



# CHAPTER 1

## Preparing to Install

---

### How the Cisco Security Agent Works

The Cisco Security Agent provides distributed security to your enterprise by deploying agents that defend against the proliferation of attacks across networks and systems. These agents operate using a set of rules provided by the Management Center for Cisco Security Agents and selectively assigned to each client node on your network by the network administrator.

This section includes the following topics.

- [Cisco Security Agent Overview, page 1-2](#)
- [Before Proceeding, page 1-2](#)
- [System Requirements, page 1-3](#)
- [Environment Requirements, page 1-9](#)
- [DNS and WINS Environments, page 1-9](#)
- [Browser Requirements, page 1-9](#)
- [Time and Date Requirements, page 1-10](#)
- [Port Availability, page 1-10](#)
- [Windows Cluster Support, page 1-11](#)
- [Internationalization Support, page 1-11](#)
- [Internationalization Support Tables, page 1-12](#)
- [About CSA MC, page 1-17](#)

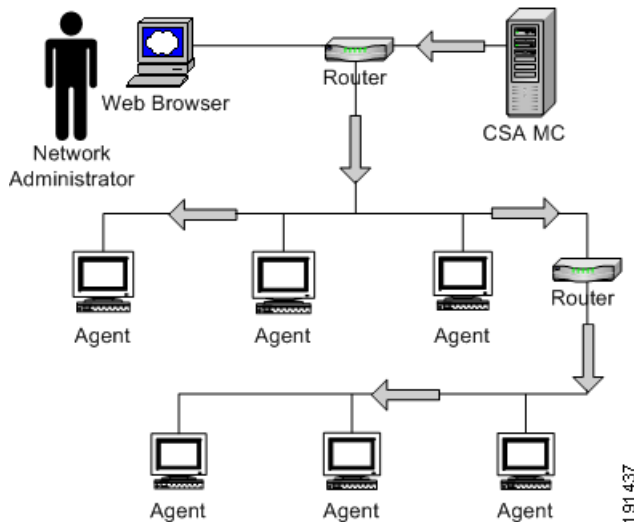
# Cisco Security Agent Overview

Cisco Security Agent contains two components:

- The Management Center for Cisco Security Agents (CSA MC)- installs on a secured server and includes a web server, a configuration database, and a web-based user interface.
- The Cisco Security Agent (the agent)- installs on desktops and servers across your enterprise and enforces security policies on those systems.

Administrators configure security policies on CSA MC using the web-based interface. They distribute these policies to agents installed on end user systems and servers. Policies can allow or deny specific system actions. The agents check policies before allowing applications access to system resources.

**Figure 1-1 Product Deployment**



## Before Proceeding

Before installing CSA MC software, refer to the Release Notes for up-to-date information. Not doing so can result in the misconfiguration of your system.

Make sure that your system is compatible with the Cisco product you are installing and that it has the appropriate software installed.

Read through the following information before installing the CSA MC software.

## System Requirements



### Note

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

[Table 1-1](#) shows the minimum CSA MC server requirements for Windows 2003 systems. These requirements are sufficient if you are running a pilot of the product or for deployments up to 1,000 agents. If you are planning to deploy CSA MC with more than 1,000 agents, these requirements are insufficient. See [Scalable Deployments, page 2-3](#) for more detailed system requirements.

**Table 1-1** *Minimum Server Requirements*

System Component	Requirement
Hardware	<ul style="list-style-type: none"> <li>IBM PC-compatible computer</li> <li>Color monitor with video card capable of 16-bit</li> </ul>
Processor	1 GHz or faster Pentium processor
Operating System	Windows 2003 R2 Standard or Enterprise Editions, Service Pack 0, 1, or 2 <b>Note</b> To run terminal services on the CSA MC system, you must edit the MC policy.
File System	NTFS
Memory	1 GB minimum memory
Virtual Memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space

- Pager alerts require a Hayes Compatible Modem.

- For optimal viewing of the CSA MC UI, you should set your display to a resolution of 1024x768 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.

If you are planning to deploy no more than 1,000 agents, the shipped version of Microsoft SQL Server Express should be adequate. For a larger deployment, you also have the option of installing Microsoft SQL Server 2005 or Microsoft SQL Server 2000 instead of using the Microsoft SQL Server Express database that is provided. 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 [Chapter 3, “Installing the Management Center for Cisco Security Agents”](#) for details.

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.

To run the Cisco Security Agent on Windows servers and desktop systems, the requirements are as follows:

**Table 1-2 Agent Requirements (Windows)**

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher  <b>Note</b> Up to eight physical processors are supported.
Operating Systems	<ul style="list-style-type: none"> <li>• Windows Server 2003 R2 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0, 1, or 2</li> <li>• Windows XP (Professional, Tablet PC Edition 2005, or Home Edition) Service Pack 0, 1, or 2</li> <li>• Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4</li> <li>• Windows NT (Workstation, Server or Enterprise Server) with Service Pack 6a</li> </ul> <b>Note</b> Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000 (Terminal Services are not supported on Windows NT.)  Supported language versions are as follows: <ul style="list-style-type: none"> <li>• For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported.</li> <li>• For Windows NT, US English is the only supported language version.</li> </ul>
Memory	128 MB minimum—all supported Windows platforms

System Component	Requirement
Hard Drive Space	50 MB or higher <b>Note</b> This includes program and data.
Network	Ethernet or Dial up <b>Note</b> Maximum of 64 IP addresses supported on a system.

To run the Cisco Security Agent on your Solaris server systems, the requirements are as follows:

**Table 1-3 Agent Requirements (Solaris)**

<b>System Component</b>	<b>Requirement</b>
Processor	UltraSPARC 400 MHz or higher  <b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	Solaris 9, 64 bit, patch version 111711-11 or higher, and 111712-11 or higher installed.  Solaris 8, 64 bit 12/02 Edition or higher (This corresponds to kernel Generic_108528-18 or higher.)  <b>Note</b> If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disc (1 of 2) in the /Solaris_8/Product directory. Install using the pkgadd -d . SUNWlibCx command.
Memory	256 MB minimum
Hard Drive Space	50 MB or higher  <b>Note</b> This includes program and data.
Network	Ethernet  <b>Note</b> Maximum of 64 IP addresses supported on a system.

**Caution**

On Solaris systems running Cisco Security Agents, if you add a new type of Ethernet interface to the system, you must reboot that system twice for the agent to detect it and apply rules to it accordingly.

To run the Cisco Security Agent on your Linux systems, the requirements are as follows:

**Table 1-4 Agent Requirements (Linux)**

System Component	Requirement
Processor	500 MHz or faster x86 processor (32 bits only) <b>Note</b> Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	RedHat Enterprise Linux 4.0 WS, ES, or AS RedHat Enterprise Linux 3.0 WS, ES, or AS
Memory	256 MB minimum
Hard Drive Space	50 MB or higher <b>Note</b> This includes program and data.
Network	Ethernet <b>Note</b> 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.

## Environment Requirements

The following are recommendations for a secure setup and deployment of CSA MC.

- The system on which you are installing the CSA MC software should be placed in a physically secure, locked down location with restricted access.
- Do not install any software on the CSA MC system that is not required by the product itself.
- You must have administrator privileges on the system in question to perform the installation.
- The CSA MC system must have a static IP address or a fixed DHCP address.

## DNS and WINS Environments

For agents and browsers to successfully communicate with CSA MC, the CSA MC machine name must be resolvable through DNS (Domain Name Service) or WINS (Windows Internet Naming Service).

## Browser Requirements

You use a web browser to access CSA MC either locally or from a remote system. Browser requirements are as follows:

*Internet Explorer:*

- Version 6.0 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.
- JavaScript must be enabled.
- If you are using Internet Explorer Version 6.0 SP1 or higher, your CSA MC FQDN cannot contain non-alphanumeric characters other than '-' and '.'. For example, if the server system name contains an underscore "\_", CSA MC will not work properly.

*FireFox:*

- Version 1.5.0.x or higher
- You must have cookies enabled. Locate this feature from the following menu, Tools>Options>Privacy>Cookies.
- JavaScript must be enabled.

## Time and Date Requirements

Before you install CSA MC, make sure that the system to which you plan install the software has the correct and current time, date, and time zone settings. If these settings are not current, you will encounter MC/agent certificate issues.

## Port Availability

CSA MC acts as a web server and requires that no other web server software is running on the CSA MC system. Having multiple web servers running on the same system causes port conflicts.



**Caution**

---

By default, Windows 2003 has the World Wide Web Publishing service running. If the CSA MC installation detects this service running, the CSA MC installation will disable all Web publishing services in order for its own installation to proceed.

---

## Windows Cluster Support

Cisco Security Agent supports Network Load Balancing and Server Cluster for Windows 2003 and 2000 Server platforms. Cluster support may require certain network permissions to operate. As with other network services, your CSA MC policies must account for these network permissions. (Component Load Balancing, and Solaris and Linux Clusters are not officially supported in this release.)

## Internationalization Support

All Cisco Security Agent kits contain localized support for English, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish language desktops. This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system will appear in the language of the end user's desktop.

The following table lists CSA localized support and qualification for various OS types.

**Table 1-5 CSA Localizations**

<b>Language</b>	<b>Operating System</b>	<b>Localized</b>	<b>Qualified</b>
Chinese (Simplified)	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
French	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
German	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Italian	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes

Language	Operating System	Localized	Qualified
	Windows 2003	Yes	Yes
Japanese	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Korean	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes
Spanish	Windows 2000	Yes	Yes
	Windows XP	Yes	Yes
	Windows 2003	Yes	Yes

#### Explanation of terms:

**Localized:** Cisco Security Agent kits contain localized support for the languages identified in [Table 1-5](#). This support is automatic in each agent kit and no action is required by the administrator. The agent UI, events, and help system will appear in the language of the end user's desktop. All localized languages are agent qualified and supported. (CSA MC is not localized.)

**Qualified:** The Cisco Security Agent was tested on these language platforms. Cisco security agent drivers are able to handle the local characters in file paths and registry paths. All qualified languages are supported.

**Supported:** The Cisco Security Agent is suitable to run on these language platforms. The localized characters are supported by all agent functions.

Refer to the following tables.

## Internationalization Support Tables

The following tables detail the level of support for each localized version of Windows operating systems. **Note that support for a localized operating system is different from localized agent.** A localized operating system may be supported even though the corresponding language is not translated in the agent. In this case, the dialogs will appear in English. The tables below define the operating system support, not agent language support. Note, for Multilingual User

Interface (MUI) supported languages, installs are *always* in English (Installshield does not support MUI), and the UI/dialogs are in English unless the desktop is Chinese (Simplified), French, German, Italian, Japanese, Korean, or Spanish.

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

The following letter combinations are used to describe the level of support:

**Table 1-6 Support Level Key**

L	Agent localized, supported and qualified. ( <b>Note:</b> L(S) – Localized and supported only)
T	Supported and qualified.
S	Supported but not qualified – Bugs will be fixed when reported by customers, but the exact configuration was not tested.
NA	Not applicable – Microsoft does not ship this combination.
NS	Not supported.

**Table 1-7 Windows 2000 Support**

	Professional	Server	Advanced Server
MUI	T	S	S
Arabic	NS	NA	NA
Chinese (Simplified)	L	L(S)	L(S)
Chinese (Traditional)	T	S	S
Czech	S	S	NA
Danish	T	NA	NA
Dutch	S	S	NA
English	L	L	L
Finnish	S	NA	NA
French	L	L(S)	L(S)
German	L	L(S)	L(S)

	<b>Professional</b>	<b>Server</b>	<b>Advanced Server</b>
Greek	S	NA	NA
Hebrew	NS	NA	NA
Hungarian	S	S	NA
Italian	L	L(S)	NA
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)
Norwegian	S	NA	NA
Polish	T	T	NA
Portuguese	S	S	NA
Russian	S	S	NA
Spanish	L	L(S)	L(S)
Swedish	S	S	NA
Turkish	S	S	NA

**Table 1-8 Windows XP Support**

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

	<b>Professional</b>	<b>Home</b>
Greek	S	S
Hebrew	NS	NS
Hungarian	S	S
Italian	L	L(S)
Japanese	L	L(S)
Korean	L	L(S)
Norwegian	S	S
Polish	T	T
Portuguese	S	S
Russian	S	S
Spanish	L	L(S)
Swedish	S	S
Turkish	S	S

**Table 1-9 Windows 2003 Support**

	<b>Standard</b>	<b>Web</b>	<b>Enterprise</b>
Chinese (Simplified)	L	L(S)	L(S)
Chinese (Traditional)	T	S	S
Chinese (Hong Kong)	S	S	S
Czech	S	S	S
Dutch	S	NA	NA
English	L	L	L
French	L	L(S)	L(S)
German	L	L(S)	L(S)
Hungarian	S	S	S
Italian	L	L(S)	L(S)
Japanese	L	L(S)	L(S)
Korean	L	L(S)	L(S)

	<b>Standard</b>	<b>Web</b>	<b>Enterprise</b>
Polish	T	T	T
Portuguese	S	S	S
Russian	S	S	S
Spanish	L	L(S)	L(S)
Swedish	S	S	S
Turkish	S	S	S

On non-localized but tested and supported language platforms, the administrator is responsible for policy changes arising from directory naming variations between languages.

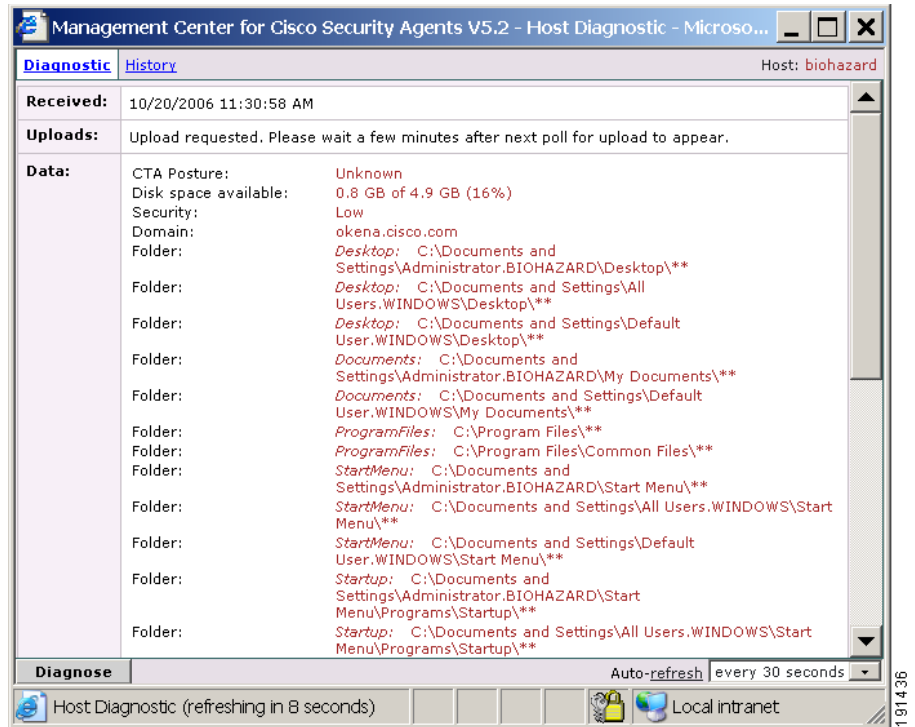
If the previous operating system tables do not indicate that CSA is localized (L) then the system administrator is responsible for checking to ensure that the tokens are in the language they expect and the directory path is the one they intend to protect.

To determine if language tokens are correct, follow this procedure:

- 
- Step 1** Move your mouse over **Systems** in the menu bar and select **Hosts** from the drop-down menu.
  - Step 2** Click the link to the host name using the language you want to verify.
  - Step 3** In the Host Status area, click the **Detailed Status and Diagnostics** link.
  - Step 4** Click the **Diagnose** button.

Look at the folder information in the Data area of the Diagnosis Data page. (See [Figure 1-2](#).) These are the values of the directory tokens CSA needs for localization. Make sure that the folder paths are in the language you expect and that they protect the correct directory.

Figure 1-2 Diagnosis for Localized Host



## About CSA MC

The CSA MC user interface installs as part of the overall Cisco Security Agent solution installation. It is through a web-based interface that all security policies are configured and distributed to agents. CSA MC provides monitoring and reporting tools, letting you generate reports with varying views of your network enterprise health and status. Providing this web-based user interface allows an administrator to access CSA MC from any machine running a web browser.

See the User Guide for further details.

Figure 1-3 CSA MC, Top Level View

The screenshot displays the Management Center for Cisco Security Agents V5.2 web interface. The browser window title is "Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer". The address bar shows "https://biohazard/csamc52/webadmin". The interface includes a navigation menu with "Events" selected, and a main content area with sections for Network Status, Most Active, Event Counts Per Day, and Database Maintenance. A status bar at the bottom indicates "No rule changes pending" and "Generate rules".

**Management Center for Cisco Security Agents V5.2**

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Status Summary

**Network Status**

- Events recorded in the past 24 hours: **13**
- Host history collection enabled: **No**
- Active hosts with Cisco Security Agent security disabled: **0**
- Hosts not actively polling (status unknown): **0**
- Groups with no policies attached: **2**

**Most Active** (last 24hr)

- Hosts >> Rules >> Applications >> Rules, Applications
- biohazard [W]** [9 events] [Top 10](#)

**Event Counts Per Day**

25

■ Error and above  
■ Warning  
■ Notice  
■ Information

20  
Oct

**Database Maintenance**

- Alerts: **2**

**Refresh**

Refreshing in 4:16 minutes | Refresh interval | 5 minutes

No rule changes pending [Generate rules](#) Logged in as: admin

Local intranet

191438