (Simplified)	L, S	L, S	L, T, S
Chinese (Simplified) (MUI)			
Chinese (Traditional)	S	S	T, S
Chinese (Traditional) (MUI)			
Chinese (Hong Kong)	S	S	S
Czech	S	S	S
Danish	S	S	T, S
Danish (MUI)			
Dutch	S	NA	S
English (Canadian)	S	S	T, S
English (UK)	S	S	T, S
English (US)	S, L	S, L	L, T, S
French	L, S	L, S	L, T, S
French (MUI)			
French (Canadian)	S	S	T, S
French (Canadian) (MUI)			
German	L, S	L, S	L, T, S
German (MUI)			

	Standard	Web	Enterprise, SP1
Hebrew	S	S	T, S
Hebrew (MUI)			
Hungarian	S	S	S
Italian	L, S	L, S	L, T, S
Italian (MUI)			
Japanese	L, S	L, S	L, T, S
Japanese (MUI)			
Korean	L, S	L, S	L, T, S
Korean (MUI)			
Norwegian	S	S	S
Polish	L, S	L, S	L, T, S
Polish (MUI)			
Portuguese (Brazilian)	L, S	L, S	L, T, S
Portuguese (Brazilian) (MUI)			
Russian	L, S	L, S	L, T, S
Russian (MUI)			
Spanish	L, S	L, S	L, T, S
Spanish (MUI)			
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.

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 9 *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 10 *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 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, Windows 2003, or Vista 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.

If Cisco Security Agent is uninstalled, the Windows Firewall is automatically re-enabled.

Windows Safe Mode

The Cisco Security Agent drivers do not load when systems are booted in Safe Mode. Therefore, the agent enforces no security in safe mode. This is done to allow the agent to be uninstalled if a system failure occurs and the system cannot be booted normally due to the agent.

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. Running of mobile code of any kind is not 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 11 provides information on known issues found in this release.

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsm25996	CSA AV does not provide protection against a quarantined virus if CSA is stopped or disabled.	<p>Symptom Quarantined Virus files are no longer quarantined by CSA.</p> <p>Conditions This occurs when CSA is disabled or stopped.</p> <p>Workaround Before stopping or disabling CSA, delete the quarantined virus files.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsm59209	Unknown Process listed in Event Log	<p>Symptom Sometimes when a NACL event is triggered, the process is listed as Unknown Process in the Event Log.</p> <p>Conditions This is observed only on On Vista Business and Enterprise editions when the process is meeting place.</p> <p>Workaround There is no known workaround.</p>
CSCsm74013	Norton Internet Security unusable after default desktop install	<p>Symptom After installing the default desktop agent kit, Norton Internet Security stops responding completely. Uninstalling CSA returns Norton to being fully functional.</p> <p>Conditions Host with Windows XP Home operating system and Norton Internet Security 2006.</p> <p>Workaround This problem is not seen in Norton version 2008 with the latest updates.</p>
CSCso27228	Group name field in Simple Mode does not support unicode characters.	<p>Symptom When using the deployment wizard, it is not possible to create a Group name with unicode characters</p> <p>Conditions This behavior is observed only in Simple Mode.</p> <p>Workaround Use Advanced Mode to create group names with Unicode characters.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCso27397	AntiVirus and Data Loss Prevention detail and non-detail reports may not report all files.	<p>Symptom There are discrepancies in Non-detailed and detailed Clam AntiVirus and Data Loss Prevention (DLP) reports.</p> <p>When an on-demand AntiVirus scan or background scan reports high number of infected files or files with DLP tags in a short time span, these events are suppressed and scan event logs are not generated for all these files.</p> <p>Conditions In AntiVirus and DLP detailed reports, information about only those files which are reported through Scan Event Log rule are provided.</p> <p>Workaround There is no workaround.</p>
CSCso63265	Closing command window during CSA 5.2 migration to CSA 6.0 causes the migration to fail.	<p>Symptom If you close the command window, during data migration, migration fails and you receive the message “Unable to find XML file to import to Management Center”.</p> <p>Conditions On a server with a 5.2 MC installed, during the 6.0 CSA MC installation</p> <p>Workaround There is no known workaround.</p>
CSCso73395	If a time of day is entered along with a date range, the time is rounded to 00:00:00 hours for the start date and 23:59:59 for the end date.	<p>Symptom In ClamAV reports, we round off the time entered by the user. For start date we round to 00:00:00 and End Date we round to 23:59:59</p> <p>Conditions When a time is entered along with a date.</p> <p>Workaround There is no known workaround</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCso85122	Static tags are not dropped on deletion of files with static tags	<p>Symptom Static tags are not dropped when files with static tags are deleted.</p> <p>Conditions This occurs when the files with static tags are moved to recycle bin.</p> <p>Workaround Permanently deleting the files with shift+delete keystroke will cause the tags to be dropped.</p>
CSCso87621	Data Scan on CLOSE event is misleading, the event shows results from previous scan.	<p>Symptom Event with the tag is not sent to the CSA MC Event log immediately but is queued and sent after a second scan.</p> <p>Conditions When a Data Scan on CLOSE set action is defined for a set of files. File is scanned and then the tag is removed and the file is rescanned.</p> <p>Workaround There is no known workaround.</p>
CSCsq01453	Cannot update Vista operating system to SP1.	<p>Symptom Installation of Vista SP1 fails and leaves the system in an unstable state.</p> <p>Conditions User updates Vista system to service pack 1 while CSA is installed.</p> <p>Workaround It is recommended that customers stop the agent when they are performing operating system updates.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsq42449	File got an additional static tag when tag configuration changed.	<p>Symptom Files show an additional static tag when tag configuration is changed.</p> <p>Conditions When a file already has a static tag applied, new static tags are applied, and the file is renamed.</p> <p>Workaround Resetting Cisco Security Agent will remove the old static tags.</p>
CSCsq50362	Clicking View Reports saves changes to the report.	<p>Symptom When viewing a report configuration page, clicking View Reports saves any changes to the report and displays the new report.</p> <p>Conditions If you choose to view default reports and make some changes to options and select the View Reports page.</p> <p>Workaround Clone the reports provided with the release and edit only the cloned versions. This preserves the default settings of the provided reports.</p>
CSCsq57852	Service restart rule enforces action when rule module is in Audit mode	<p>Symptom The service restart rule is enforced.</p> <p>Conditions The rule is in audit mode.</p> <p>Workaround There is no known workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsq73155	“Installation outdated” message for ClamAV is shown in freshclamlog.txt. This message does not mean that the signature updated has failed.	<p>Symptom A warning is logged:</p> <p>WARNING: Your ClamAV installation is OUTDATED!</p> <p>WARNING: Current functionality level = 29, recommended = 31</p> <p>DON'T PANIC! Read http://www.clamav.net/support/faq</p> <p>Database updated (315253 signatures) from db.local.clamav.net (IP: 64.142.100.50)</p> <p>Conditions When agent tries to update the Clam AntiVirus signatures, a warning is logged in freshclamlog.txt Version bundled with CSA 6.0 is Clam AV 0.93, whereas the one on Clam AV website is 0.93.1.</p> <p>Workaround There is no known workaround.</p>
CSCsq73373	Application deployment product association showing wrong product information.	<p>Symptom Application deployment product association lists software that has been uninstalled.</p> <p>Conditions All conditions.</p> <p>Workaround There is no known workaround.</p>
CSCsq73787	Skype crashes with CSA installed.	<p>Symptom Skype crashes with CSA installed</p> <p>Conditions Vista machines only.</p> <p>Workaround No known workaround</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsq75853	Users do not receive queries when copies of rules are in protect mode and learn mode.	<p>Symptom Users do not receive queries when copies of rules are in protect mode and learn mode. CSA acts assuming the default answers to the queries.</p> <p>Conditions This may happen when the same rules with query action are in both learn mode and protect mode, the learn mode may fire first.</p> <p>Workaround There is no known workaround.</p>
CSCsq90230	When installing CSA on “Host A,” from a remote desktop on “Host B,” the CSA installation reboot message fails to appear on “Host A.”	<p>Symptom The user of a remote desktop will not see the CSA installation reboot message.</p> <p>Conditions This occurs only when CSA is installed using remote desktop.</p> <p>Workaround There is no known workaround.</p>
CSCsq96130	A file in quarantine as well as a member of the White List results in ambiguity.	<p>Symptom You can see the file both in the quarantine list as well as in white list, and the file is quarantined and not “white-listed.”</p> <p>Conditions You have a rule that globally quarantines the file, and you add the file in the white list.</p> <p>Workaround The rules that apply to quarantine files are high priority denies and take precedence over the rules governing files on the white list. Remove the file from quarantine list and it will be subject to the rules of the white list.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsq99914	Zipping large files take a long time to complete.	<p>Symptom Zipping a large set of files (e.g. a vmware image) takes longer with CSA on than with CSA off.</p> <p>Conditions Zipping a large set of files when Data Loss Prevention functionality is enabled.</p> <p>Workaround There is no known workaround.</p>
CSCsr00872	Network portscan correlated - CSA MC sends initial polling hint to agents.	<p>Symptom CSAMC reports a network scan.</p> <p>Conditions If the initial agent kit is built without the polling hint enabled, the agent will not be listening on port 5401.</p> <p>When the polling hint is enabled on the CSA MC and rules are generated, the CSA MC will issue a polling hint to the agents in that group. The agent interprets it as a port scan.</p> <p>Workaround There is no known workaround.</p>
CSCsr01598	Incorrect data in Data Discovery report	<p>Symptom When the data discovery report is grouped by Host Name, all the newly created scanning tags with the same name, but different description, will be listed.</p> <p>When the data discovery report is grouped by Tag Name, multiple entries for the same host are listed.</p> <p>Conditions This happens when you have multiple scanning data tags with the same name.</p> <p>Workaround Give all scanning data tags a different name.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr02899	Wizard to Allow operation on rundll32 problem throws a CSA MC exception.	<p>Symptom When using the Event Management Wizard to allow an operation for a .dll, the wizard fails, logging an error in csalog.tx</p> <p>Conditions This happens when the .dlls have parameters present.</p> <p>Workaround There is no known workaround.</p>
CSCsr04675	Cached responses block messages after Log All Deny is enabled.	<p>Symptom Turning on “Log All Deny” does not clear the agent state so that the next deny event is sent to the CSAMC event log.</p> <p>Conditions This happens only when group parameters are changed.</p> <p>Workaround There is no known workaround.</p>
CSCsr09081	Agent service control rule with set security level does not work as expected.	<p>Symptom Agent service control rule with Set Security Level set to Low and a clone of this rule with Set Security Level set to High was deployed on the agent machines. The log stated that the security level was set to High but the security level did not change from what it was previously. When the service is started again the security level is reset to Medium.</p> <p>Conditions On agents installed on Linux and Solaris operating systems.</p> <p>Workaround There is no known workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr09751	AntiVirus background scan executes when agent security is disabled.	<p>Symptom Background scans run on agent machine when the agent security is disabled. Any files tagged during this scan are no longer visible when agent security is enabled.</p> <p>Conditions Agent security is disabled before when an AntiVirus background scan is scheduled to run.</p> <p>Workaround There is no known workaround.</p>
CSCsr10317	Unprotected hosts report fails	<p>Symptom The unprotected hosts report generates too much data and the report generation fails.</p> <p>Conditions All conditions.</p> <p>Workaround Configuring report to display in HTML limits size of report and the report is generated.</p>
CSCsr11301	DSCP marking not working in Audit Mode for Windows OS.	<p>Symptom NACL SET DSCP rules do not trigger in Audit mode. Packets are not marked with the DSCP values requested.</p> <p>Conditions Only observed when rule is in Audit mode on Windows OS.</p> <p>Workaround There is no known workaround.</p>
CSCsr14000	Token: @csanode special token is not working.	<p>Symptom Hosts running CSA are not tagged as csanodes. Using this special token in NACL rule has no effect.</p> <p>Conditions On Windows platforms, with NACL rule referencing the csanode special token.</p> <p>Workaround There is no known workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr17840	Application Control rules (APCR) and Network Access Control (NACL) rules do not work as expected in Learn Mode on Solaris.	<p>Symptom In Learn mode, APCR doesn't default to terminate process. NACL doesn't default to Deny.</p> <p>Conditions On Solaris Platforms, when the APCR and NACL rules are in learn mode.</p> <p>Workaround There is no known workaround.</p>
CSCsr18162	Similar rules in Learn mode and Protect mode; Learn mode rules triggered.	<p>Symptom When there are two rule modules with similar rules, and one rule module is in learn mode and one is in protect mode, the rules from the rule module in Learn Mode are triggered, instead of the one in Protect mode.</p> <p>Conditions On Solaris platforms, when rules are in both learn and protect mode.</p> <p>Workaround There is no known workaround.</p>
CSCsr22650	E-mail alert misleading - rule ID points to no log allow and not monitor.	<p>Symptom When an email alert is generated from a monitor rule, the message points to the cover rule such as no log allow rather than the monitor rule.</p> <p>Conditions When email alert used and a monitor rule is triggered.</p> <p>Workaround There is no known workaround.</p>
CSCsr22768	Blank application name in target application for modify memory by PSXSS.EXE	<p>Symptom The target field in an APCR is blank.</p> <p>Conditions PSXSS.EXE is the application in an APCR rule.</p> <p>Workaround There is no known workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr23344	Data Loss Prevention notify events on CSA MC do not consistently identify the resource accessed.	<p>Symptom The DLP rule “Applications recently reading Proprietary Data and White List, client for TCP and UDP services with external hosts” shows blank resource name.</p> <p>Conditions All conditions.</p> <p>Workaround There is no known workaround.</p>
CSCsr23551	Agent GUI shutdown confirmation query confusing.	<p>Symptom Selecting OK in the agent UI shutdown query does not shutdown the agent.</p> <p>Conditions Agent shutdown is attempted and wrong options are chosen.</p> <p>Workaround To successfully shut down the agent: select the “yes” radio button, type justification, and click OK.</p>
CSCsr29061	Wireless: Prevent Wireless connectivity if Ethernet is active.	<p>Symptom With a policy that attempts to prevent wireless connectivity if Ethernet connectivity is active, attempting to run a TCP Server on the machine, the wireless access is denied. The wired access is also denied for a minute.</p> <p>Once it is accepted, subsequent wireless attempts are allowed.</p> <p>Also all subsequent wireless connections are accepted if connection to wired interface is attempted first for both TCP and UDP Servers.</p> <p>Conditions On Vista platform, with “Block Wireless bridging” attached to the agent group.</p> <p>Workaround The caching timeout causes wired access to be denied. Wait for one minute before attempting connectivity through the wired interface.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr31984	If a driver is identified by CSA as malicious, and CSA does not include the path to the driver in the event it reports, an exception rule that does identify the path to the driver will not have effect.	<p>Symptom If an exception is created to add a driver to the white list, and the full path is given in the exception, but the original event never indicated the full path to the driver, the exception does not trigger.</p> <p>Conditions Logged rule has only the file name not the full path name.</p> <p>Workaround There is no known workaround.</p>
CSCsr39583	Multiple issues with Application Deployment Reports.	<p>Symptom Application deployment reports show these symptoms:</p> <ul style="list-style-type: none"> • Do not find Clam as an AV on the host machine. • Install products reports displays both “Generic Windows Operating System” and the actual operating system name in the list of programs. • Network data flows reports pick up freshclam.exe traffic to/from the CSA MC • Network Server Applications reports do not appear to work at all on any platform. <p>Conditions Application Deployment Reports run with the latest CSA 6.0 agents.</p> <p>Workaround There is no known workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr39721	Reports displayed in HTML do not print correctly.	<p>Symptom Various printing issues with reports displayed in HTML.</p> <ol style="list-style-type: none"> 1. Printing All pages will only print the current page. 2. Printer default is set to portrait, and if the report is formatted in landscape, all text is cropped. 3. Cannot specify a range of pages to print or specify a single page. 4. Nothing is spooled to the printer. <p>Conditions Reports in HTML display mode, attempting to print.</p> <p>Workaround Use PDF display mode.</p>
CSCsr39832	MSI installation of browser plugin / DLL was not detected	<p>Symptom The rule module - “Security - User running Untrusted install app” doesn’t provide an alert to the installation of a DLL into a running browser.</p> <p>Conditions Install a browser plugin with the Security – User Running Untrusted install app” rule module enabled.</p> <p>Workaround There is no known workaround.</p>
CSCsr41294	DLP classification tag not consistently reported in events.	<p>Symptom Events from DLP rules do not show consistent data classification information for same user and same process ID.</p> <p>Conditions Two different events happens after at least a minutes interval.</p> <p>Workaround There is no known workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr45854	Allow deletion of a scanning tag if another with same name exists.	<p>Symptom When two scanning tags are present with the same name, one is in use and the other is not in use, the user is not allowed to delete the scanning tag which is not in use.</p> <p>Conditions When two scanning tags of the same names are present, and one is in Use.</p> <p>Workaround Give all scanning data tags a different name.</p>
CSCsr51036	No way to check which Set rule triggered a user-defined system state.	<p>Symptom The “System State” link in the event log does not have an option to determine which rule triggered the system state.</p> <p>Conditions On all Windows platforms where rule modules for tagging static tags are deployed.</p> <p>Workaround There is no known workaround.</p>
CSCsr52901	DLP False Positives: INDEX.BTR files reported to have 1000+ SSNs	<p>Symptom Data Loss Prevention Reports 1000+ Social Security Numbers for the INDEX.BTR file.</p> <p>Conditions Hosts running Windows operating systems.</p> <p>Workaround There is no known workaround.</p>
CSCsr53644	Reset Custom System State not working.	<p>Symptom When a reset of Cisco Security Agent is attempted, the custom system states are not cleared.</p> <p>Conditions When multiple custom system states are triggered.</p> <p>Workaround There is no workaround.</p>

Table 11 Known Issues in Cisco Security Agent 6.0

Bug ID	Summary	Explanation
CSCsr54192	SOFTWARE_UPDATE_PROMPT_FAIL needs better retry mechanism	<p>Symptom Prompt for software update is attempted before user logs in. Due to absence of GUI, it is deferred till the next poll.</p> <p>Even when software update is available, agent UI shows no update pending.</p> <p>Conditions When user is not logged on.</p> <p>Workaround There is no workaround.</p>
CSCsr57820	Firefox add-on download/installation not detected with default Desktop policy.	<p>Symptom When Google toolbar is download for Firefox, the user does not receive a query.</p> <p>Conditions Agent installation on Windows XP SP3.</p> <p>Workaround There is no known workaround.</p>
CSCsr59075	Background scan results are often out-of-date	<p>Symptom The Data Loss Prevention (DLP) background scans report an earlier date than actual date of start.</p> <p>Conditions When DLP Background scans are configured.</p> <p>Workaround There is no known workaround.</p>
CSCsr65094	An infected .zip file gets removed from quarantined files list after a signature update	<p>Symptom A quarantined .zip file is removed from the quarantine list. It is restored to the system but not listed as “Restored.”</p> <p>Conditions When the zip file has been quarantined as a result of an on demand scan, and an AntiVirus signature update occurs.</p> <p>Workaround There is no workaround.</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>

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)

Copyright © 2010, Cisco Systems, Inc.
All rights reserved.

