Release Notes for Management Center for Cisco Security Agents 6.0.1

Revision Date: March 9, 2010

Part Number: OL-18679-01

Management Center for Cisco Security Agents (CSA MC) 6.0.1 contains new features and improves on the CSA 6.0 release.

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

New Features

CSA 6.0.1 contains many new features and enhances the functionality of CSA 6.0. For a complete understanding of all the new features delivered in both the CSA 6.0 and CSA 6.0.1 releases, see the **New Features** section of the Release Notes for Management Center for Cisco Security Agents 6.0 in addition to these new feature descriptions.

CSA MC High Availability Solution

The Management Center for Cisco Security Agents (CSA MC) high availability solution uses a primary and secondary CSA MC to provide agents with maximum access to a Management Center. Generally, Cisco Security Agents (agents) communicate with CSA MC when it is in the “reachable” system state. When the CSA MC is not reachable, the agents will not send events, receive software upgrades, or receive policy updates. The CSA MC may not be reachable for many reasons including scheduled upgrades, network connectivity issues, the CSA MC service has been stopped, or there has been a server outage.

The current method of recovering from a down CSA MC is to create a secondary CSA MC, keeping it offline, with same name and IP address as primary CSA MC, copy all SSL certificates from the primary to the secondary CSA MC, export all data from the primary CSA MC, import the data to the secondary CSA MC, shutdown the primary CSA MC, and start the secondary CSA MC. This is a very time consuming process during which agents have no access to a CSA MC.

With the CSA MC HA solution, the secondary CSA MC is ready to take over for the primary CSA MC as soon as it is needed. The primary CSA MC does not need to have network connectivity in order for this switch-over to occur. When the primary CSA MC is ready to resume its role, it connects to the network and it begins to act as the primary once again.

The high availability solution is fully described in *Management Center for Cisco Security Agents High Availability White Paper:*
http://www.cisco.com/en/US/docs/security/csa/csa601/white_papers/Management_Center_for_Cisco_Security_Agent_High_Availability_White_Paper.pdf

CSA MC on a Virtual Machine

Administrators can create a VMware™ image of the Management Center for Cisco Security Agents (CSA MC) and maintain it on the VMware ESXi 3.5 hypervisor.

This virtual CSA MC has the same features and performs the same functions of any CSA MC installed on its own physical machine:

- The virtual CSA MC must meet all the requirements for a CSA MC as described in System Requirements, page 20.
- Administrators can manage hosts using a virtual CSA MC.
- A virtual CSA MC can be installed along with the Microsoft SQL Server Express database.
- One or two virtual CSA MCs can work with a remote Microsoft SQL Server 2005 (or 2000) database.
- Virtual CSA MCs can be used in a High Availability solution described in *Management Center for Cisco Security Agents High Availability White Paper.*

VMware is a registered trademark of VMware, Inc.

Expanded Platform Support

Cisco Security Agents can now be installed on these platforms:

- Red Hat Enterprise Linux 5.0
- Solaris 10
- SUSE Linux 10

Management Summary Reports

Management Summary reports are designed to provide administrators with the information they need most often. They are brief targeted reports, no more than a page in length.

The reports can be generated in HTML or in PDF formats. These are the Management Summary Reports provided with this release:

- **Daily Events by Event Type**. Use this report to view trends in the number of triggered events, from different types of rules, over time.
- **Events by Enforcement Action Over Time**. Use this report to view trends in the number and type of enforcement actions reported throughout your deployment.
- **Host Count Summary**. Use this report to see total numbers of hosts reporting different statuses, broken down by group and operating system.
- **Queried Events by Response Type Over Time**. Use this report to view trends in the number and type of user responses to queries reported throughout your deployment.

- **Summary of Queried Events by Response Type Over Time**. Use this report to view total numbers and types of user responses to queries reported throughout your deployment.
- **Summary of Events by Enforcement Action**. Use this report to view total numbers and types of enforced actions reported throughout your deployment.
- **Top 20 Infected Hosts**. Use this report to view the 20 hosts infected with the most number of viruses, found by CSA AV, throughout your CSA deployment. The report could include signature-based viruses, behavior-based viruses, and Potentially Unwanted Applications (PUAs).
- **Top 20 Identified Viruses**. Use this report to view the 20 most frequently occurring viruses, found by CSA AV, throughout your CSA deployment. The report could include signature-based viruses, behavior-based viruses, and Potentially Unwanted Applications (PUAs).

"My Custom" Components

Policies, rule modules, and file sets labeled with "My Custom" are exposed to administrators in order to make customizations of CSA deployments easier.

The "My Custom" rule modules give users easily recognizable locations for specialized rules created for their deployments. Rules placed in the "My Custom" rule modules immediately become included in their corresponding "My Custom" policy.

Here is an example of how a "My Custom" rule module and a "My Custom" policy could be used. If an administrators needs to create a custom rule for the Windows Desktops group, and cannot do so through an event exception or by adding an application to the "white list," then the administrator could create a rule in the "My Custom Module for Windows Desktops" rule module. My Custom Module for Windows Desktops is already a member of "My Custom Policy for Windows Desktops" policy. After the administrator assigns the My Custom Policy for Windows Desktops to a group, moves hosts into that group, and generates rules, CSA MC distributes the customized rules to the hosts in the group.

Two "My Custom" file sets have also been added to this release:

- My Custom Executables - Backup tools
- My Custom Software Distribution and Inventory

These file sets are visible, writable, and are marked as requiring customization.

The "My Custom Executables - Backup tools" file set is already a member of the Windows "Backup Applications" application class. That application class is already used by several rules, some of which are deployed through the <All Window> group. Adding your custom backup tool to the My Custom Executables - Backup tools file set ensures that all Windows users will treat the custom backup tool the way they treat other, more common, backup tools.

The same kind of example would apply if an enterprise uses a software distribution tool other than Microsoft's System Management Server or Symantec's Altiris. Specifying that alternative software distribution tool in the "My Custom Software Distribution and Inventory" file set automatically makes it part of application classes, used in rules, that are distributed to hosts in the <All Windows> group.

Note After an upgrade or a migration, when comparing the contents of the Base Security policies, look for the insertion of the "My Custom" components in the new versions of these policies.

Digital Signature Identification

CSA now identifies digitally signed files. Once these files are identified, they can become "trusted." CSA does not restrict trusted files as much as it does "untrusted" files.

This feature makes downloading and installing applications with trusted digital signatures easier. If end users download an application from the Internet, and it is digitally signed, and that signature is defined as coming from a trusted source, the user receives fewer messages and warnings from CSA during the entire process.

There are new components delivered with this release which implement this feature. The **Good Digital Signers** file set stores the list of trusted digital signatures. The **Base - Digital Signatures for Downloaded Executables** rule module contains the rules that identify the digital signature and classify the file as "trusted." This rule module is part of the **Base - Basic Application Classification** policy which is delivered to members of the **<All Windows>** group. The Good Digital Signers file sets comes pre-loaded with several digital signatures, so this feature will benefit Windows users as soon as the agent kits are deployed.

Scheduling Software Update Wizard

The wizard steps administrators through the process of scheduling a software update and automatically generates rules at the end of the process. The Scheduling Software Update Wizard is available for Simple Mode and Advanced Mode users.

Issues Resolved by this Release

The following table provides a list of defects that were reported in CSA 6.0 and are resolved by this release.

Table 1 Issues Resolved by CSA 6.0.1 Release

Bug ID	Summary	Resolution
CSCso63265	Closing command window during CSA 5.2 migration to CSA 6.0 causes the migration to fail.	We now add an indication in the command window that something is running and minimize the command window so users are less inclined to close it.
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.	Reports now allow for specifying a specific start and end time along with the start and end date.
CSCso85122	Static tags are not dropped on deletion of files with static tags	When the agent starts up, the static tag entry is dropped if the file does not exist. On deletion (move to recycle bin) static tags must not be dropped off the files that were statically tagged. The delete operation is considered as a file rename and hence the static tag for the file must be retained with the new path for the file.

Bug ID	Summary	Resolution
CSCsq50362	Clicking **View Reports** saves changes to the report.	Clicking View Reports no long saves changes to reports. This maintains the default report settings.
CSCsq73155	"Installation outdated" message for ClamAV is shown in freshclamlog.txt. This message does not mean that the signature updated has failed.	The message to the user is suppressed to avoid to confusion that the signature update has failed when it has not.
CSCsq73787	Skype crashes with CSA installed.	Skype no longer crashes when CSA is installed.
CSCsq99914	Zipping large files take a long time to complete.	Changed data scanning methods for .zip files.
CSCsr09081	Agent service control rule with set security level does not work as expected.	The agent now "remembers" its configured security level when it is disabled. When the agent is re-enabled, it is operating at the correct security level.
CSCsr09751	AntiVirus background scan executes when agent security is disabled.	Background scans no longer run on agent machine when the agent security is disabled.
CSCsr29061	Wireless: Prevent Wireless connectivity if Ethernet is active.	CSA accepts ethernet connections quickly and blocks wireless connection while there is an ethernet connection.
CSCsr41294	DLP classification tag not consistently reported in events.	Events from DLP rules show consistent data classification information for same user and same process ID.

Product Notes

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

- **Issue**: When 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**: Any customized global report configuration settings revert to the default global report configurations following an upgrade. This ensures report generation using the latest release.

  Solution: Reconfigure global report configuration settings with your customized settings after the upgrade. See “Report Configuration” in the CSA MC help.

Known Issues

Table 2 provides information on known issues found in this release.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsm25996	CSA AV does not provide protection against a quarantined virus if CSA is stopped or disabled.	**Symptom** Quarantined Virus files are no longer quarantined by CSA. **Conditions** This occurs when CSA is disabled or stopped. **Workaround** Before stopping or disabling CSA, delete the quarantined virus files.
CSCsm59209	Unknown Process listed in Event Log	**Symptom** Sometimes when a NACL event is triggered, the process is listed as Unknown Process in the Event Log. **Conditions** This is observed only on On Vista Business and Enterprise editions when the process is meeting place. **Workaround** There is no known workaround.
CSCso27228	Group name field in Simple Mode does not support unicode characters.	**Symptom** When using the deployment wizard, it is not possible to create a Group name with unicode characters **Conditions** This behavior is observed only in Simple Mode. **Workaround** Use Advanced Mode to create group names with Unicode characters.
CSCso27397	AntiVirus and Data Loss Prevention detail and non-detail reports may not report all files.	**Symptom** There are discrepancies in Non-detailed and detailed Clam AntiVirus and Data Loss Prevention (DLP) reports. 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. **Conditions** In AntiVirus and DLP detailed reports, information about only those files which are reported through Scan Event Log rule are provided. **Workaround** There is no workaround.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsq01453	Cannot update Vista operating system to SP1.	**Symptom** Installation of Vista SP1 fails and leaves the system in an unstable state. **Conditions** User updates Vista system to service pack 1 while CSA is installed. **Workaround** It is recommended that customers stop the agent when they are performing operating system updates.
CSCsq42449	File got an additional static tag when tag configuration changed.	**Symptom** Files show an additional static tag when tag configuration is changed. **Conditions** When a file already has a static tag applied, new static tags are applied, and the file is renamed. **Workaround** Resetting Cisco Security Agent will remove the old static tags.
CSCsq57852	Service restart rule enforces action when rule module is in Audit mode	**Symptom** The service restart rule is enforced. **Conditions** The rule is in audit mode. **Workaround** There is no known workaround.
CSCsq73373	Application deployment product association showing wrong product information.	**Symptom** Application deployment product association lists software that has been uninstalled. **Conditions** All conditions. **Workaround** There is no known workaround.
CSCsq75853	Users do not receive queries when copies of rules are in protect mode and learn mode.	**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. **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. **Workaround** There is no known workaround.
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.”	**Symptom** The user of a remote desktop will not see the CSA installation reboot message. **Conditions** This occurs only when CSA is installed using remote desktop. **Workaround** There is no known workaround.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsq96130	A file in quarantine as well as a member of the White List results in ambiguity.	**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." **Conditions** You have a rule that globally quarantines the file, and you add the file in the white list. **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.
CSCsr00872	Network portscan correlated - CSA MC sends initial polling hint to agents.	**Symptom** CSAMC reports a network scan. **Conditions** If the initial agent kit is built without the polling hint enabled, the agent will not be listening on port 5401. 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. **Workaround** There is no known workaround.
CSCsr01598	Incorrect data in Data Discovery report	**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. When the data discovery report is grouped by Tag Name, multiple entries for the same host are listed. **Conditions** This happens when you have multiple scanning data tags with the same name. **Workaround** Give all scanning data tags a different name.
CSCsr02899	Wizard to Allow operation on rundll32 problem throws a CSA MC exception.	**Symptom** When using the Event Management Wizard to allow an operation for a .dll, the wizard fails, logging an error in csalog.tx **Conditions** This happens when the .dlls have parameters present. **Workaround** There is no known workaround.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsr10317	Unprotected hosts report fails	**Symptom** The unprotected hosts report generates too much data and the report generation fails. **Conditions** All conditions. **Workaround** Configuring report to display in HTML limits size of report and the report is generated.
CSCsr11301	DSCP marking not working in Audit Mode for Windows OS.	**Symptom** NACL SET DSCP rules do not trigger in Audit mode. Packets are not marked with the DSCP values requested. **Conditions** Only observed when rule is in Audit mode on Windows OS. **Workaround** There is no known workaround.
CSCsr14000	Token: @csanode special token is not working.	**Symptom** Hosts running CSA are not tagged as csanodes. Using this special token in NACL rule has no effect. **Conditions** On Windows platforms, with NACL rule referencing the csanode special token. **Workaround** There is no known workaround.
CSCsr17840	Application Control rules (APCR) and Network Access Control (NACL) rules do not work as expected in Learn Mode on Solaris.	**Symptom** In Learn mode, APCR doesn't default to terminate process. NACL doesn't default to Deny. **Conditions** On Solaris Platforms, when the APCR and NACL rules are in learn mode. **Workaround** There is no known workaround.
CSCsr18162	Similar rules in Learn mode and Protect mode; Learn mode rules triggered.	**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. **Conditions** On Solaris platforms, when rules are in both learn and protect mode. **Workaround** There is no known workaround.
CSCsr22650	E-mail alert misleading - rule ID points to no log allow and not monitor.	**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. **Conditions** When email alert used and a monitor rule is triggered. **Workaround** There is no known workaround.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsr22768	Blank application name in target application for modify memory by PSXSS.EXE	**Symptom** The target field in an APCR is blank. **Conditions** PSXSS.EXE is the application in an APCR rule. **Workaround** There is no known workaround.
CSCsr23344	Data Loss Prevention notify events on CSA MC do not consistently identify the resource accessed.	**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. **Conditions** All conditions. **Workaround** There is no known workaround.
CSCsr39583	Multiple issues with Application Deployment Reports.	**Symptom** Application deployment reports show these symptoms: • 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. **Conditions** Application Deployment Reports run with the latest CSA 6.0 agents. **Workaround** There is no known workaround.
CSCsr39721	Reports displayed in HTML do not print correctly.	**Symptom** Various printing issues with reports displayed in HTML. 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. **Conditions** Reports in HTML display mode, attempting to print. **Workaround** Use PDF display mode.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsr39832	MSI installation of browser plugin / DLL was not detected	**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. **Conditions** Install a browser plugin with the Security – User Running Untrusted install app" rule module enabled. **Workaround** There is no known workaround.
CSCsr45854	Allow deletion of a scanning tag if another with same name exists.	**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. **Conditions** When two scanning tags of the same names are present, and one is in Use. **Workaround** Give all scanning data tags a different name.
CSCsr51036	No way to check which Set rule triggered a user-defined system state.	**Symptom** The "System State" link in the event log does not have an option to determine which rule triggered the system state. **Conditions** On all Windows platforms where rule modules for tagging static tags are deployed. **Workaround** There is no known workaround.
CSCsr52901	DLP False Positives: INDEX.BTR files reported to have 1000+ SSNs	**Symptom** Data Loss Prevention Reports 1000+ Social Security Numbers for the INDEX.BTR file. **Conditions** Hosts running Windows operating systems. **Workaround** There is no known workaround.
CSCsr53644	Reset Custom System State not working.	**Symptom** When a reset of Cisco Security Agent is attempted, the custom system states are not cleared. **Conditions** When multiple custom system states are triggered. **Workaround** There is no workaround.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsr54192	SOFTWARE_UPDATE_PROMPT_FAIL needs better retry mechanism	**Symptom** Prompt for software update is attempted before user logs in. Due to absence of GUI, it is deferred till the next poll. Even when software update is available, agent UI shows no update pending. **Conditions** When user is not logged on. **Workaround** There is no workaround.
CSCsr57820	Firefox add-on download/installation not detected with default Desktop policy.	**Symptom** When Google toolbar is download for Firefox, the user does not receive a query. **Conditions** Agent installation on Windows XP SP3. **Workaround** There is no known workaround.
CSCsr59075	Background scan results are often out-of-date	**Symptom** The Data Loss Prevention (DLP) background scans report an earlier date than actual date of start. **Conditions** When DLP Background scans are configured. **Workaround** There is no known workaround.
CSCsr65094	An infected .zip file gets removed from quarantined files list after a signature update	**Symptom** A quarantined .zip file is removed from the quarantine list. It is restored to the system but not listed as “Restored.” **Conditions** When the zip file has been quarantined as a result of an on demand scan, and an AntiVirus signature update occurs. **Workaround** There is no workaround.
CSCsw19270	Data Leakage feature increases Social Security Number False Positives	**Symptom** Sometimes false positives social security numbers (SSN) are reported in security catalog files. **Conditions** This occurs when Data Loss Prevention policy is deployed and security catalog files are scanned. **Workaround** None.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsw96875	Management Summary reports do not report data if the result of the query that generated the report is zero.	**Symptom** If a user has specified a particular rule/enforcement/response type for a report, and the resulting count for the entire date range is 0, the data are not reported. **Conditions** Management summary reports that allow the user to select Rule Types, Enforcement Action, and Response Types. This issue is applicable only to following reports: • Daily Events by Event Type • Events by Enforcement Action Over Time • Queried Events by Response Type Over Time **Workaround** None
CSCsx81869	When a Data Access Control rule uses a data set, the rule does not honor the pattern matching “but not” field defined in the data set.	**Symptom** When a Data Access Control rule uses a data set, the rule does not honor the pattern matching “but not” field defined in the data set. **Conditions** This occurs only if DACL uses exceptions under data set. **Workaround** Create a second rule that specifies the data set exceptions to the initial rule. Give the second rule a higher than the initial rule, this overrides the initial rule’s data set and the exceptions will be made.
CSCsx94237	Monitor role user account has unrestricted access to view Management Summary reports.	**Symptom** A monitor role user with access control restrictions on which groups the user can view, will still be able to view complete Management Summary reports. **Conditions** Access control restrictions are applied to the monitor role user account **Workaround** None.
CSCsx96954	CSA installation causes windows registration requirement.	**Symptom** After install of CSA 6.0 agent kit, the user is prompted to enter the registration key for the device and register with microsoft. **Conditions** New CSA 6.0 agent kit install (upgrade from previous versions apparently unaffected) **Workaround** Enter registration key and register with MS. issue no longer seen.

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsx97196	Warning Message is displayed while loading CSA datafilter module for Apache 1.3 on Solaris.	**Symptom** After the CSA data filter is installed for Apache 1.3 and the Apache service is restarted, CSA displays this warning message: "Loaded DSO libexec/mod_csa32_apache1_3.so uses plain Apache 1.3 API, this module might crash under EAPI! (please recompile it with -DEAPI)" **Conditions** This occurs only when the CSA data filter is installed for Apache 1.3 on Solaris OS. **Workaround** None.
CSCsx97296	Data filter, once installed, cannot be uninstalled on Solaris machines	**Symptom** After the web server data filter is installed on Solaris, it cannot be uninstalled using the **i.csafilter** script. **Conditions** This occurs only when data filter is installed for Apache 1.3. **Workaround** Uncomment the data filter from Apache configuration file to prevent the CSA data filter from being loaded by Apache.
CSCsy35047	Many svchost related notifications after installing server agent kit.	**Symptom** After the server agent kit is installed, CSA displays many svchost related pop-up messages. **Conditions** This occurs when the server agent kit is installed on Windows Server 2003 Enterprise Edition system. The pop-ups are observed only after installation. **Workaround** None

Table 2 Known Issues in Cisco Security Agent 6.0.1

Bug ID	Summary	Explanation
CSCsy58166	After Agent installation, RHEL 4 Linux AS(Update 4) freezes on reboot.	**Symptom** After Agent installation, RHEL 4 Linux AS(Update 4) freezes on reboot. **Conditions** • HP xw4400 Workstation • nVidia Corporation Quadro FX 560 graphics card • check_nvidia_module service **Workaround** 1. Disable **check_nvidia_module** service at runlevel 5 and reboot the system. 2. When prompted, run X configuration program and specify VESA driver. Subsequent reboots do not cause any system freeze and the GUI came up without any problem.
CSCsy74583	CSA 6.0.0.220 causes Microsoft Outlook 2007 to crash upon closing.	**Symptom** With CSA 6.0.0.220 installed, Microsoft Outlook 2007 crashes when a user closes it. **Conditions** All. **Workaround** None
CSCsy79491	Rule generation fails after importing CSA 5.2 migration data	**Symptom** After importing the 5.2.0.272 migration data into the 6.0 CSA MC, the 6.0 CSA MC rule generation fails with the following error message: “Invalid application process class identifier "" “ **Conditions** When <*Processes Writing Untrusted Content> application class is used in a customized rule in CSA 5.2. **Workaround** Find all occurrences of <*Process Writing Untrusted Content> used in CSA 5.2 rules and rewrite the rules to use <*Process Executing Untrusted Content>. CSA 5.2 has these two built-in application classes: <*Process Writing Untrusted Content> and <*Process Executing Untrusted Content>. CSA 6.0 only has the <*Process Executing Untrusted Content> application class. Customized CSA 5.2, rules referencing <*Process Writing Untrusted Content> do not have a built-in application class to map to after the migration.

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 components 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.

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 is beneficial.

CSA 6.0.1 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.

Windows Policies and Groups

The majority of Windows policies provided in this release are intended to be used as they are. A short pilot program is always prudent but administrators should not have to perform much, if any, tuning of the Windows policies.

There a few Windows policies provided with this release that are labeled “Sample”. These policies are starting points and provide examples on how to allow benign behaviors safely while preventing malicious ones. Sample policies require testing and tuning in a pilot program.

Any Windows agent kit automatically includes the <All Windows> group. This group is deployed in live mode. The objectives of the policy in this group are to grant explicit permissions to allow basic operating system functions to run normally, and to place applications into application classes so that their behavior is interpreted correctly.

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

All Windows policies are visible in Advanced Mode, some windows policies are configured to be visible in Simple Mode. Policies visible in Simple Mode are displayed on the Host Security page. If the policy is relevant to desktops, it will be visible in any group intended for desktops. If the policy is relevant to servers, it will be visible in any group intended for servers.

Unix Policies and Groups

The UNIX policies delivered with this release are examples of how customers can write and organize rules in order to protect Linux or Solaris endpoints. Before deploying them throughout their organization, customers should test these policies and tune them during a pilot program.

There are several pre-configured UNIX groups included with this release. Any Solaris or Linux agent kits automatically include either the <All Solaris> or <All Linux> groups. These groups are deployed in live mode. The objectives of the policies in these groups are to grant explicit permissions to allow basic operating system functions to run normally, and to place applications into application classes so that their behavior is interpreted correctly.

There is a Sample Desktop group for Linux desktops and a Sample Servers groups for Linux and Solaris servers included in this release. These groups are marked Sample and they are configured to run in audit mode. These groups contain policies designed to prevent malicious behavior. As mentioned previously, the policies in these groups provide examples of how you to write rules, organize rule modules and policies in order to protect a server or a desktop.

The policies attached to the <All Solaris> and <All Linux> group do not provide any protection for the endpoint. Hosts must in the <All Solaris> or <All Linux> group and a desktop or server group in order to receive the proper balance of permissions and protections.

The UNIX policies are not visible to users looking at the CSA MC interface in Simple Mode, they are only visible to users viewing the CSA MC in Advanced Mode.

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."

CSA and Microsoft Windows Interaction

CSA MC System Default Policy and Windows Updates

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**.

Hotfixes for Windows 2003 R2 are not individually qualified for the CSA MC. When new service packs are available for Windows 2003 R2, their impact on the CSA MC is evaluated, appropriate updates are made to the product, and the CSA MC is qualified for that service pack. Support for Windows service packs is provided with a formal CSA hotfix or a scheduled release of the product.

Windows Firewall Disabled

The Cisco Security Agent automatically disables the Windows Vista, Windows XP, and Windows 2003 firewalls. 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

When a Windows operating system is booted in Safe Mode, CSA drivers are loaded but CSA does not perform any of its functions. If you are trying to diagnose the cause of a system failure, and you suspect CSA is involved, try one of these tests:

- Boot Windows in Safe Mode and leave CSA installed. If the system failure you experienced in Windows normal mode still occurs in Windows Safe Mode, you can eliminate CSA as the cause of the problem.
- Boot Windows in Safe Mode and uninstall CSA. Reboot Windows normally. If you still experience the system failure when you reboot Windows in normal mode, you can eliminate CSA as the cause of the problem.

System Requirements

CSA MC System Requirements

Note The acronym CSA MC is used to represent the Management Center for Cisco Security Agents.

Table 3 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* for more detailed information about scalable deployments.

Table 3 Minimum Server Requirements

System Component	Requirement
Hardware	• IBM PC-compatible computer • Color monitor with video card capable of 16-bit
Processor	1 GHz or faster Pentium processor
Operating System	Windows 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. The CSA MC may also be installed on a VMware image of a Windows 2003 R2 server, as described above, which is maintained on a VMware ESXi hypervisor. See "Virtual Machine Support," in Chapter 1 of *Installing Management Center for Cisco Security Agents* for more information.
File System	NTFS
Memory	1 GB minimum memory

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

- 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.

Agent Requirements for Windows Systems

These are the system requirements for running Cisco Security Agent on Windows servers and desktops:

Table 4 Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher **Note** Up to eight physical processors are supported.
Operating Systems	• 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 **Note** Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000. Supported language versions: For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported. See Internationalization and Localization Support, page 26 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.
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.

Agent Requirements for Solaris Systems

These are the system requirements for running Cisco Security Agent on Solaris servers:

Table 5 Agent Requirements (Solaris)

System Component	Requirement
Processor	UltraSPARC 400 MHz or higher **Note** Uni-processor, dual processor, and quad processor systems are supported.
Hardware	Sun4u for Solaris 8,9, and 10.
Operating Systems	• Solaris 10, 64 bit kernel, 6/06 edition or higher. Recommended Patch for Solaris 10: 120068-03: SunOS 5.10: in.telnetd Patch • Solaris 9, 64 bit, patch version 111712-11 or higher installed. • Solaris 8, 64 bit 12/02 edition or higher (This corresponds to kernel Generic_108528-18 or higher.) Recommended patch levels for Solaris 8: 108434-17 and 108435-17. **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 for Solaris 8 and 9 512 MB minimum for Solaris 10
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.

Agent Requirements for Linux Systems

These are the requirements for running Cisco Security Agent on Linux systems:

Table 6 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	• Red Hat Enterprise Linux 5.0 with Update 1 or Update 2. These operating system implementations are supported for the Desktop, Server, and Advanced Platform releases. Minimum supported kernel: 2.6.18 • Red Hat Enterprise Linux 4.0 WS, ES, or AS Minimum supported kernel: 2.6.9-11 • Red Hat Enterprise Linux 3.0 WS, ES, or AS Minimum supported kernel: 2.4.0 • SUSE Linux Enterprise 10, with Service Pack 2 for Server and Desktop editions. Minimum supported kernel: 2.6.18
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.

Note Agent systems must be able to communicate with CSA MC over HTTPS.

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

Caution When upgrading or changing operating systems, uninstall the agent first. When the new operating system is in place, you can install a new agent kit. Because the agent installation examines the operating system at install time and copies components accordingly, existing agent components may not be compatible with operating system changes.

VMware Environment Support

These VMware™ products can run on host operating systems that CSA supports, or can host guest operating system images that CSA supports.

- VMware WS 5.x (workstation)
- VMware GSX 3.2 (enterprise)
- VMware ESX 3.5i, 3.5, 3.0 and 2.5 (enterprise)
- VMware Player
- VMware Server

Not every VMware product can run on every host operating system that CSA supports.

All of the operating systems that the agent supports can be run as VMware guest operating systems.

We recommend visiting http://www.vmware.com for a complete discussion of what VMware products support which common operating systems as hosts or guests.

Installing Management Center for Cisco Security Agents V6.0.1

Installation, upgrade, and migration instructions are described in *Installing Management Center for Cisco Security Agents 6.0.1*.

The Management Center for Cisco Security Agents V6.0.1 kit is signed by Cisco Systems. This can be verified using Windows Explorer. Select the setup.exe file in the Management Center for Cisco Security Agents installation kit and from the File menu select Properties and click the Digital Signatures tab.

You can also verify the authenticity of the contents of the kit with the File Integrity Check Instructions provided in Chapter 2 of the Installation Guide.

You must have local administrator privileges on the system in question to perform the CSA MC installation. Once you have 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 CSA 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,* 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 Center (CSA MC).** This license enables the core functionality of CSA MC along with signature-based and behavior-based AntiVirus functionality and content-scanning.
- A license for **server platforms**.This includes all supported Windows, Solaris, and Linux server platforms.
- A license for **workstation platforms**. This includes all supported Windows and Linux desktop platforms.
- 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.*
- 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,* for more information about uploading licenses. See the **Data Loss Prevention** chapter in the *Using Management Center for Cisco Security Agents* 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. The file integrity check ensures that the CSA kit you downloaded from Cisco.com, or that was delivered to you on a CD, is the kit that we provided and that it has not been tampered with.

See Chapter 2, "Installing the Management Center for Cisco Security Agents" in *Installing the Management Center for Cisco Security Agents* for the procedures on performing file integrity checks.

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 7. 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 7 Windows 2000 Support

	Professional, SP4	Server	Advanced Server
Arabic	NS	NA	NA
Chinese (Simplified) Chinese (Simplified) (MUI)	L, T, S	L, S	L, S
Chinese (Traditional) Chinese (Traditional) (MUI)	T, S	S	S
Czech	S	S	NA
Danish (Native OS) Danish (MUI)	T, S	NA	NA
Dutch	S	S	NA
English (Canadian)	T, S	S	S
English (UK)	T, S	S	S
English (US)	L, T, S	L, S	L, S
Finnish	S	NA	NA
French French (MUI)	L, T, S	L, S	L, S
French (Canadian) French (Canadian) (MUI)	T, S	S	S
German German (MUI)	L, T, S	L, S	L, S
Greek	S	NA	NA
Hebrew Hebrew (MUI	T, S	NA	NA
Hungarian	S	S	NA
Italian Italian (MUI)	L, T, S	L, S	NA
Japanese Japanese (MUI)	L, T, S	L, S	L, S
Korean Korean (MUI)	L, T, S	L, S	L, S
Norwegian	S	NA	NA
Polish Polish (MUI)	L, T, S	L, S	NA
Portuguese (Brazilian) Portuguese (Brazilian) (MUI)	L, T, S	L, S	NA

	Professional, SP4	Server	Advanced Server
Russian Russian (MUI)	L, T, S	L, S	NA
Spanish Spanish (MUI)	L, T, S	L, S	L, S
Swedish	S	S	NA
Turkish	S	S	NA

Table 8 Windows XP Support

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

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

Table 9 Windows 2003 Support

	Standard, SP2	Web	Enterprise
Chinese (Simplified) Chinese (Simplified) (MUI)	L, T, S	L, S	L, S
Chinese (Traditional) Chinese (Traditional) (MUI)	T, S	S	S
Chinese (Hong Kong)	S	S	S
Czech	S	S	S
Danish Danish (MUI)	T, S	S	S
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 French (MUI)	L, T, S	L, S	L, S
French (Canadian) French (Canadian) (MUI)	T, S	S	S
German German (MUI)	L, T, S	L, S	L, S

	Standard, SP2	Web	Enterprise
Hebrew (Native) Hebrew (MUI	T, S	S	S
Hungarian	S	S	S
Italian Italian (MUI)	L, T, S	L, S	L, S
Japanese Japanese (MUI)	L, T, S	L, S	L, S
Korean Korean (MUI)	L, T, S	L, S	L, S
Norwegian	S	S	S
Polish Polish (MUI)	L, T, S	L, S	L, S
Portuguese (Brazilian) Portuguese (Brazilian) (MUI)	L, T, S	L, S	L, S
Russian Russian (MUI)	L, T, S	L, S	L, S
Spanish Spanish (MUI)	L, T, S	L, S	L, S
Swedish	S	S	S
Turkish	S	S	S

Table 10 Windows Vista Support

	Standard	Web	Enterprise, SP1
Chinese (Simplified) Chinese (Simplified) (MUI)	L, S	L, S	L, T, S
Chinese (Traditional) Chinese (Traditional) (MUI)	S	S	T, S
Chinese (Hong Kong)	S	S	S
Czech	S	S	S
Danish Danish (MUI)	S	S	T, S
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 French (MUI)	L, S	L, S	L, T, S

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

Related CSA Documentation

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

- *Installing Management Center for Cisco Security Agents 6.0.1* on Cisco.com at the following location: http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_installation_guides_list.html.
- *Using Management Center for Cisco Security Agents 6.0.1* on Cisco.com at the following location: http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_and_configuration_guides_list.html
- *Release Notes for Management Center for Cisco Security Agents 6.0.1* on Cisco.com at the following location: http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_notes_list.html
- *Management Center for Cisco Security Agents High Availability White Paper:* http://www.cisco.com/en/US/docs/security/csa/csa601/white_papers/Management_Center_for_Cisco_Security_Agent_High_Availability_White_Paper.pdf

Location of CSA Documents on Cisco.com

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

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

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

Step 1 Browse to Cisco's home page, http://www.cisco.com.

Step 2 Mouse over the **Products & Services** menu and click **Security**.

Step 3 Scroll down to the **Product Portfolio** area.

Step 4 Find **Endpoint Security** and click **Cisco Security Agent.**

Step 5 Look for the **Support** box on the right side of the page.

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

Cisco Security Forum

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

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

Cisco Professional Services

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

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

---