Release Notes for Management Center for Cisco Security Agents 6.0.2

Part Number: OL-21167-01

Management Center for Cisco Security Agents (CSA MC) 6.0.2 extends support to Windows 7 and Windows 2008 operating systems running on 32-bit and 64-bit architectures.

This document includes the following sections:

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

New Features and Updates

CSA 6.0.2 provides expanded platform support, new features, and updates to CSA 6.0.1 functionality.

Security Update Regarding the Use of the @digsig Token

If you have made any policy changes related to digital signatures (apart from editing the list of signatures in the Content field of the pre-configured **File Content - Signed - Trusted Publishers** file set) please restore the default settings. Any other deviation from the default digital-signatures policies could compromise security.

Warning **CSA uses digital signatures solely for the purpose of marking a file Trusted in a Scan Event Log rule, as done by the default policies and documented in the Scan Event Log section of online Help. Do NOT use digital-signature-content file sets for any other purpose, such as Application Class specifications, Modules that load after system startup in Kernel Protection rules, targets of FACLs, etc. Doing so would be a mis-configuration which could cause unexpected results.**

It is safe to edit the signatures in the Content matching field of the default file sets (such as File Content - Signed - Trusted Publishers). Do not make any other changes to CSA default digital-signatures rules; do not introduce digital-signatures constraints to existing file sets, etc.

Newly Supported Operating Systems

You can now install Cisco Security Agents on these platforms:

- Windows 7 (Professional and Enterprise) 32-bit platform
- Windows 7 (Professional and Enterprise) 64-bit platform
- Windows Server 2008 (Standard, Enterprise, and Web Edition) 32-bit
- Windows Server 2008 (Standard, Enterprise, and Web Edition) 64-bit
- VMware WS 6.x (workstation)

Note For a full list of the operating systems which CSA supports, see System Requirements for CSA MC, page 11.

Updates to Rule Modules and Differences in 64-bit Implementation

To create a a rule module specifically for 32-bit or 64-bit Windows 7 or Windows 2008, you can configure the OS field in the Rule Module configuration screen.

If you are creating a rule module specifically for 32-bit Vista, Windows 7, or Windows 2008 operating systems, select **Vista/Win7/W2k8 x86** in the OS drop down menu.

If you are creating a rule module specifically for 64-bit Windows 7 or Windows 2008 operating systems, select **Win7/W2K8 x64** in the OS drop down menu.

Updates to Rules and Differences in 64-bit Implementation

System API Control Rule Updates

The operations on System API Control rules have been reorganized and expanded.

There is a new group of operations called **Code Executing in Data or Stack Space** in System API Control rules. There are three options in that area:

- **Potential Buffer overflow:** Use this checkbox to detect applications accessing system functions from code executing in data or stack space.
- **Self-extracting code:** Use this checkbox to detect self extracting code executing in data or stack space.
- **Handle Data Execution Prevention Exceptions**: In some circumstances, Windows generates Data Execution Prevention (DEP) exceptions when a process unexpectedly attempts to execute code from the stack or heap sections. By checking the **Handle Data Execution Prevention Exceptions** checkbox in a System API Control rule, the CSA MC administrator instructs CSA to act on a DEP exception when it is generated. Though Windows stops the undesired behavior, this enables CSA to take additional actions such as identify an IP address from which an attack originates or collect information in order to automatically generate a virus signature.

  Generally, this checkbox is analogous to the "Handle exceptions" checkbox, in the sense that you should use the CSA MC Event Wizard to populate the "Included patterns:" field. See the "MS spoolsv, allow MSRPC requests to cause exceptions" rules as examples of how this field is used.

These aspects of System API Control rules work differently on a 64-bit operating system than they do in a 32-bit operating system:

- Trapping keystrokes

  On 64-bit operating systems, CSA cannot detect when a driver loaded into the kernel hooks the keyboard. However, on 32-bit and 64-bit operating systems, CSA can detect when a user-space application attempts to capture key strokes.

- Invoke unusual system calls

  This feature is not supported for 64-bit platforms. Windows Kernel Patch Protection prevents modification to the System Service Descriptor Table (SSDT) and the functions contained in the SSDT.

NT Event Log Rule

The NT Event Log Rule has been changed to follow the conventions of other rules that specify enforcement actions.

You can now use NT Event Log rules to take one of several actions when the conditions of the rule have been met:

- **Priority Allow.** This action is used to allow exceptions to existing deny rules that prevent NT Events from being written to the CSA MC event log. You can also require the allow action to be logged to the CSA MC event log and if this rule should take precedence over other allow rules.
- **Monitor.** This action records the NT Event in the CSA MC event log.
- **Notify**. This action notifies users if an NT Event has been triggered on their host. You can also require the notify action to be logged to the CSA MC Event Log.

- **Set.** The Sect action initiates a one-time configuration action to occur if the rule is triggered. For example, if a particular NT Event is recorded, the Set action could be used to set CSA's security level to **High** to enforce tighter security or **Low** to allow a greater range of behavior.

Now you can also write NT Event Log rules to trigger based on the enforcement action CSA took when the event was logged to the NT Event log. Specifying **Allow by default** or **Allow if triggered by a rule** indicates that CSA allowed the event to be written to the Event Log. The **Terminated** and **Denied by rule** options are not valid for this rule type.

Kernel Protection Rules

The **Modules modify kernel functionality** option in Kernel Protection Rules are not supported due the presence of Windows Kernel Patch Protection (KPP). See Rootkit Detection with Windows Kernel Patch Protection and CSA, page 8 for a complete description of the CSA's interaction with KPP.

Data Access Control Rules

For any 64-bit implementations of Apache, Data Access Control Rules have no effect, and do not function.

Sniffer and protocol detection

Sniffer and Protocol Detection rules are not supported for agents running on 32-bit or 64-bit versions of Windows Vista, Windows 7, Windows 2008 or subsequent versions of Windows operating systems.

Updates to Variables and Differences in 64-bit Implementation

Network Address Sets

You can now specify fully qualified domain names in Network Address Sets. If a domain name resolves to an IPv4 address and the IPv4 address resolves to the same domain name, you can use that domain name in a network address set in a rule. The feature is most useful when identifying hosts in a domain under an administrator's control such as a company-wide internal web site.

Note

- CSA can only evaluate domain names that resolve to IPv4 addresses. If the IP address of the domain is IPv6, CSA treats the domain as if it were unknown.
- If the address does not resolve to a fully qualified domain name or the IP address resolves to an unexpected name, you **should not** use the domain name to represent the IP address in the address set.

YouTube.com is an example of a fully qualified domain name you **should not** use in a network address set.

Performing an nslookup on youtube.com, yields three IP addresses:

```
C:\>nslookup youtube.com

Non-authoritative answer:
Name:    youtube.com
Addresses:  74.125.127.100, 74.125.45.100, 74.125.67.100
```

None of the IP addresses retrieved from the nslookup of the domain name resolve to the original domain name: youtube.com

```
C:\>nslookup 74.125.127.100
Name:    pz-in-f100.1e100.net
Address:  74.125.127.100

C:\>nslookup 74.125.45.100
Name:    yx-in-f100.1e100.net
Address:  74.125.45.100

C:\>nslookup 74.125.67.100
Name:    gw-in-f100.1e100.net
Address:  74.125.67.100
```

Nola.com is an example of a fully qualified domain name that you **could** use in a network address set. Performing an nslookup on nola.com yields one IP address: 69.2.101.59.

```
C:\>nslookup nola.com
Non-authoritative answer:
Name:    nola.com
Address:  69.2.101.59
```

If you were to then perform an nslookup on 69.2.101.59, the IP address would resolve to nola.com

```
C:\>nslookup 69.2.101.59
Name:    www.nola.com
Address:  69.2.101.59
```

To see examples of Network Address Sets, connect to the CSA MC and from the **Configuration** menu, select **Variables > Network Address Sets**.

These are the changes to network address sets:

- In the **Address ranges matching** and **But not** fields of the Configuration area, you can enter fully qualified domain names.
- You can use wildcards to generalize parts of the domain name.
- You can combine domain names and numeric IP addresses in the **Address ranges matching** and the **But not** fields.

Table 1 Examples of FQDN Syntax in Network Address Sets

Syntax	Valid	Invalid
Fully qualified domain names	cisco.com boxborough.cisco.com	http://www.cisco.com cisco.com/go/csa
Use of wildcards	*.cisco.com sanjose.*.cisco.com	cisco.*

Use of Wildcards in Network Address Sets

Though wildcards can be used to generalize a domain name, you need to be careful that the same domain name isn't used for two different domains.

For example, the nslookup of the youtube.com domain yielded three IP addresses which resolved to these domain names:

- pz-in-f100.**1e100.net**
- yx-in-f100.**1e100.net**
- gw-in-f100.**1e100.net**

Initially, this looks like a candidate for the use of wildcards. Perhaps you could generalize the results and use ***.1e100.net** as the address set?

Doing so would give you unexpected results. Performing an nslookup on google.com also yields three IP addresses, one of which is 74.125.67.100 which resolves to **gw-in-f100.1e100.net**. So using a wildcard like this ***.1e100.net** would affect YouTube.com, Google.com, and many other domains you could not anticipate.

Referencing the Values of Registry Keys in CSA Variables

One of the ways Windows accommodates 32-bit applications running on 64-bit operating systems is by using the Registry Redirector. You can learn more about the Registry Redirector at http://msdn.microsoft.com/en-us/library/aa384232(VS.85).aspx.

A registry access control rule only protects the registry key accessed by the Windows operating system. If the Windows OS performs Registry Redirection or Reflection prior to accessing the key, the OS will access a different key than the one you may have expected. For example, if you were to write a rule to protect the **HKLM\Software\App\MyInfo** registry key, and a 32-bit application running on a 64-bit operating system attempts to access the **HKLM\Software\App\MyInfo** key, the operating system will redirect the 32-bit application to the **HKLM\Software\Wow6432Node\App\MyInfo** registry key and your rule would not have protected it.

You can use wildcards in registry sets to generalize the location of the registry key you want to protect. For example you could specify **HKLM\Software**\App\Info** in a registry set to protect both registry keys mentioned previously.

You can use the @reg token to configure file sets, network address sets, network services sets, and registry sets to reference data stored in the values of registry keys. You can use the @regpath token to configure file sets, application classes, and registry sets. These tokens use the same syntax.

If the value of a key specified in the @reg or @regpath token is ambiguous because it could be interpreted by Windows differently for 32-bit and 64-bit applications, CSA uses the default value specified in the @reg or @regpath notation. This affects environmental variables such as %programfiles%, %commonprogramfiles%, %windir%\system32, %systemroot%\system32.

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 6.0.2 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. These Sample policies are hidden by default; you need to select “Show all items” in the Visibility Filter drop-down menu on the Policy list to see them. Sample policies do 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 policies 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.

CSA and Microsoft Windows Interoperability

Interoperability of Microsoft Kernel Patch Protection with CSA Rules

"Kernel patch protection in the x64-based versions of Microsoft Windows Server 2003 SP1, Microsoft Windows XP, and later versions of Microsoft Windows for x64-based systems protects code and critical structures in the Windows kernel from modification by unknown code or data. 'Unknown code or data' is any code or data that is not provided by Microsoft as part of the Windows kernel."[1]

Rootkit Detection with Windows Kernel Patch Protection and CSA

CSA does not detect kernel modifications (patches) on 64-bit Windows operating systems as it does on 32-bit Windows operating systems. The 64-bit Windows OSs use the kernel patch protection (KPP) feature to protect the Windows kernel and prevent CSA from determining if the kernel has been modified. This affects the **Modules modify kernel functionality** option in CSA's kernel protection rules.

In this release, we put forth our best effort to have CSA's behavior complement KPP's. CSA helps you identify the source of a rootkit, isolate it, prevent it from loading, and prevent your system from being caught in a cycle of booting and rebooting.

This is how a rootkit, KPP, and CSA would interact on a host with a 64-bit Windows operating system:

1. A rootkit gets installed on the computer.
2. CSA marks that content "untrusted."
3. When the rootkit executes, it tries to patch the Windows kernel.
4. When KPP detects that the kernel has been patched, it forces the computer to shut down to prevent further corruption or damage of the Windows operating system. (Users will recognize this shut down as the "Blue Screen of Death.") The computer then automatically restarts after the BSOD message has been displayed to the user.
5. When the computer reboots, it writes an entry into the Windows NT Event Log that begins: "**The computer has rebooted from a bugcheck. The bugcheck was: 0x00000109...**" This message is how you will be able to determine if the shutdown was caused by KPP.
6. If the agent receives the new Kernel Protection rule before KPP detects changes to the kernel, CSA MC could receive an event in the Event Log showing the name of the file that loaded after system startup.

   If you can gather that file name, you can create a File Access Control rule to monitor the actions of the suspected file or deny any application from reading or writing that file. You could also add the filename to the Black List on the Application Trust Levels page.

   A final approach to getting your system to boot is to create a kernel protection rule that denies all untrusted drivers from loading after system startup.

CSA can help diagnose the cause of the BSOD by monitoring and identifying suspect drivers that load after boot time. Use this procedure to attempt to identify the rootkit file:

Step 1 Boot the computer, that experienced the shut down, in Safe Mode.

Step 2 Open the Windows Registry.

1. **Windows Hardware Developer Center**. *Kernel Patch Protection: Frequently Asked Questions*. http://www.microsoft.com/whdc/driver/kernel/64bitpatch_FAQ.mspx

Step 3 Open this registry key:

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\csacenter\Persistent\@DownloadedDB`

CSA maintains it's list of "untrusted content" in this registry key.

Step 4 Examine the list for suspicious .dll, .sys, and other files and record the file names.

Step 5 On the CSA MC, create a **File Set** that identifies the files you suspect of patching the kernel.

Step 6 Create a rule module for a 64-bit windows operating system. In the OS field of the rule module, specify **Win7/Win2k8 x64**.

Step 7 Create a **Kernel Protection** rule, in the rule module with the following characteristics:

- Set the Kernel Protection rule to **Monitor** in order to learn what modules are loading after boot.
- Check the **Modules load after system startup** check box.
- In the **Included Modules** field, insert the file set that defines the list of suspicious files.
- Use the rest of the default settings for the rule.

Step 8 Click **Save**.

Step 9 Attach the rule module to a policy, add the policy to a group, add the affected host to the group, and generate rules.

Step 10 Boot the affected host and poll for updates.

Using an NT Event Log Rule to Report Rootkit Detection by KPP

If KPP shuts down the Windows operating system because of a suspected rootkit, on reboot it writes a message to the Windows event log that begins, "**The computer has rebooted from a bugcheck. The bugcheck was: 0x00000109...**"

You can create a NT Event Log rule in order to report this event to CSA MC; the bugcheck event is not reported to CSA MC by default.

Step 1 In the rule module you created in the Rootkit Detection with Windows Kernel Patch Protection and CSA section, create an NT Event Log rule with the following characteristics:

- Set the action to **Monitor**.
- In the Event Source field add **`Cisco Security Agent`**.
- Use the rest of the default settings for the rule.

Step 2 Click **Save**.

Step 3 **Generate rules**. This rule module should already be attached to a policy, the policy to a group, and the affected host should be a member of that group.

Step 4 Boot the affected host and poll for updates.

If CSA can collect the NT Event Log information before KPP identifies the kernel modification and shuts down the operating system on the computer, CSA MC will report this event:

```
"CSA detected that this machine has rebooted from a Microsoft PatchGuard bug check due
to the detection of kernel modification or corruption. If this occurs repeatedly,
consider configuring CSA to prevent the suspect driver(s) from loading: Get the list
of drivers by uploading CSA diagnostics from the affected host, then follow the
PatchGuard bug check directions in the CSAMC User's Guide."
```

Interoperability with Data Execution Prevention Exceptions and System API Control Rules

In some circumstances, Windows generates **Data Execution Prevention (DEP)** exceptions when a process unexpectedly attempts to execute code from the stack or heap sections. By checking the **Handle Data Execution Prevention Exceptions** checkbox in a System API Control rule, the CSA MC administrator instructs CSA to act on a DEP exception when it is generated. Though Windows stops the undesired behavior, this enables CSA to take additional actions such as identify an IP address from which an attack originates or collect information in order to automatically generate a virus signature.

Interoperability with Digital Rights Management and System API Control Rules

Windows Vista and subsequent Windows operating system releases support the creation of "protected processes" to support Digital Rights Management (DRM). The Windows OS places limitations on what can be done to protected processes. On 64-bit Windows operating systems, CSA cannot detect buffer overflow and code injection into protected processes.

A protected process could be any application created using the Windows Media Format SDK w/ DRM Addendum, the most common application using DRM technologies will be audiodg.exe. Audiodg.exe hosts the Windows audio engine.

Although CSA's ability to protect audiodg.exe is hampered somewhat by DRM/PMP (protected media path), presumably this application is less vulnerable to attacks because of its protected status and, as such, security is not greatly compromised by their presence.

Consider this interoperation when writing System API Control rules.

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 7, Windows 2008, 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, open the **Windows Security Center** console in one of those Windows operating systems, click **Windows Firewall**, click the **What else should I know about Windows Firewall?** link, and then enter "Why you should only use one firewall" in the Search field of the Help and Support Center dialog box.

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 for CSA MC

Table 2 shows the minimum server requirements for the Management Center for Cisco Security Agents (CSA MC). 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 2 Minimum Server Requirements

System Component	Requirement for a physical server	Requirements for Virtual Server
Hardware	• PC-compatible computer • Color monitor with video card capable of 16-bit color	VMware ESXi version 3.5, UP 3.
Processor	1 GHz or faster Pentium processor	2 GHz or faster processor

Table 2 Minimum Server Requirements

System Component	Requirement for a physical server	Requirements for Virtual Server
Operating System	Windows 2003 R2 Standard or Enterprise Editions without a service pack Windows 2003 R2 Standard or Enterprise Editions, with Service Pack 2 **Note** To run terminal services on the CSA MC system, you must edit the MC policy.	Windows 2003 R2 Standard or Enterprise Editions without a service pack Windows 2003 R2 Standard or Enterprise Editions, with Service Pack 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 VMware image of a Windows 2003 R2 server, as described above, which is maintained on a VMware ESXi hypervisor. See "Virtual Machine Support" in *Installing Management Center for Cisco Security Agents, 6.0.2* for more information.
File System Format	NTFS	NTFS
Memory	1 GB minimum memory	1 GB minimum memory
Virtual Memory	2 GB virtual memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space	9 GB minimum available disk drive space

Note CSA MC qualification and first level support for operation on Japanese OS (JOS) platforms is provided by Cisco Japan.

Browser Requirements to Access CSA MC

The browser you use to access CSA MC must meet the following requirements:

Screen Resolution

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.

Note We recommend connecting to the CSA MC interface using a browser on a remote machine rather than using a browser installed directly on the CSA MC's server.

Internet Explorer

- Version 7.0 or later.
- You must have cookies enabled. This means using a maximum setting of “medium” as your Internet security setting. Locate this feature from the following menu, Tools>Internet Options. Click the Security tab.
- Pop-up blockers must be disabled.
- JavaScript must be enabled.

Firefox

- Version 3.0 or later.
- You must have cookies enabled. Locate this feature from the following menu, Tools>Options>Privacy>Cookies.
- Pop-up blockers must be disabled.
- JavaScript must be enabled.

Microsoft SQL Servers

You can use Microsoft SQL Server Express or Microsoft SQL Server 2005 (or 2000) as the CSA MC database.

Note CSA does not support 64-bit versions of Microsoft SQL Servers.

Microsoft SQL Server Express

You can use the Microsoft SQL Server Express Edition (provided with the product) if you are planning to deploy no more than 1,000 agents. 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. Microsoft SQL Server Express Edition has a 4 GB limit.

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.)

Microsoft SQL Server 2005 or 2000

You also have the option of installing Microsoft SQL Server 2005 with Service Pack 0, 1, 2, or 3, or Microsoft SQL Server 2000, instead of using the Microsoft SQL Server Express Edition that is provided. MS SQL Server can be installed can be installed on the same system as the CSA MC or on a separate system.

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 Installing Management Center for Cisco Security Agents, 6.0.2 for details on installation options.)

System Requirements Cisco Security Agents

Agent Requirements for All Operating Systems

This information applies to agents on all operating systems:

- The Cisco Security Agent uses approximately 30 MB of memory.
- Agent systems must be able to communicate with CSA MC over HTTPS.
- If we do not claim CSA support for a Windows operating system in Table 3, a Solaris operating system in Table 4, or a Linux operating system in Table 5, CSA does not support the operating system.

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.

Agent Requirements for Windows Systems

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

Table 3 Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher **Note** Up to eight physical processors are supported

Table 3 Agent Requirements (Windows)

System Component	Requirement
Operating Systems	64-bit operating systems • Windows 7 (Professional and Enterprise) • Windows Server 2008 (Standard, Enterprise, and Web Edition) 32-bit operating systems • Windows 7 (Professional and Enterprise) • Windows Server 2008 (Standard, Enterprise, and Web Edition) • Windows Vista Business and Enterprise editions with Service Pack 0, 1, and 2. • 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 32 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.

Non-supported Windows Operating System

To prevent any confusion, we wanted to clarify that CSA does not support these recent releases of Windows operating systems:

- 64-bit Windows Vista with no service pack, with SP1, or with SP2.
- Windows Server 2008 R2.
- Other 64-bit editions of Windows Vista, 2007, and 2008 that are not listed among the supported platforms in Table 3 are not supported.
- Windows 7 XPM. In Windows 7, Microsoft is releasing a feature called XP Mode (“XPM”). XP Mode is a virtual machine that will come with a fully licensed copy of Windows XP SP3 pre-installed, and will allow users to run Windows XP applications on Windows 7. The CSAgent will not run in (and will not support) the XP Mode virtual machine within Windows 7.

Agent Requirements for Solaris Systems

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

Table 4 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 5 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.

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 6.x (workstation)
- 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 V6.0.2

Installation, upgrade, and migration instructions for CSA 6.0.2 are available in *Installing Management Center for Cisco Security Agents, 6.0.2.*

The Management Center for Cisco Security Agents V6.0.2 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 *Installing Management Center for Cisco Security Agent*.

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 CSA MC system. Changing the system name after the product installation will cause communication problems between the CSA MC and its agents.

Piloting the Product

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 if you are upgrading CSA, a short pilot program will be beneficial.

CSA 6.0.2 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.

If CSA is blocking what you know to be the benign behavior of an application which you understand thoroughly, and trust completely, and you cannot fully enable your application using the Event Management Wizard; you can configure certain rules to exempt your application from all CSA protection and control.

Warning **The CSA Bypass function should only be used as a last resort. If the applications you choose to exempt from CSA's protection and control are compromised, the host system will be vulnerable to attack even with CSA running.**

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.

Caveats Resolved by this Release

Caveats describe unexpected behavior or defects in Cisco software releases. Table 6 provides a list of defects that were reported in CSA 6.0.1 and are resolved by this release.

Table 6 Issues Resolved by CSA 6.0.2 Release

Bug ID	Summary	Resolution
CSCsx96954	CSA installation causes windows registration requirement.	Users are no longer be prompted to register with Microsoft after installing CSA.
CSCsy58166	After Agent installation, RHEL 4 Linux AS (Update 4) freezes on reboot.	Agent installation on RHEL 4 Linux no longer freezes upon reboot.
CSCsy74583	CSA 6.0.0.220 causes Microsoft Outlook 2007 to crash upon closing.	CSA 6.0.0.220 no longer causes Microsoft Outlook 2007 to crash upon closing.
CSCsy79491	Rule generation fails after importing CSA 5.2 migration data	Rule generation succeeds after importing CSA 5.2 migration data.
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.	Web page name patterns listed in the 'but not:' pattex.com rns matching field in a Data Set are allowed access to if the corresponding DACL rule is an enforcement rule with action to be takes as deny, query or terminate.
CSCtc72478	Upgrade: CSAMC install unable to load sample policies.	CSA now loads sample policies during upgrades from 6.0.1 to 6.0.2.
CSCtd28793	NT Event Log Rule is Broken	CSA now logs NT Events to CSA MC.

Product Notes

The following are issues that exist with the product, but are not product defects; therefore, they are not in the caveat 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**: There have been issues with Compaq/HP Teaming and the Cisco Security agent (CSA). Symptoms include the NICs not being enabled automatically after an agent installation. This has to do with issues between Compaq/HP Teaming software and the agent's network shim. This is an example of the behavior: Installing CSA on an HP DL380G2 server with an HP-NC3163 Ethernet card disables the ethernet card. After CSA is installed, and before the PC is rebooted to complete the installation, the ethernet adapter is disabled.

  Solutions: There are several different solutions to this issue:

  - Reboot the system immediately after CSA is installed.
  - Dissolve the team before installing CSA. Then, re-create the team after CSA has been installed.

  There may be other issues between CSA's network shim and Compaq/HP Teaming and thus we highly recommend dissolving the team prior to installing CSA if you plan to install the network shim.

- **Issue**: The 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**: If the Local File Protection feature of the Cisco Security Agent UI is modified, the protection 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.

Open Caveats in this Release

Caveats describe unexpected behavior or defects in Cisco software releases. Table 7 provides information on known caveats found in this release.

Table 7 Known Issues in Cisco Security Agent 6.0.2

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.
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.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation
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.
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.
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.
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.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation
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.
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.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation
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.
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.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation
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.
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 7 Known Issues in Cisco Security Agent 6.0.2

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** There is no workaround.

Table 7 Known Issues in Cisco Security Agent 6.0.2

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** There is no workaround.
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** There is no workaround.
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** There is no workaround.
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.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation
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** There is no workaround.
CSCta69326	The sshd exception created by the event wizard does not work	**Symptom** There is a network access control rule in the the Security-Network Lockdown rule module that denies all applications from acting as a client or server for TCP and UDP services. If you create an excpetion to that rule, in order to allow /usr/sbin/sshd to act as a server, the exception rule will not work and CSA will still prevent sshd from acting as a server. **Conditions** Linux operating system supporting IPv6 with Security-Network Lockdown rule module. **Workaround** Without using the wizard, create network access control rules that allow sshd to act as a server, for $TCP and $UDP services, when communicating with the IPv4 address and IPv6 of the remote host. In addition, the IPv4 address of the remote host must be added to the exception in it's IPv6 format. For example: If a remote host has IPv4 address as 192.168.24.64 and IPv6 address as 2607:f0d0:1002:11:0:0:0:5, then apart from including these host addresses, the new rule should also include the IPv4 address in IPv6 format, in this case c0a8:1840::(which is equivalent to 192.168.24.64).
CSCtd53466	CSA causes System Restore service to malfunction soon after boot	**Symptom** System Restore failures in the event log. The component shows up as "sr" and the message says that System Restore has stopped monitoring a volume. The event may appear after a reboot. **Conditions** All conditions when running in protect mode. **Workaround** There is no workaround.
CSCtf21778	Suse hangs when executing init 5 command from init 1 level.	**Symptom** When a user tries to move from init level 5 to 1 and then tries move from init level 1 to init level 5 without rebooting. These actions reproduce the behavior. 1. From init level 5, goto init 1. 2. Execute init 5 command. The machines stops at "starting udevd". **Conditions** Suse 10 with service pack 2 for servers and desktops. **Workaround** Issue System reboot from Run level 1.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation

CSCtf48029	Event Log does not open after CSA MC installation with backed up database.	**Symptom** After installing CSA MC with a backed-up CSA MC database, administrator was not able to open the Event Log. When navigating Events > Event Log from the CSA MC menu, the administrator sees a blank page with the error message, "Operation failed. See csamclog.txt for details."
		
		Conditions CSA MC installed on Windows Server 2003 R2 Enterprise Edition with SP2 using a remote or local Microsoft SQL Server 2005, Enterprise SP2 database, with a backed-up CSA MC database.
		
		Workaround On the system in which the database is present, execute the following steps:
		
		1. Open command prompt.
		2. Type `osql -E` and then press **Enter**.
		3. Execute the following commands.
		`use csamc60`
		`update statistics formatted_event_log with fullscan`
		`go`
		4. Type `Exit`.

Table 7 Known Issues in Cisco Security Agent 6.0.2

Bug ID	Summary	Explanation
CSCtf85656	Received alert event in CSA MC after installation of OpenGL API on Solaris 10	**Symptom** Receive alert event in CSA MC after installing OpenGL API on Solaris 10. While the system was booting up, csaadapt hung on loading. **Conditions** After installing OpenGL 1.5 API on Solaris 10 - Update 4. **Workaround** There is no workaround.

CSCtf96908	Errors and failures on group reports	**Symptom** Failure of "Event by group" report "Application deployment investigation" reports.
		You could see this error in the csamclog.txt file:
		`ms-csa: Mar 12 2010 13:39:55.140 -0700: %CSA-6-TRACE: %[Component=webadmin][PID=11780]: Error : java.sql.SQLException: I/O`
		You could receive this error on the remote database:
		`Encryption is required to connect to this server but the client library does not support encryption; the connection has been closed. Please upgrade your client library. [CLIENT: 10.1.2.12]`
		You could see this error after trying to generate Application Deployment Investigation
		`Error:java.sql.SQLException: I/O Error: DB server closed connection`
		You could see this error after trying to create a "Events by Groups" report:
		`Error: Operation failed. See csamclog.txt for details`
		
		Conditions Occurs with remote MS SQL Server 2000, 2005, 2008 servers with "Force Encryption" enabled on SQL server but not on the client.
		
		Workaround There is no workaround.

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

The localized languages above are **supported** on these operating systems:

- Windows 7 (Professional and Enterprise) 32-bit platform
- Windows 7 (Professional and Enterprise) 64-bit platform
- Windows Server 2008 (Standard, Enterprise, and Web Edition) 32-bit
- Windows Server 2008 (Standard, Enterprise, and Web Edition) 64-bit

Internationalization Support Tables

This section details 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.

This section defines 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 8. 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 8 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

	Professional, SP4	Server	Advanced Server
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
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 9 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

	Professional, SP3	Home
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
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 10 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

	Standard, SP2	Web	Enterprise
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
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 11 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

	Standard	Web	Enterprise, SP1
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
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 on Cisco.com

CSA 6.0.2 documentation is maintained and updated on cisco.com. Follow the links below to HTML and PDF versions of all CSA 6.0.2 technical documentation.

- *Installing Management Center for Cisco Security Agents 6.0.2* 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 6.0.2*

  http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_and_configuration_guides_list.html
- *Open Source License Acknowledgements and Third Party Copyrights for CSA 6.0.2*

  http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_licensing_information_listing.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 Information on Cisco.com

Cisco Security Center

If you would like early-warning intelligence information, threat and vulnerability analysis, and Cisco mitigation solutions to help protect your network, visit the **Cisco Security Center**:

http://tools.cisco.com/security/center/home.x

Cisco Security Forum

If you would like to post questions about CSA or read questions others are posting, visit the **Cisco Security Forum:** 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

---