



Installing Management Center for Cisco Security Agents 6.0.1

Revision Date: March 29, 2010

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-18678-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Installing Management Center for Cisco Security Agents 6.0.1
Copyright © 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

Audience vii

Related Documentation vii

Documents on Cisco.com viii

Obtaining Documentation, Obtaining Support, and Security Guidelines viii

CHAPTER 1

Preparing to Install 1-1

How the Cisco Security Agent Works 1-1

Cisco Security Agent Overview 1-2

About CSA MC 1-3

Before Proceeding 1-3

System Requirements 1-4

CSA MC System Requirements 1-4

Agent Requirements for Windows Systems 1-6

Agent Requirements for Solaris Systems 1-7

Agent Requirements for Linux Systems 1-8

Environment Requirements 1-9

Browser Requirements 1-9

DNS and WINS Environments 1-9

Port Availability Requirements 1-10

Time and Date Requirements 1-10

Windows Cluster Support 1-11

Required Regional and Language Options Settings for CSA MC 1-11

Virtual Machine Support 1-11

Adobe Reader 1-12

Internationalization and Localization Support 1-12

Localization Support for Cisco Security Agents 1-12

Internationalization Support Tables 1-13

Verifying Language Tokens 1-18

Scalable Deployments 1-19

Hardware Sizing 1-19

Software Considerations 1-20

Configuration Recommendations for Scalability 1-21

Factors in Network Sizing 1-21

Factors in Database Sizing 1-22

CHAPTER 2

Installing the Management Center for Cisco Security Agents 2-1

Overview 2-1

Licensing Information 2-2

PAK Certificates 2-2

License Types 2-2

License File Contents 2-3

Managing and Troubleshooting Licenses 2-4

Uploading a License 2-4

File Integrity Check Instructions 2-5

File Integrity Check on Downloaded CSA Software 2-5

File Integrity Check on CSA Software Delivered on CD 2-6

Upgrading from CSA V6.0 to CSA V6.0.1 2-7

Migrating Configurations and Hosts to CSA V6.0.1 from CSA V5.2 and Earlier 2-7

Upgrade and Migration Scenarios 2-8

Overview of Installing CSA MC with Local and Remote DB 2-10

New Installation Configuration Options 2-10

Installing CSA MC with a Local Database 2-12

Installing CSA MC with a Remote Database 2-21

Information for Installing Multiple CSA MCs on Separate Systems 2-30

Installing CSA MC with a Previous Version's Database (Same System Installation) 2-31

Installation Log 2-35

Accessing Management Center for Cisco Security Agents 2-35

Local Access 2-36

Remote Access 2-36

Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1 2-37

Upgrading CSA MC with a Local or Remote Database from CSA V6.0 to V6.0.1 2-37

Upgrading Multiple CSA MCs with a Remote Database from CSA V6.0 to V6.0.1 2-38

Migration Instructions 2-39

Initiating Secure Communications 2-41

Internet Explorer 7.0: Importing the Root Certificate 2-45

Uninstalling Management Center for Cisco Security Agents 2-46

Hotfix Information 2-47

Clearing the cache in Internet Explorer 2-47

Clearing the cache in Mozilla Firefox. 2-47

CHAPTER 3**Quick Configuration & Deployment 3-1**

- Overview 3-1
- Logging on to the CSA MC 3-2
 - Access Management Center for Cisco Security Agents 3-2
 - Simple View and Advanced View Modes 3-3
 - Visible, Hidden, and Read-only Components on CSA MC 3-3
- Cisco Security Agent Policies 3-4
- Piloting the Product 3-4
 - Running a Pilot Program 3-4
- Quick Configuration and Deployment 3-5
 1. Update your Licenses 3-5
 2. Pick your Policies 3-5
 3. Update the Agent Kits 3-6
 4. Distribute and Install the Kits 3-6
 5. Create Exceptions as Necessary 3-6
- View Registered Hosts 3-7
- Policy Tuning and Troubleshooting 3-7
 - Overall Guidelines 3-7
 - Creating Policies for Your Special Applications 3-8
 - Using Audit Mode 3-9
 - Disabling Specific Rules 3-9
 - Caching and Resetting Query Responses 3-9
 - Setting Up Exception Rules 3-10
- Configuring Your Own Policies 3-11
- Distributing Agent Kits Using a Third Party Tool 3-11
 - Setup.exe Command Switches 3-12
 - Command Examples 3-14

APPENDIX A**Cisco Security Agent Installation and Overview A-1**

- Overview A-1
- Downloading and Installing A-1
 - The Cisco Security Agent User Interface A-3
- Installing the Solaris Agent A-4
- Installing the Linux Agent A-6

APPENDIX B**Open Source License Acknowledgements and Third Party Copyrights B-1**

- OpenSSL/Open SSL Project B-1
- License Issues B-2

Apache [version 2.0.59]	B-3
TCL license	B-6
Perl	B-6
Socket6	B-7
libpcap	B-7
CMU-SNMP Libraries	B-8
Open Market FastCGI	B-8
CGIC License	B-9
Mozilla 1.xx (libcurl)	B-9
MICROSOFT SOFTWARE LICENSE TERMS	B-9
.Net Framework 2.0	B-12
MarshallSoft Computing SMTP/POP3 Email Engine	B-13
Jasper Reports V1.2.0 and JFreeChart V1.0.5	B-13
iText version 1.3.1	B-20
Java Runtime Environment JRE 1.5.0.06	B-26
The GNU General Public License (GPL)	B-29



Preface

This manual describes how to install the Management Center for Cisco Security Agents on Microsoft Windows 2003 R2 operating systems and the Cisco Security Agent on supported Microsoft Vista (32-bit), Microsoft Windows 2003, Microsoft Windows XP, Microsoft Windows 2000, Sun Solaris 10, Sun Solaris 9, Sun Solaris 8, RedHat Enterprise Linux 5.0, RedHat Enterprise Linux 4.0, RedHat Enterprise Linux 3.0, and SUSE Linux Enterprise 10 operating systems.

In addition to the information contained in this manual, the release notes contain the latest information for this release. Note that this manual does not provide tutorial information on the use of any operating systems.

Audience

This manual is for system managers or network administrators who install, configure, and maintain Management Center for Cisco Security Agents software. Installers should be knowledgeable about networking concepts and system management and have experience installing software on Windows operating systems.

Related Documentation



Note

Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review Cisco Security Agent documentation on Cisco.com for any updates.

These are the documents that describe this offering of Cisco Security Agent, Release 6.0.1

- *Installing Management Center for Cisco Security Agents 6.0.1*
- *Using Management Center for Cisco Security Agents 6.0.1*
- *Release Notes for Management Center for Cisco Security Agents 6.0.1*
- *Management Center for Cisco Security Agents High Availability Whitepaper*. This whitepaper describes a High Availability solution compatible with the CSA MC for versions 6.0 and later.

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.
 - Step 6** Click **Cisco Security Agent**. This brings you to a linking page where you will find links to all CSA user documents.

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>



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](#)
- [About CSA MC, page 1-3](#)
- [Before Proceeding, page 1-3](#)
- [System Requirements, page 1-4](#)
 - [CSA MC System Requirements, page 1-4](#)
 - [Agent Requirements for Windows Systems, page 1-6](#)
 - [Agent Requirements for Solaris Systems, page 1-7](#)
 - [Agent Requirements for Linux Systems, page 1-8](#)
- [Environment Requirements, page 1-9](#)
 - [Browser Requirements, page 1-9](#)
 - [DNS and WINS Environments, page 1-9](#)
 - [Time and Date Requirements, page 1-10](#)
 - [Port Availability Requirements, page 1-10](#)
 - [Windows Cluster Support, page 1-11](#)
 - [Required Regional and Language Options Settings for CSA MC, page 1-11](#)
 - [Virtual Machine Support, page 1-11](#)
 - [Adobe Reader, page 1-12](#)
- [Internationalization and Localization Support, page 1-12](#)
 - [Internationalization Support Tables, page 1-13](#)
 - [Verifying Language Tokens, page 1-18](#)
- [Scalable Deployments, page 1-19](#)

- [Hardware Sizing, page 1-19](#)
- [Software Considerations, page 1-20](#)
- [Configuration Recommendations for Scalability, page 1-21](#)
- [Factors in Network Sizing, page 1-21](#)
- [Factors in Database Sizing, page 1-22](#)

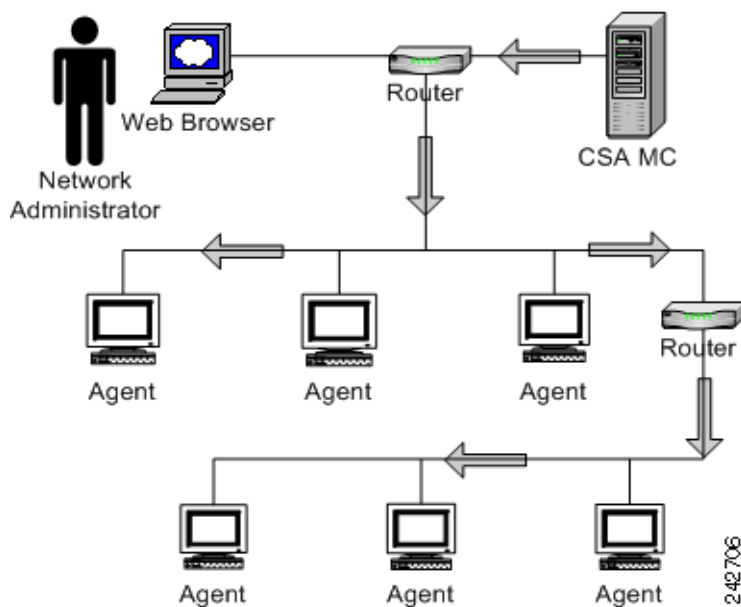
Cisco Security Agent Overview

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.

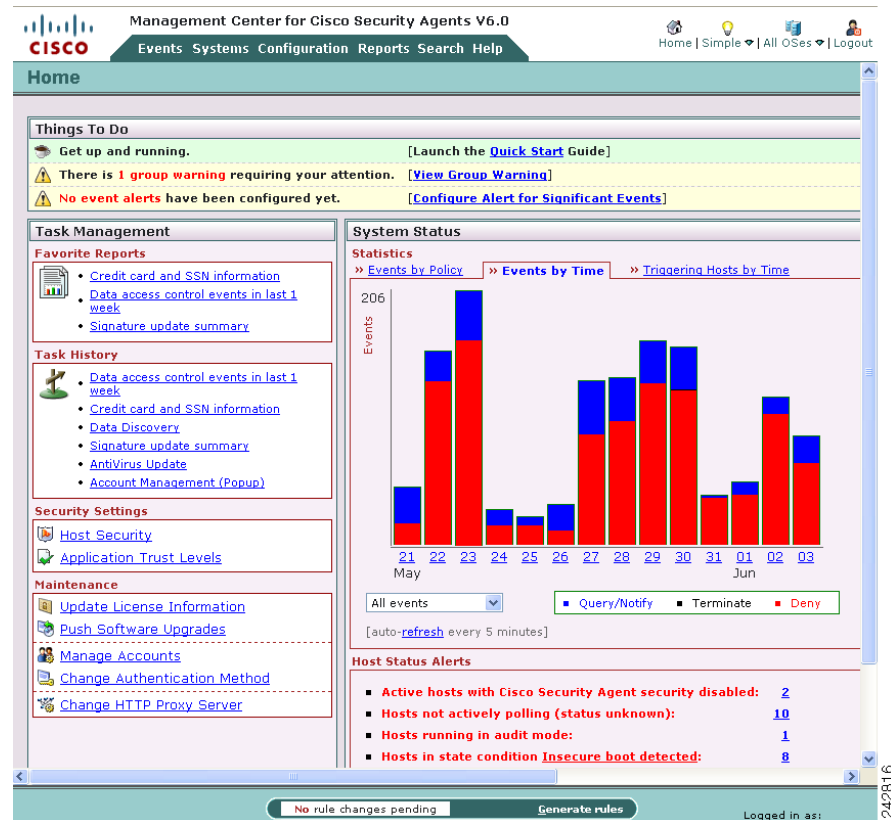
Figure 1-1 *Product Deployment*



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. [Figure 1-2](#) shows the CSA MC home page. See *Using Management Center for Cisco Security Agent* for further details.

Figure 1-2 CSA MC, Home Page



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

CSA MC 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 1-19](#) for more detailed system requirements.

Table 1-1 Minimum Server Requirements

System Component	Requirements for a physical server	Requirements for a virtual server
Hardware	- PC-compatible computer - Color monitor with video card capable of 16-bit	VMware ESXi version 3.5, UP 3.
Processor	1 GHz or faster processor	2 GHz or faster processor
Operating Systems	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, page 1-11 for more information.
File System	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

- CSA MC qualification and first level support for operation on Japanese OS (JOS) platforms is provided by Cisco Japan.
- The minimum recommended screen resolution for viewing the CSA MC UI is 1024x768. For optimal viewing of the CSA MC UI, you should set your display to a resolution of 1280x600 or higher.


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.

- On a system where CSA MC has never been installed, the CSA MC setup program first installs Microsoft SQL Server Express and the required .NET environment. If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express, the installation will abort. This database configuration is not supported.

SQL Server Express Edition

As part of the installation process on a system where CSA MC has not previously been installed, the setup program first installs Microsoft SQL Server Express Edition and the required .NET environment. You can use the included Microsoft SQL Server Express Edition (provided with the product) if you are planning to deploy no more than 1,000 agents.



Caution

If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express Edition, the CSA MC installation will abort. This database configuration is not supported by Cisco. (Installation process aborts if any databases other than those listed here are found: master, tempdb, model, msdb, pubs, Northwind, profiler and AnalyzerLog.)

For a local database configuration, you also have the option of installing Microsoft SQL Server 2005 or 2000 instead of using the Microsoft SQL Server Express Edition that is provided. Microsoft SQL Server Express Edition has a 4 GB limit. In this case, you can have CSA MC and Microsoft SQL Server 2005 on the same system if you are planning to deploy no more than 5,000 agents. Note that if you are using SQL Server 2005 or 2000, it must be licensed separately and it must be installed on the system before you begin the CSA MC installation.

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.

See [Chapter 2, “Installing the Management Center for Cisco Security Agents”](#) for more information.

Agent Requirements for Windows Systems

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

Table 1-2 Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher Note Up to eight physical processors are supported.
Operating Systems	- Windows Vista Business and Enterprise editions with service pack 0 or 1. - Windows Server 2003 (Standard, Enterprise, Web, or Small Business Editions) Service Pack 0, 1, or 2 - Windows XP (Professional, Tablet PC Edition 2005, or Home Edition) Service Pack 0, 1, 2, or 3. - Windows Embedded Point of Service (WEPOS) 1.1 - Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, 3, or 4 Note Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows 2003, Windows XP, and Windows 2000. Supported language versions are as follows: - For Windows 2003, XP, and 2000, all language versions, except Arabic and Hebrew, are supported.
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.

See [Port Availability Requirements, page 1-10](#) for the ports that need to be available for agents to communicate with the CSA MC.



Note

Cisco Security Agent uses approximately 30 MB of memory. This applies to agents running on all supported Microsoft 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.

Agent Requirements for Solaris Systems

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

Table 1-3 Agent Requirements (Solaris)

System Component	Requirement
Processor	UltraSPARC 400 MHz or higher Note Uni-processor, dual processor, and quad processor systems are supported.
Hardware platform	Sun4u for Solaris 8,9, and 10.
Operating Systems	- Solaris 10, 64 bit kernel, 6/06 edition or higher. Recommended patch levels 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.

See [Port Availability Requirements, page 1-10](#) for the ports that need to be available for agents to communicate with the CSA MC.

Agent Requirements for Linux Systems

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

Table 1-4 Agent Requirements (Linux)

System Component	Requirement
Processor	500 MHz or faster x86 processor (32 bits only) Note Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	- 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.

See [Port Availability Requirements, page 1-10](#) for the ports that need to be available for agents to communicate with the CSA MC.

**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 DHCP reservation.

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.
- Pop-up blocking must be disabled.
- 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.
- Pop-up blocking must be disabled.
- JavaScript must be enabled.

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).

Port Availability Requirements

This section describes the ports that need to be available for Cisco Security Agents to communicate with the Management Center. These ports need to be open on both the host running the agent, whether that host is a server or a desktop, and the server running the CSA MC. These ports perform the same tasks on all operating systems.

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.

During installation, the CSA MC installer determines if any application or service is using the ports mentioned in [Table 1-5](#) below. If there is an application or service using a port, the installation aborts and the user is asked to shut down the services that are using those ports.

Table 1-5 Required Port Availability for Agents and the CSA MC

Port Number	Purpose
25	E-mail alerts are sent on this port.
80	Agent kit caching is performed on this port.
162	Used for SNMP traps.
443	The web browser on the host communicates with CSA MC on this port.
1433	If you have SQLServer on a remote machine or running locally on the same machine as the CSA MC, make sure the SQLServer port is open.
1741, 1742	Ports 1741 and 1742 are used to access Cisco Works VPN Security Management Solutions (VMS) center. (Then, to communicate with the CSA MC within VMS, you need to have port 443 open.)
5401	Application Analysis jobs are performed over this port.
5401 or 443	Cisco Security Agent communicates with the Management Center over port 5401. If port 5401 is not available, port 443 is used by default.

Time and Date Requirements

Before you install CSA MC, make sure that the system on 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.

You can use the Network Time Protocol (NTP), TIME, and DAYTIME protocols for synchronizing time between the CSA MC and its agents. When using these protocols, you will also need to distribute a Network Access Control Rule (NACL) allowing hosts to access various ports for these kinds of network services. See the **Sample - Microsoft Domain Controller** rule module for an example of a NACL that allows hosts to act as a client or server for time protocols.

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.)

Required Regional and Language Options Settings for CSA MC

The following Windows OS values on the CSAMC machine must all be set to U.S. English:

- User Locale
- Language
- System Locale

If they are not configured for U.S. English, database restore operations may fail.

To set these language and locale values, follow this procedure:

-
- Step 1** Log on to the Windows 2003 Server machine as an Administrator and open the Control Panel.
- Step 2** Double-click **Regional and Language Options**.
- Step 3** To set the User Locale, click the **Regional Options** tab and select **English (United States)** in the Standards and Formats area. Click **Apply**.
- Step 4** To set the Language, click the **Languages** tab and click **Details and** set all values to US English.
- Step 5** To set the System Locale, click the **Advanced** tab and set the Language for non-Unicode programs to **English (United States)**. Click **OK**.
- Close the Control Panel.

Virtual Machine Support

Administrators can create a VMware image of the Management Center for Cisco Security Agents and maintain it on the VMware ESXi 3.5 hypervisor. A VMware CSA MC gives administrators flexibility by giving them remote access to the MC and eliminates the expense of buying a separate physical server.

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

- The virtual CSA MC must meet all the requirements for a CSA MC as described in [Table 1-1 on page 1-4](#).
- Administrators can manage hosts using a virtual CSA MC.
- A virtual CSA MC can be installed along with the Microsoft SQL Server Express database.
- One or two virtual CSA MCs can work with a remote Microsoft SQL Server 2005 (or 2000) database.
- Virtual CSA MCs can be used in a High Availability solution described in *Management Center for Cisco Security Agents High Availability White Paper*.

The CSA MC installed on VMware does have these limitations:

- Using VMware “snapshots” of the CSA MC is not supported.

- The sizing requirements for a VMware CSA MC are different than an MC on a physical system. See [Scalable Deployments, page 1-19](#) for more information about how a virtual MC scales.

The following outline provides information about installing CSA MC on a VMware image. This procedure assumes you have experience with virtualized machines and environments:

-
- Step 1** Installing VMware ESXi as described at VMware.com at this URL:
<http://www.vmware.com/products/esxi/>.
- Step 2** Load the ISO files for Windows 2003 R2 Server and create an image of a Windows 2003 R2 machine (as described in the [CSA MC System Requirements, page 1-4](#)).
- Step 3** Log on to your VMware ESXi server through a VMware Infrastructure Client in order to install and configure CSA MC 6.0.1. Follow any of these procedures to install the CSA MC:
- [Installing CSA MC with a Local Database, page 2-12](#)
 - [Installing CSA MC with a Remote Database, page 2-21](#)
 - [Information for Installing Multiple CSA MCs on Separate Systems, page 2-30](#)

Adobe Reader

Reports generated on the CSA MC can be created in PDF format. We recommend that you use the most recent version of Adobe Reader to view the reports.

Internationalization and Localization Support

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

Localization Support for Cisco Security Agents

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

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

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

Internationalization Support Tables

The following tables detail the level of support for each localized version of Windows operating systems.

Note that support for a localized operating system is different from having a localized agent.

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

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



Note

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

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

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

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

Look at the entry for Chinese (Simplified) in [Table 1-6](#). For Windows 2000 Professional with Service Pack 4, Cisco Security Agent has been localized (L) for Simplified Chinese, Cisco Security Agent has been tested (T) on the operating system, and Cisco Security Agent is supported (S) for use with the operating system.

Table 1-6 Windows 2000 Support

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

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

Table 1-7 Windows XP Support

	Professional, SP3	Home
Arabic	NS	NS
Chinese (Simplified)	L, T, S	L, S
Chinese (Simplified) (MUI)		

	Professional, SP3	Home
Chinese (Traditional)	T, S	S
Chinese (Traditional) (MUI)		
Chinese (Hong Kong)	S	S
Czech	S	S
Danish	T, S	S
Danish (MUI)		
Dutch	S	S
English (Canadian)	T, S	S
English (UK)	T, S	S
English (US)	L, T, S	L, S
Finnish	S	S
French	L, T, S	L, S
French (MUI)		
French (Canadian)	T, S	S
French (Canadian) (MUI)		
German	L, T, S	L, S
German (MUI)		
Greek	S	S
Hebrew	T, S	NS
Hebrew (MUI)		
Hungarian	S	S
Italian	L, T, S	L, S
Italian (MUI)		
Japanese	L, T, S	L, S
Japanese (MUI)		
Korean	L, T, S	L, S
Korean (MUI)		
Norwegian	S	S
Polish	L, T, S	L, S
Polish (MUI)		
Portuguese (Brazilian)	L, T, S	L, S
Portuguese (Brazilian) (MUI)		
Russian	L, T, S	L, S
Russian (MUI)		
Spanish	L, T, S	L, S
Spanish (MUI)		

	Professional, SP3	Home
Swedish	S	S
Turkish	S	S

Table 1-8 Windows 2003 Support

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

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

Table 1-9 Windows Vista Support

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

	Standard	Web	Enterprise, SP1
Polish	L, S	L, S	L, T, S
Polish (MUI)			
Portuguese (Brazilian)	L, S	L, S	L, T, S
Portuguese (Brazilian) (MUI)			
Russian	L, S	L, S	L, T, S
Russian (MUI)			
Spanish	L, S	L, S	L, T, S
Spanish (MUI)			
Swedish	S	S	S
Turkish	S	S	S

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

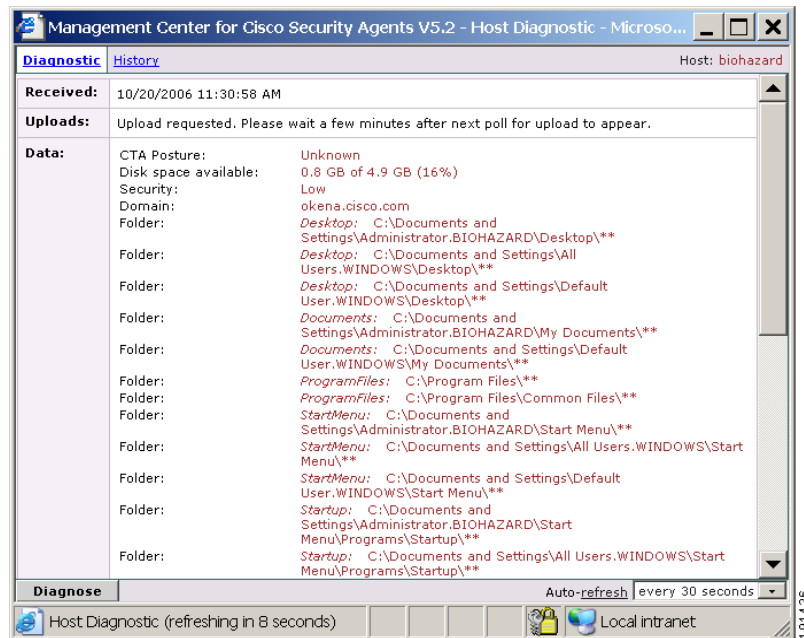
If the previous operating system tables do not indicate that CSA is localized (L) then the system administrator is responsible for checking to ensure that the tokens are in the language they expect and the directory path is the one they intend to protect.

Verifying Language Tokens

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

- Step 1** Log on to CSA MC as a user with configure or deploy privileges and switch to **Advanced Mode**.
- Step 2** From the CSA menu bar, mouseover **Systems** and select **Hosts** from the drop-down menu.
- Step 3** Click the link to the host name using the language you want to verify.
- Step 4** In the Host Status area, click the **Detailed Status and Diagnostics** link.
- Step 5** Click the **Diagnose** button.

Look at the folder information in the Data area of the Diagnosis Data page. (See [Figure 1-3](#).) 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 1-3 *Diagnosis for Localized Host*

Scalable Deployments

This release of CSA offers scaling of agents to 100,000 systems. To reach this deployment number, there are recommended multi-tiered CSA MC server system hardware, CPU, and memory requirements. Please refer to [Hardware Sizing, page 1-19](#).

Hardware Sizing

This section provides three server configuration examples and three hardware configuration examples. The server and hardware combinations will be charted in three tables providing information on how many agents can be deployed using each server and hardware configuration combination. This should give you an idea of how to configure CSA to scale up to a 100,000 agent deployment.

Server Configurations:

For the purpose of this guide, we will use three server configuration examples.

1. Single server
2. Two servers: one server for polling and configuration, one database server
3. Three servers: one server for polling, one server for configuration, one database server

Hardware Configurations:

We will use the following hardware configurations.

1. Single processor Pentium 4 (3Ghz+) with 2 GB RAM
2. Dual processor Xeon (2.5 Ghz+) with 4 GB RAM
3. Quad processor Xeon (2.5 Ghz+) with 8 GB RAM
4. Eight-Way Xeon (2.5 Ghz+) with 8 GB RAM

The following tables approximate the number of agents you could deploy with each server configuration installed on one of four hardware configurations provided.

Table 1-10 Server Configuration 1: Single Server

Hardware Configuration	Number of agents supported by CSA MC on physical server	Number of agents supported by CSA MC on virtual server
Hardware Configuration 1	2,500	1,000
Hardware Configuration 2	5,000	2,500
Hardware Configuration 3	10,000	5,000
Hardware Configuration 4	20,000	not applicable

Table 1-11 Server Configuration 2: Two Servers

Hardware Configuration	Number of agents supported by CSA MC on physical server	Number of agents supported by CSA MC on virtual server
Hardware Configuration 1	7,500	2,500
Hardware Configuration 2	15,000	7,500
Hardware Configuration 3	30,000	20,000
Hardware Configuration 4	75,000	not applicable

Table 1-12 Server Configuration 3: Three Servers

Hardware Configuration	Number of agents supported by CSA MC on physical server	Number of agents supported by CSA MC on virtual server
Hardware Configuration 1	10,000	2,500
Hardware Configuration 2	20,000	7,500
Hardware Configuration 3	50,000	30,000
Hardware Configuration 4	100,000	not applicable

Software Considerations

- CSA MC is only supported on Windows 2003 R2 Standard and Enterprise operating systems. Only Hardware Configurations 1 and 2 (referenced in previous tables) support Windows 2003 R2 Standard. Hardware Configuration 3 with 8GB RAM requires Windows 2003 R2 Enterprise to take advantage of the increased memory. Refer to the Microsoft web site product information section for details.
- To support any deployment over 1,000 agents, you should use Microsoft SQL Server 2005 in lieu of Microsoft SQL Server Express. Only Hardware Configuration 1 supports Microsoft SQL Server 2005 Workgroup or Standard editions with their 4GB RAM limitation.



Note

Your memory consumption needs should dictate your CSA MC operating system choice, i.e. Windows 2003 R2 Standard and Enterprise.

Configuration Recommendations for Scalability

If you intend to scale to a deployment of approximately 100,000 agents, there are some configuration recommendations you should consider:

Set Polling Interval

With 100,000 agents deployed across your enterprise, you want to ensure that no more than 20 agents are communicating with the MC approximately every second or so. Therefore, with a deployment of this size, it is recommended that you set the polling interval to 24 hours and enable polling hints.

Use Content Engines

For large deployments, it is highly recommended that you use content engines with transparent web caching. It makes sense to direct groups of agents to different content engines in large deployment scenarios. Content engines reduce the load on the MC by caching rule downloads and software updates.

Factors in Network Sizing

You can use the following data points for computing product network usage. The following numbers average tasks based on the upper limit of a 100,000 agent deployment.

Agent and Configuration Statistics

- Number of agents: 100,000
- Polling interval: 24 hours
- Event retention: 60 days
- Event updates: 3 per agent per day

Task Size Statistics

- Hint message: 1 Kb
- Poll size: 2 Kb
- Event update size: 2.5 Kb
- Policy update size: 35 Kb
- Agent update size: 25,000 Kb
- Tracker (Application Behavior Investigation) (Product only): 100 Kb
- Tracker (Application Behavior Investigation) (Product and non-verbose network): 2,000 Kb
- Tracker (Application Behavior Investigation) (Product and verbose network): 8,000 Kb

Tracker (Application Behavior Investigation) Agent Installation Statistics

- Number of agents in Tracker (Product only) group: 1,000
- Number of agents in Tracker (Product and non-verbose network) group: 100
- Number of agents in Tracker (Product and verbose network) group: 10

Bandwidth Statistics

- Downstream from CSA MC: 1333.33 Kb/sec, continuous
- Upstream to CSA MC: 3600 Kb/sec, continuous
- Policy update (downstream): 5833.33 Kb/sec, during update timeframe
- Agent update (downstream): 2666666.67 Kb/sec, during update timeframe

As an example of how you could compute network load using the data points provided here, take 100,000 agents, each generating an average of 3 events per day, and multiply Event update size, by number of Event updates, by number of agents, per a time frame of your choosing and average out a network load.

Factors in Database Sizing

You can use the following data points for computing database sizing. The following numbers average table size based on the upper limit of a 100,000 agent deployment.

- Event table size: 11,707.02 Mb
- Formatted event table: 13,658.20 Mb
- Other tables: 20,000 Mb
- Total database size; 45,365.23 Mb



CHAPTER 2

Installing the Management Center for Cisco Security Agents

Overview

This chapter provides instructions for installing CSA MC. Once you have reviewed the preliminary information outlined in the previous chapter, you are ready to proceed.

It is through CSA MC that you create agent installation kits. The tools for creating agent kits are installed as part of CSA MC.

This chapter contains the following topics:

- [Licensing Information, page 2-2](#)
 - [PAK Certificates, page 2-2](#)
 - [License Types, page 2-2](#)
 - [License File Contents, page 2-3](#)
 - [Managing and Troubleshooting Licenses, page 2-4](#)
 - [Uploading a License, page 2-4](#)
- [File Integrity Check Instructions, page 2-5](#)
 - [File Integrity Check on Downloaded CSA Software, page 2-5](#)
 - [File Integrity Check on CSA Software Delivered on CD, page 2-6](#)
- [Upgrading from CSA V6.0 to CSA V6.0.1, page 2-7](#)
- [Migrating Configurations and Hosts to CSA V6.0.1 from CSA V5.2 and Earlier, page 2-7](#)
- [Upgrade and Migration Scenarios, page 2-8](#)
- [Overview of Installing CSA MC with Local and Remote DB, page 2-10](#)
 - [New Installation Configuration Options, page 2-10](#)
 - [Installing CSA MC with a Local Database, page 2-12](#)
 - [Installing CSA MC with a Remote Database, page 2-21](#)
 - [Information for Installing Multiple CSA MCs on Separate Systems, page 2-30](#)
 - [Installing CSA MC with a Previous Version's Database \(Same System Installation\), page 2-31](#)
 - [Installation Log, page 2-35](#)
- [Accessing Management Center for Cisco Security Agents, page 2-35](#)

- Local Access, page 2-36
- Remote Access, page 2-36
- Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1, page 2-37
 - Upgrading CSA MC with a Local or Remote Database from CSA V6.0 to V6.0.1, page 2-37
 - Upgrading Multiple CSA MCs with a Remote Database from CSA V6.0 to V6.0.1, page 2-38
- Migration Instructions, page 2-39
- Initiating Secure Communications, page 2-41
- Uninstalling Management Center for Cisco Security Agents, page 2-46
- Hotfix Information, page 2-47

Licensing Information

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. (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 [License Types, page 2-2](#) for more information.

The information contained in your CSA MC license includes the number of server-agent licenses that have been allotted to you. When you receive your license from Cisco, you should copy it to the system to which you are installing CSA MC (or to a file share accessible from the CSA MC system). Then you can upload the licenses you need for your enterprise. See [Uploading a License, page 2-4](#) for more information.

PAK Certificates

PAK certificates will be delivered in packages separate from the software, often arriving in multiple packages. It is strongly suggested that you wait until you have received all packages (software and certificates) before registering the PAK numbers at the link below. Often, certificates arrive before software. Once you register the PAK numbers, you will then be emailed the license file(s).

When you receive your PAK information via email or mail, you can register the files at the following URL. You must have a CCO account to reach this URL:

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



Note

If you have further licensing questions or are having trouble with your license, refer to the [Managing and Troubleshooting Licenses](#) section at the end of this document.

License Types

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

- A license for the **Management Console (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 [Uploading a License, page 2-4](#) 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.

License File Contents

The license for each product can arrive in a single *.lic file or in multiple *.lic files. For example, the following is an example of what is contained in an evaluation *.lic file. (Notice that all 4 items listed above are referenced in this single file.):

```
INCREMENT managementcenter cisco 1 09-apr-2005 uncounted \ VENDOR_STRING=Count=1
HOSTID=ANY ISSUER="Cisco Systems, Inc." \
NOTICE="<LicFileID>20050310082639273</LicFileID><LicLineID>1</LicLineID> \<PAK></PAK>"
TS_OK SIGN=BEE0095EFC0A
INCREMENT serveragent cisco 1 09-apr-2005 uncounted \VENDOR_STRING=Count=10 HOSTID=ANY
ISSUER="Cisco Systems, Inc."
\NOTICE="<LicFileID>20050310082639273</LicFileID><LicLineID>2</LicLineID> \<PAK></PAK>"
TS_OK SIGN=8E5A416A0C3C
INCREMENT desktopagent cisco 1 09-apr-2005 uncounted \
VENDOR_STRING=Count=25 HOSTID=ANY ISSUER="Cisco Systems, Inc."
\NOTICE="<LicFileID>20050310082639273</LicFileID><LicLineID>3</LicLineID> \<PAK></PAK>"
TS_OK SIGN=8282418012F8
INCREMENT profiler cisco 1 09-apr-2005 uncounted \
VENDOR_STRING=Count=1 HOSTID=ANY ISSUER="Cisco Systems, Inc."
\NOTICE="<LicFileID>20050310082639273</LicFileID><LicLineID>4</LicLineID> \<PAK></PAK>"
TS_OK SIGN=EB0183B81748
```

Notice that the license is for a particular part of the product, indicated by the first line of each license. For example:

```
"INCREMENT managementcenter. . ." is the license for the CSA MC.
"INCREMENT serveragent. . ." is the license for servers.
```

The number of seats is referenced in the “Count=x” part of the license.

Each of the licenses can arrive in a single file as well. So, for example, you can receive a *.lic file containing this information:

```
INCREMENT serveragent cisco 1 09-apr-2005 uncounted \VENDOR_STRING=Count=10 HOSTID=ANY
ISSUER="Cisco Systems, Inc."
\NOTICE="<LicFileID>20050310082639273</LicFileID><LicLineID>2</LicLineID> \<PAK></PAK>"
TS_OK SIGN=8E5A416A0C3C
```

This example license is only for 10 server licenses and nothing else. Usually this kind of license arrives when you order additional seats for servers or desktops for a particular operating system.

Managing and Troubleshooting Licenses

- All license files are stored in this directory on the CSA MC:
Program Files\Cisco\CSAMC\CSAMC<version #>\cfg
- Rename license files that you receive from Cisco to have a more descriptive name. For example, you may get a license called 123456789.lic. Rename that to reflect the contents of the license (e.g. server_100.lic). This will help you keep a quick-glance inventory of each license type and seat count.
- Never upload a license file that contains within the title “CORE”. This is not a CSA license and might cause system instability.
- Never edit the contents of the license file itself (though the name of the *.lic file itself is editable). It may look like a straight text file but any changes in the contents of the license file itself will render it invalid.
- Always remove or rename the license file stored in the
Program Files\Cisco\CSAMC\CSAMC<version #>\cfg directory of your CSA MC machines before attempting to reload the file. (You may have multiple CSA MC machines - remove/rename the files on all of them.)
- If you are having licensing issues, try to re-upload the licenses prior to contacting Cisco TAC. This means you should:
 - Stop the CSA MC HTTP Server service on your CSA MC machine(s).
 - Rename or delete all the *.lic files located in
Program Files\Cisco\CSAMC\CSAMC<version #>\cfg
 - Start the MC service

Upload the license(s), starting with the CSA MC license or the license that contains the CSA MC license first, via the CSA MC GUI. (Go to the Home page and click Update License Information.)

Uploading a License

Proceed with the installation of CSA MC first and then upload additional licenses for servers and desktops. You may use either of these methods to upload agent licenses.

Using the Home Page

You can upload licenses from the Home page in either **Simple** or **Advanced Mode**:

-
- Step 1** Login to the CSA MC as an administrator with “configure” privileges.
 - Step 2** Click **Home** to view the Home page.
 - Step 3** In the **Maintenance** area, click **Update License Information**.

- Step 4** In the **Update License Information** pop-up, browse to the license file by clicking the **Browse** button.
- Step 5** Once the license file is located, click the **Upload** button to copy the file into the CSA MC directory. You do **not** need to generate rules after uploading a license.

Using the Maintenance Menu

You can also upload licenses from choices in the Maintenance menu. This is available to users of Advanced Mode only.

-
- Step 1** Login to the CSA MC as an administrator with “configure” privileges.
- Step 2** Mouse-over the **Maintenance** in the menu bar and select **License Information**.
- Step 3** In the Update License Information area, browse to the license file by clicking the **Browse** button.
- Step 4** Once the license file is located, click the **Upload** button to copy the file into the CSA MC directory. You do **not** need to generate rules after uploading a license.

File Integrity Check Instructions

You can perform an integrity check on the files provided with this release of 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 authentic.

File Integrity Check on Downloaded CSA Software

-
- Step 1** Download CSA software from Cisco.com and save the file locally.
- Step 2** Extract the contents of the zip file to its own directory.
- Step 3** View the contents of the directory in Windows Explorer. Among the files extracted is a file named **cisco_V#_verify_digests.exe** where # stands for the CSA version number. For example, the file could be named **cisco_V6.0.1.90_verify_digests.exe**.
- Step 4** Double-click **cisco_V#_verify_digests.exe**. The pre-computed MD5 values of the files contained in the kit are displayed in a command prompt window.
- Step 5** At the **Enter kit directory [.] :** prompt, press **Enter**.
- If the hash computed by **cisco_V#_verify_digests.exe** is the same as that displayed in the previous step, the file is authentic and the output for the file is “OK”. See [Example 2-1 on page 2-6](#) for an example of this output.
 - If the hash computed by **cisco_V#_verify_digests.exe** is different than that displayed in the previous step, the file may not be authentic and the output for the file is “failure”. See [Example 2-2 on page 2-6](#) for an example of this output.



Note

If you receive a “failure” message, try downloading the CSA software again and re-running the **cisco_V#_verify_digests.exe** application. If you still receive a failure message, contact Cisco Technical Services.

File Integrity Check on CSA Software Delivered on CD

- Step 1** Insert the CSA software CD into the CD drive.
- Step 2** View the contents of the CSA software CD in Windows Explorer. Among the files is a file named **cisco_V#_verify_digests.exe** where # stands for the version number. For example, the file could be named **cisco_V6.0.1.90_verify_digests.exe**.
- Step 3** Double-click **cisco_V#_verify_digests.exe**. The pre-computed MD5 values of the files contained in the kit are displayed in a command prompt window.
- Step 4** At the **Enter kit directory [.] :** prompt, enter the drive letter for the CD drive, followed by a colon, and press **Enter**. For example, if the CD drive is assigned letter D, enter **D:** and press **Enter**.
- If the hash computed by **cisco_V#_verify_digests.exe** is the same as that displayed in the previous step, the file is authentic and the output for the file is “OK”. See [Example 2-1 on page 2-6](#) for an example of this output.
 - If the hash computed by **cisco_V#_verify_digests.exe** is different than that displayed in the previous step, the file may not be authentic and the output for the file is “failure”. See [Example 2-2 on page 2-6](#) for an example of this output.



Note

If you receive a “failure” message, contact Cisco Technical Services.

Example 2-1 Successful authentication of files output from **cisco_v#_verify_digests.exe**

```
Enter kit directory [.] :
```

```
Verifying kit files in directory '..'...
Autorun.inf : ok
Documentation\CSAMC_InstallGuide.pdf : ok
Documentation\CSAMC_ReleaseNotes.pdf : ok
Documentation\CSAMC_UserGuide.pdf : ok
DotNet\NetFx20SP1_x86.exe : ok
OpenSource\clamav\ClamAVsrc-0.93.zip : ok
OpenSource\clamav\csaclamutil.zip : ok
OpenSource\clamav\GMPsrc-4.1.zip : ok
OpenSource\reports\itext-src-1.3.1.tar.gz : ok
OpenSource\reports\jasperreports-1.3.1.tar.gz : ok
OpenSource\reports\jfreechart-1.0.5.tar.gz : ok
OpenSource\reports\jtds-1.2-dist.tar.gz : ok
OpenSource\reports\jtds-1.2-src.tar.gz : ok
setup.exe : ok
SQL\setup.bat : ok
SQL\SQLExpr32.exe : ok
v51\v51setup.exe : ok
```

```
Num of files in built kit = 17
Num of files in this kit, Verified = 17
All files in this kit were verified successfully!
```

Example 2-2 Failed authentication of files output from **cisco_v#_verify_digests.exe**

```
Enter kit directory [.] :
```

```
Verifying kit files in directory '..'...
Autorun.inf : ok
Documentation\CSAMC_InstallGuide.pdf : ok
```

```

Documentation\CSAMC_ReleaseNotes.pdf      : ok
Documentation\CSAMC_UserGuide.pdf          : failure
DotNet\NetFx20SP1_x86.exe                 : ok
OpenSource\clamav\ClamAVsrc-0.93.zip      : ok
OpenSource\clamav\csaclamutil.zip         : ok
OpenSource\clamav\GMPsrc-4.1.zip          : ok
OpenSource\reports\itext-src-1.3.1.tar.gz : ok
OpenSource\reports\jasperreports-1.3.1.tar.gz: ok
OpenSource\reports\jfreechart-1.0.5.tar.gz: ok
OpenSource\reports\jtds-1.2-dist.tar.gz  : ok
OpenSource\reports\jtds-1.2-src.tar.gz    : ok
setup.exe                                 : ok
SQL\setup.bat                             : ok
SQL\SQLExpr32.exe                         : ok
v51\v51setup.exe                          : ok

```

```

Num of files in built kit      = 17
Num of files in this kit, Verified = 16
Not all files in this kit were verified. Please check list above.

```

Upgrading from CSA V6.0 to CSA V6.0.1

If you have CSA V6.0 installed on your Windows Server 2003 R2 system, installing Management Center for Cisco Security Agents 6.0.1 upgrades version 6.0 to version 6.0.1. Upgrades are much simpler if you are reusing the same CSA V6.0 system.

After installing CSA 6.0.1, you can push software upgrades to 6.0 agents using the software update tools provided. Wherever the policies from the old version of CSA are exactly the same as the policies from the new version of CSA, the old policies are replaced by the new policies. Any rules that you changed, or policies you added to your V6.0 CSA MC will be maintained in the correct group after the upgrade.

After you have updated the hosts with the CSA 6.0.1 software, locate updated versions of policies that you deployed with CSA 6.0. Compare the contents of the new and old policies. Once you have reviewed the new policies and configured them for your deployment, you can distribute the new policies if you desire.

Upgrade scenarios are detailed in this chapter. See [Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1, page 2-37](#) for more information.

Migrating Configurations and Hosts to CSA V6.0.1 from CSA V5.2 and Earlier

If you have previous versions (V5.2, V5.1, V5.0, V4.5.x, or 4.0) of the product installed on your Windows 2003 R2 system, installing Management Center for Cisco Security Agents 6.0.1 does not upgrade those previous versions. CSA V6.0.1 coexists with V5.2 or V5.1. CSA V5.0 configurations and V4.x configurations need to be migrated to V5.1 before you can migrate them to CSA V6.0.1.

When migrating from V5.0, be sure to backup the local database before migrating. If you are reusing the same hardware, you must uninstall CSA MC V5.0 and VMS from your Windows 2000 system. You must then uninstall Windows 2000 and perform a clean installation of Windows 2003 R2 because you cannot install CSA V6.0.1 on Windows 2000.

**Caution**

Do not perform an operating system upgrade of Windows 2000 Server to Windows 2003 R2. Prior versions of system and SQL libraries may not be compatible with the CSA 5.2/6.0.1 environment running on Windows 2003 R2. After installing the clean version of Windows 2003 R2, you can install CSA 6.0.1 on your newly installed Windows 2003 system.

After installing CSA 6.0.1, you can migrate older V5.0.x configurations and hosts to your 6.0.1 CSA MC using migration tools that are provided.

The migration procedure is more straightforward if you are not reusing the same hardware. In that case, you could install Management Center for Cisco Security Agents 6.0.1 on the Windows 2003 system and migrate configurations and hosts from the Management Center for Cisco Security Agents 5.1, 5.0 or 4.5.x on the Windows 2000 system.

And if you are running Management Center for Cisco Security Agents 5.2 or 5.1 on Windows 2003, the migration is quite simple.

All migration scenarios mentioned here are detailed in this chapter.

Upgrade and Migration Scenarios

CSA V6.0.1 supports the following upgrade and migration scenarios:

- **Scenario 1 - Upgrading V6.0 to V6.0.1 - Same System:** Install V6.0.1 on the same machine as V6.0. The upgrade is done in place; there is no data migration. Use the [Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1, page 2-37](#).
- **Scenario 2 - Migrating V5.2 to V6.0.1 - Same System:** Install V6.0.1 on the same machine as V5.2. Data migration is done automatically. See [Migration Instructions, page 2-39](#) for more information.
- **Scenario 3 - Migrating V5.2 to V6.0.1 - Separate System:** Install V6.0.1 on a new machine. Data migration is done manually. See [Migration Instructions, page 2-39](#) to move V5.2 configurations and hosts to the newly installed V6.0.1 system.
- **Scenario 4 - Migrating V5.1 to V6.0.1 - Same System:** Install V6.0.1 on the same machine as V5.1. Data migration is done automatically. See [Migration Instructions, page 2-39](#) for more information.
- **Scenario 5 - Migrating V5.1 to V6.0.1 - Separate Systems:** Install V6.0.1 on a new machine. Data migration is done manually. See [Migration Instructions, page 2-39](#) to move V5.1 configurations and hosts to the newly installed V6.0.1 system.
- **Scenario 6 - Migrating V5.0 to V5.1 to V6.0.1 - Same System:** Follow this migration approach:
 - a. Backup CSA MC V5.0 database
 - b. Uninstall CSA MC V5.0
 - c. Uninstall VMS (Cisco Works)
 - d. Install a new Windows 2003 R2 OS on system. Do not perform an upgrade of Windows 2000 to Windows 2003 R2.
 - e. Install CSA MC V6.0.1
 - f. Specify 5.0 database migration during installation
 - g. CSA MC 5.1 is installed along with CSA MC 6.0.
 - h. Automatic migration occurs

- i. See [Migration Instructions, page 2-39](#) for more information.

You can install V6.0.1 on the same machine where V5.0 resided, once V5.0 and VMS are uninstalled, the database is backed up safely (if local DB) and the system is running a Windows 2003 R2 operating system. Then you can use the migration tools provided to access and migrate the backed-up V5.0 database while installing 5.1 and 6.0.1 MCs.

- **Scenario 7- Migrating V5.0 to V6.0.1 - Separate Systems:** Install V6.0.1 on a new Windows 2003 R2 system. See [Migration Instructions, page 2-39](#) to move V5.0 configurations and hosts to the newly installed V6.0.1 system.
- **Scenario 8 - Migrating V4.5.x or 4.0.3 (4.x) to V6.0.1 - Same Systems:** If you are running CSA MC V4.5.x or 4.0.3 on the same system where V6.0.1 will be installed, you must first upgrade to CSA MC V5.0 before you can migrate to CSA MC V6.0.1 using one of the previously mentioned scenarios. Follow this migration approach:
 - a. Upgrade to CSA MC 5.0
 - a. Backup CSA MC V5.0 database
 - b. Uninstall CSA MC V5.0
 - c. Uninstall VMS (Cisco Works)
 - d. Install New Windows 2003 R2 OS on system. Do not perform an upgrade of Windows 2000 to Windows 2003 R2.
 - e. Install CSA MC V6.0.1
 - f. Specify 5.0 DB Migration during installation
 - g. CSA MC 5.1 is installed along with CSA MC 6.0.1
 - h. Automatic migration occurs
 - i. See [Migration Instructions, page 2-39](#) for more information
- **Scenario 9 - Migrating V4.5.x or 4.0.3 (4.x) to V6.0.1 - Separate Systems:** Install V6.0.1 on a new Windows 2003 R2 system. See [Migration Instructions, page 2-39](#) to move these older versions of CSA configurations and hosts to the newly installed V6.0.1 system.

**Note**

If you have a CSA MC with V5.1 and V5.2 already installed, you can not add V6.0.1 to the same system. There can only be two versions of CSA MC running on the same system. Either V5.1 or V5.2 must be uninstalled before V6.0 can be installed.

The CSA MC V6.0.1 installation does not automatically upgrade or overwrite CSA versions 5.2 or older. Content defined as “untrusted” by the earlier version of CSA will also be treated as untrusted content by CSA 6.0.1.

Ultimately, the migration process will allow you to import your older configuration items into the newly installed V6.0.1 system. It will also allow you to migrate hosts to V6.0.1. After installing V6.0.1, it is expected that you will spend some time examining how policies and other functionality has changed between versions and you will gradually apply the V6.0.1 policies to the migrated hosts.

**Caution**

For Scenario 5, you should not uninstall V5.1 until you have migrated all agents to V6.0.1. Once you install V6.0.1, you can apply hotfixes to the old V5.1 version, but you cannot install a V5.1 version of the product once the V6.0.1 version is installed in a one system installation scenario.

If you do apply hotfixes to an old V5.1 version after you install V6.0.1, you have to manually restart the CSA MC system for both MCs to begin running again.

CSA MC V6.0.1 creates a new directory structure if it is being installed on a new system. However, if CSA MC V5.2 is being upgraded to CSA MC V6.0.1, CSA MC V6.0.1 will use the existing CSA MC V5.2 directory structure. Refer to the following for a list of directory paths:

Table 2-1 Directory Paths for CSA Versions

CSA Version	Directory Path to CSA MC
CSA 6.0.1	Cisco\CSAMC\CSAMC60
CSA 6.0	
CSA 5.2	Cisco Systems\CSAMC\CSAMC52
CSA 5.1	Cisco Systems\CSAMC\CSAMC51
CSA 5.0	CSCOpX\CSAMC50

Overview of Installing CSA MC with Local and Remote DB

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.



Warning

Changing the system name after installing the CSA MC will cause communication problems between agents and the CSA MC. Therefore, you should not change the name of the server on which the CSA MC is installed. Changing the system name after installing CSA MC is not supported.



Tip

Give the server, on which the CSA MC resides, a generic name to avoid the need to rename it in the future.

New Installation Configuration Options

For a new product installation, you have three installation configuration options to consider before launching the CSA MC installation process.

- You can install CSA MC and the database on the same machine. (Select the **Local Database** radio button during the CSA MC installation.)

For a local database configuration, you have the option of installing CSA MC and the included Microsoft SQL Server Express Edition (provided with the product) on the same system if you are planning to deploy no more than 1,000 agents. In this case, the CSA MC installation also installs its own version of Microsoft SQL Server Express Edition on the system.

For a local database configuration, you also have the option of installing Microsoft SQL Server 2005 Service Pack 2 instead of using the Microsoft SQL Server Express Edition that is provided. Microsoft SQL Server Express Edition has a 4 GB database size limit. In this case, you can have CSA MC and Microsoft SQL Server 2005 on the same system depending on the number of agents

you are deploying (see [Scalable Deployments, page 1-19](#)). Note that if you are using SQL Server 2005, it must be licensed separately and it must be installed on the system before you begin the CSA MC installation.

See [Installing CSA MC with a Local Database, page 2-12](#) for this installation method.



Note There is no upgrade path from Microsoft SQL Server Express to Microsoft SQL 2005 Service Pack 2.



Note If your plan is to use SQL Server 2005, it is recommended that you choose one of the other installation configuration options rather than the local database configuration.



Note Microsoft SQL Server 2005 is the database version that will be used for this installation section, but you should note that SQL Server 2000 is also supported at this time.

- You can install CSA MC on one machine and install the database on a remote machine. (Select the **Remote Database** radio button during the CSA MC installation. Note that you must install a Cisco Security Agent on this remote database to protect this system. See [Microsoft SQL Server 2005 Remote Database Setup, page 2-22](#).)

Use this configuration option depending on the number of agents you are deploying (see [Scalable Deployments, page 1-19](#)). If you are using a separately licensed, managed, and maintained SQL Server 2005 database, SQL Server 2005 must be installed and configured on the remote system before you begin the CSA MC installation.

See [Installing CSA MC with a Remote Database, page 2-21](#) for this installation method.



Caution

If you are installing CSA MC and the database to multiple machines, make sure the clocks of each machine are in sync. If all clocks are not in sync, unexpected behavior may occur.

- You can install two CSA MCs on two separate machines and install the database on a remote machine. In this case, both CSA MCs use the same remote database. (Select the **Remote Database** radio button during the CSA MC installation. Note that you must install a Cisco Security Agent on this remote database to protect this system. See [Microsoft SQL Server 2005 Remote Database Setup, page 2-22](#).)

This is the recommended configuration if you are deploying more than 5,000 agents and are using a separately licensed, managed, and maintained SQL Server 2005 database. SQL Server 2005 must be installed and configured on the remote system before you begin the MC installations.

Using this configuration, you can deploy up to 100,000 agents. Having two CSA MCs lets you use one MC for host registration and polling and another MC for editing configurations.

See [Installing CSA MC with a Remote Database, page 2-21](#) for this installation method and read the important information at [Information for Installing Multiple CSA MCs on Separate Systems, page 2-30](#).

**Caution**

If you are installing two CSA MCs with one of the MCs residing on the machine where the database is installed, you must select the Remote Database radio button during the installation of both MCs. Even though one MC is “local” to the database, for the two MCs configuration to work properly, they must both be configured to communication with the database as though it were remote.

Installing CSA MC with a Local Database

If you are installing both CSA MC and the database to the same machine with the provided Microsoft SQL Server Express database, you should install Microsoft SQL Server Express Edition as part of the CSA MC installation. The CSA MC installation runs the Microsoft SQL Server Express installation program choosing the Microsoft SQL Server Express settings the MC needs. During the MC installation, if you want to install the database on a different system drive from the MC, the install prompts allow you to do this.

It is recommended that you install SQL Server Express via the CSA MC installer. If you install it manually as implied that you might do in step 8 on [page 2-14](#), you should know that if you take the SQL Server Express defaults, then your subsequent CSA MC installation will fail. (See Caution below)

**Caution**

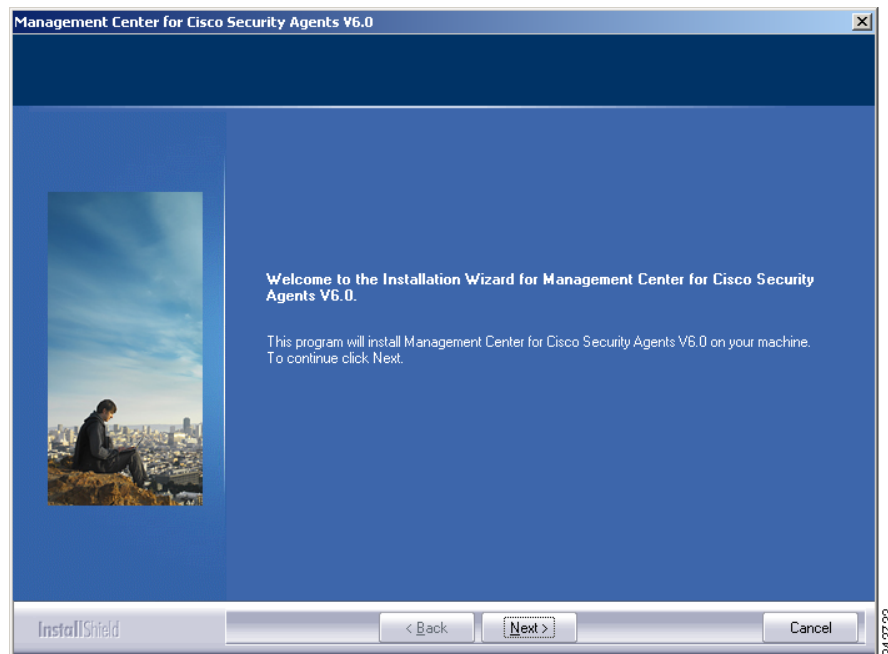
Because Microsoft SQL Server Express is provided on the CD separately, you might be tempted to install it yourself manually. This is not recommended. If you install it yourself, you must select specific non-default settings for the database to work with CSA MC. Those settings are provided in another section here, see [Microsoft SQL Server Express Manual Installation Settings, page 2-20](#). But again, this is not the recommended deployment.

If you want to install a local Microsoft SQL Server 2005 or 2000 database rather than using Microsoft SQL Server Express, install the Microsoft SQL Server 2005 or 2000 before you install the CSA MC. See [Microsoft SQL Server 2005 and 2000 Local Installation Notes, page 2-19](#) for important information.

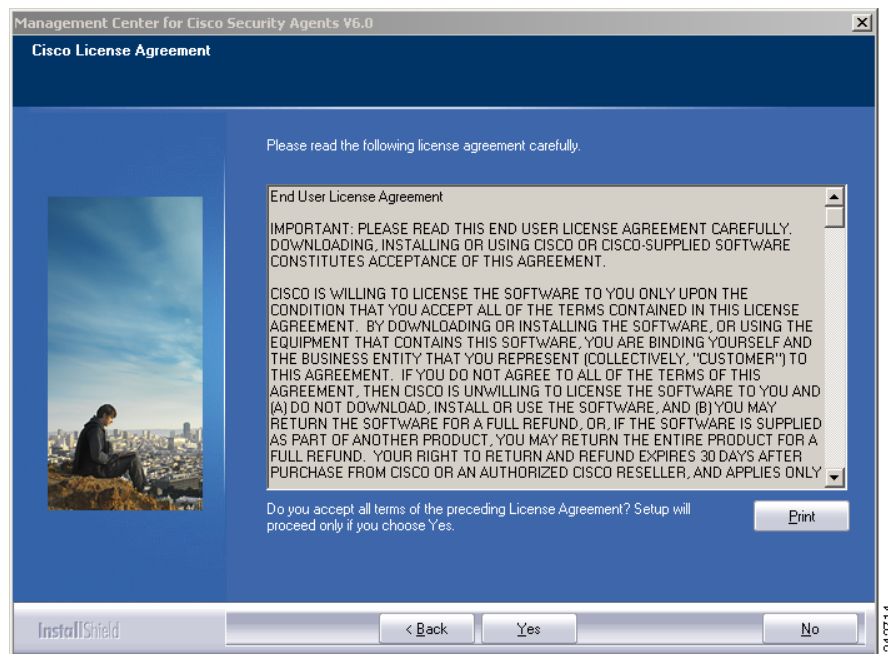
Before beginning, exit any other programs you have running on the system where you are installing CSA MC.

To install the CSA MC, follow this procedure:

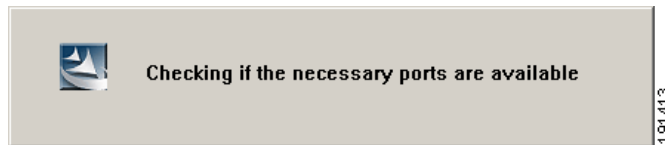
-
- Step 1** Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - Step 2** Put the Management Center for Cisco Security Agents CD into the CDRom drive. The welcome screen appears. Click **Next** to begin the installation. See [Figure 2-1](#). (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)

Figure 2-1 CSA MC Installation Welcome Screen

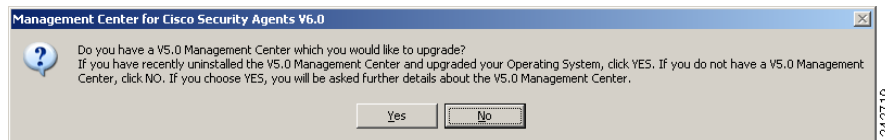
- Step 3** After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.
- Step 4** When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See [Figure 2-2](#).

Figure 2-2 CSA MC End User License Agreement

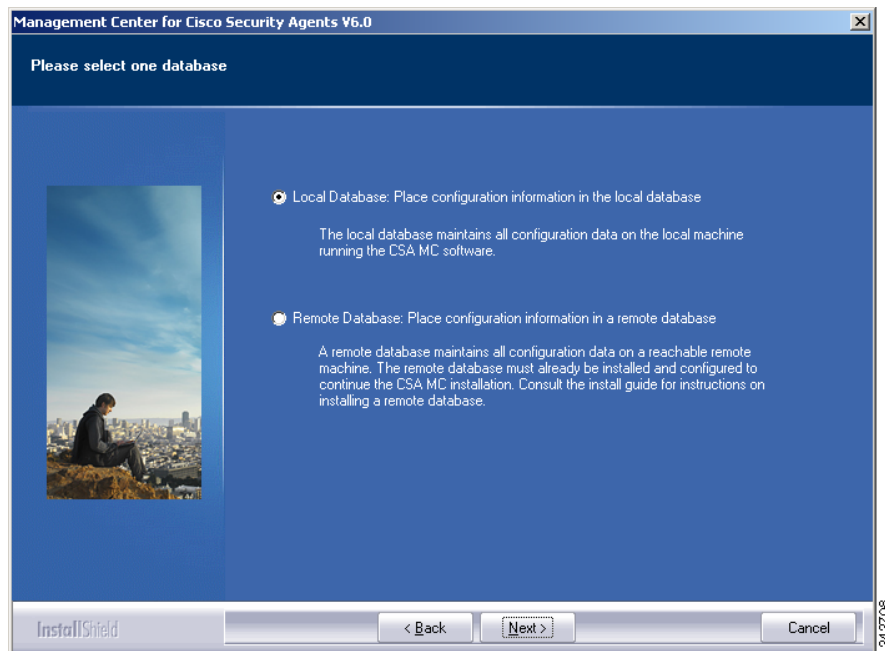
- Step 5** The installation checks if the needed ports are available.

Figure 2-3 *Installation Port Check*

- Step 6** The installation next asks if you are upgrading from a V5.0 Management Center. In this case, click **No** to continue. See [Figure 2-4](#). (If you are upgrading from a V5.0 Management Center, click **Yes** and refer to [Installing CSA MC with a Previous Version's Database \(Same System Installation\)](#), page 2-31.)

Figure 2-4 *Upgrade Question Window*

- Step 7** The install then begins by prompting you to select a database location. In this case, you will keep the default selection of **Local Database** and click the **Next** button. See [Figure 2-5](#).

Figure 2-5 *Database Setup Type*

- Step 8** If installing locally, the installation next checks to see if you have Microsoft SQL Server Express Edition installed. CSA MC uses Microsoft SQL Server Express Edition for its local configuration database. If this software is not detected, you are prompted to install it. See [Figure 2-6](#).

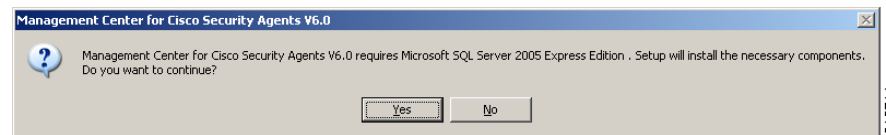
**Note**

For installations exceeding 1,000 agents, it is recommended that you install Microsoft SQL Server 2005 instead of using the Microsoft SQL Server Microsoft SQL Server Express Edition that is provided with the product. Refer to [New Installation Configuration Options](#), page 2-10 for more information. If you are using Microsoft SQL Server 2005, refer to [Microsoft SQL Server 2005 and 2000 Local Installation Notes](#), page 2-19 for details.

**Caution**

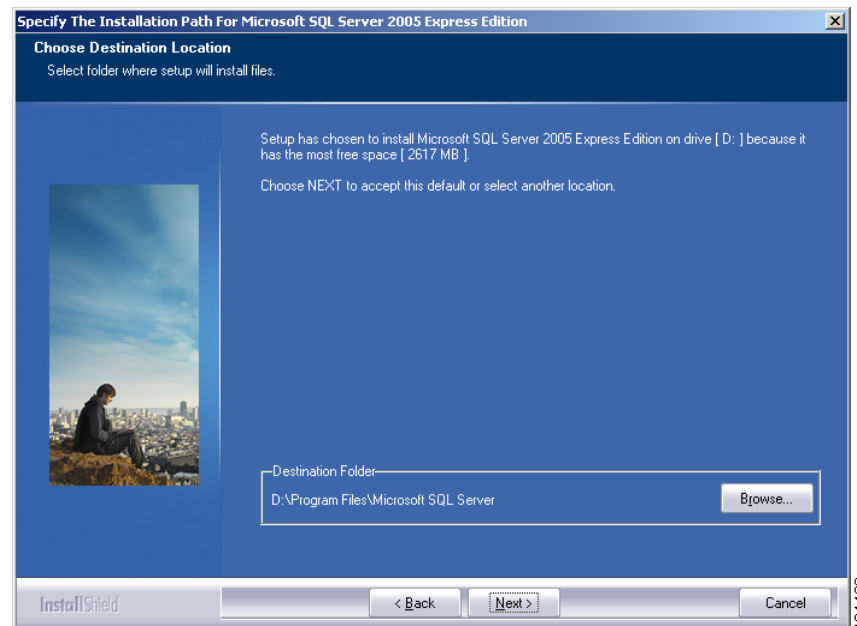
On a system where CSA MC has not previously been installed, the setup program first installs Microsoft SQL Server Express Edition. If the CSA MC installation detects any other database type attached to an existing installation of Microsoft SQL Server Express Edition, the installation will abort. This database configuration is not qualified.

Figure 2-6 *Install Microsoft SQL Server Express Edition Prompt*



After clicking **Yes**, you are prompted to select an Microsoft SQL Server Express Edition install directory.

Figure 2-7 *SQL Server Installation Directory Selection*



Step 9 You are prompted to select a CSA MC directory installation path. Either accept the default installation path or browse to a different path for installation.

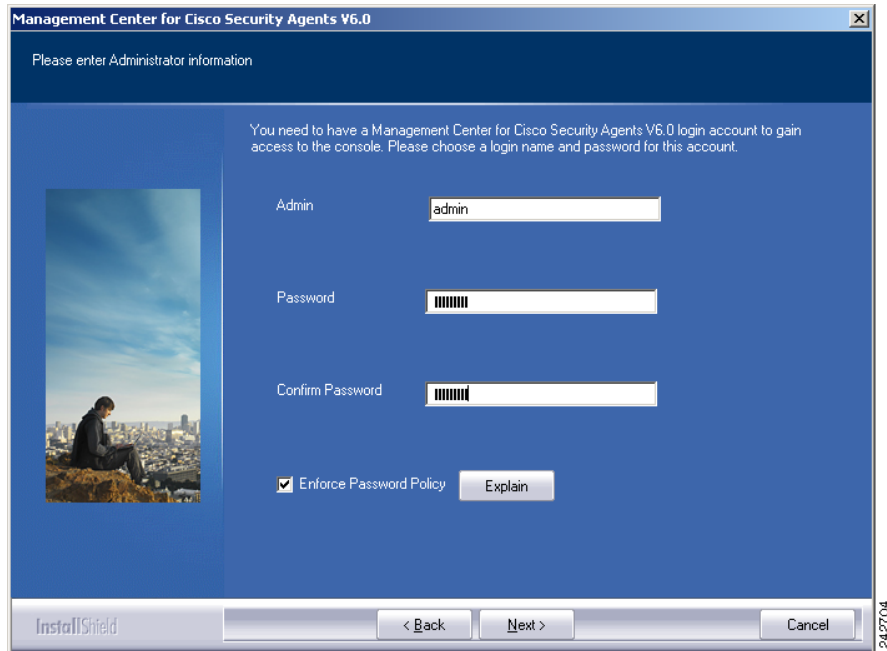
Step 10 You are next prompted to enter Administrator Name and Password information. This is the user name and password you will use to login in to CSA MC. Checking the **Enforce password policy** checkbox places these constraints on the password you enter:

- Password cannot be the same as, or contain, the login name
- Password must be between 6 and 32 characters long
- Password must contain characters from at least three of the following classes:
 - lower case letters
 - upper case letters
 - digits

- non-alphanumeric characters

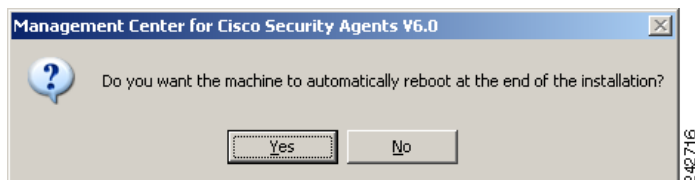
See [Figure 2-8](#). Enter this information and click **Next**.

Figure 2-8 Enter Administrator Name and Password

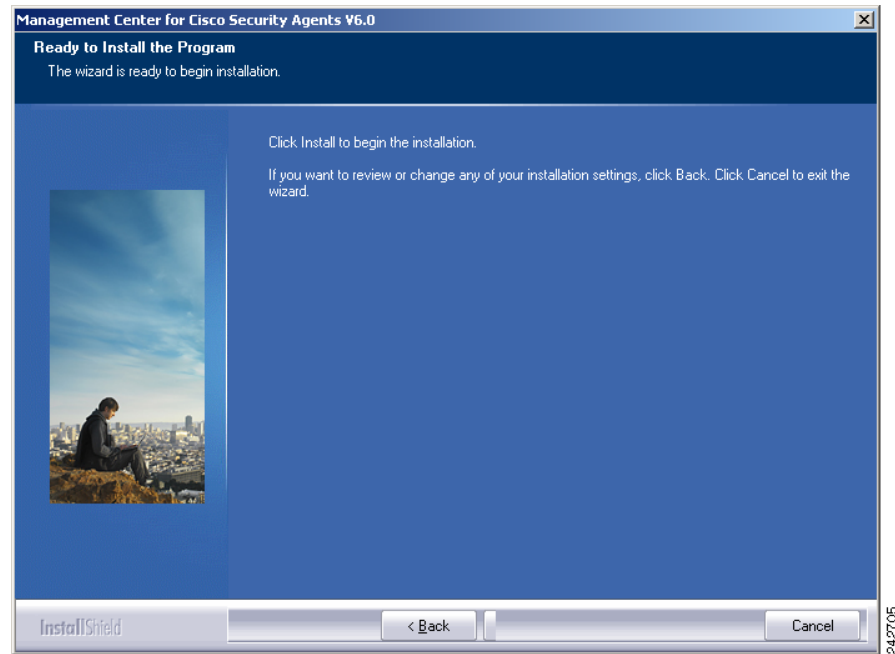


- Step 11** You are next prompted to select whether or not you want the system to automatically reboot once the installation is complete (see [Figure 2-9](#)). It is required that you reboot the system after the installation is complete whether you select **Yes** to have it done automatically or you choose to manually reboot at the end.

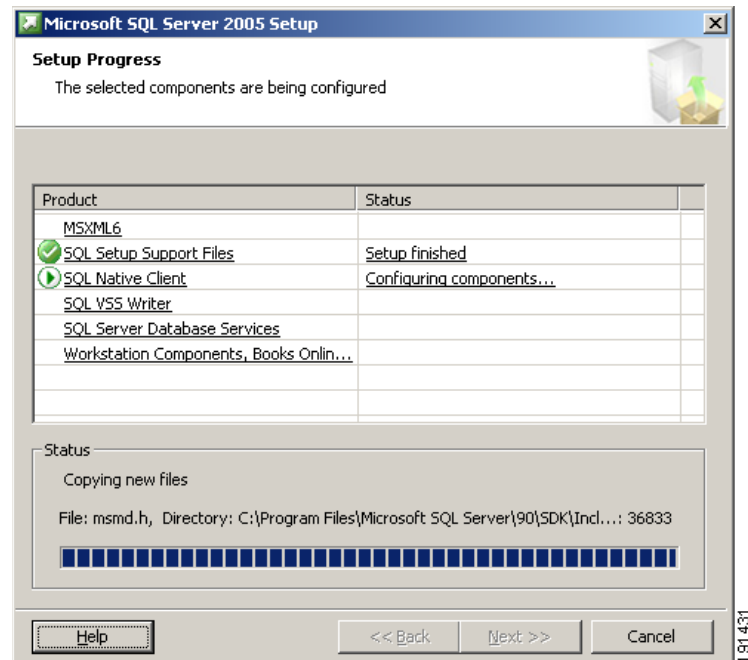
Figure 2-9 Automatic Reboot Option Prompt



- Step 12** You are next prompted to begin the installation. Click the **Install** button (see [Figure 2-10](#)).

Figure 2-10 *Begin Install*

SQL Server Express Edition installs .NET Framework on the system and continues to perform configuration tasks (see [Figure 2-11](#)). The SQL Server Express Edition windows that appear require no user action.

Figure 2-11 *SQL Server Express Edition Configuration Status Window*

When the Microsoft SQL Server Express Edition installation finishes, the CSA MC installation automatically begins again, copying the necessary files to your system, (see [Figure 2-12.](#)) and then installing them (see [Figure 2-13.](#)).

Figure 2-12 Copy Files

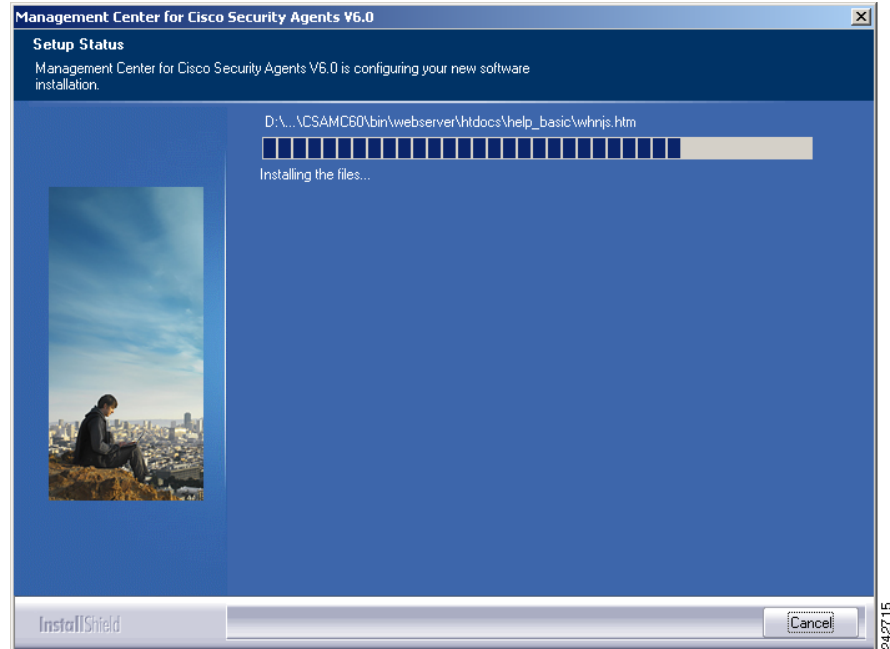
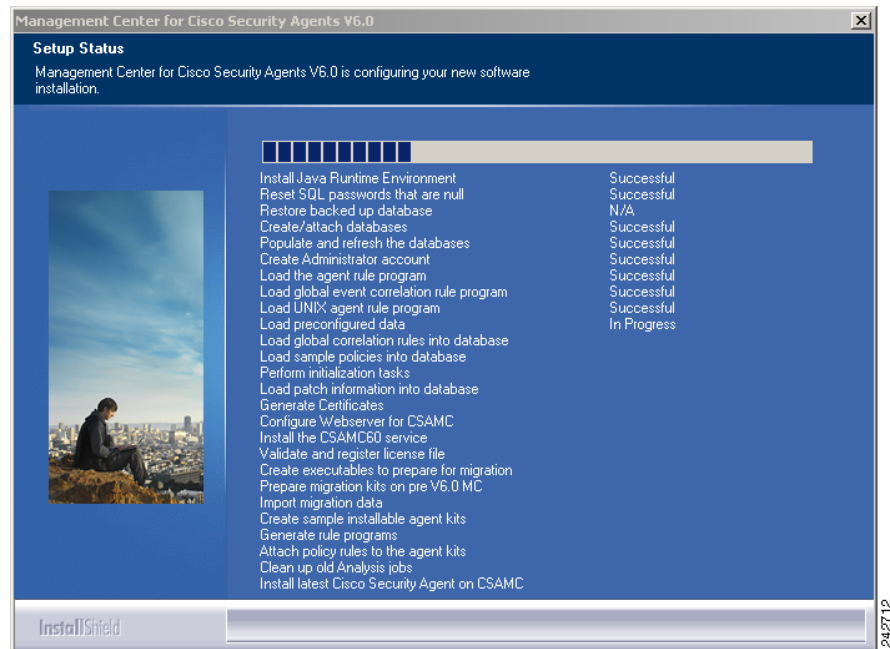


Figure 2-13 Installation Proceeds



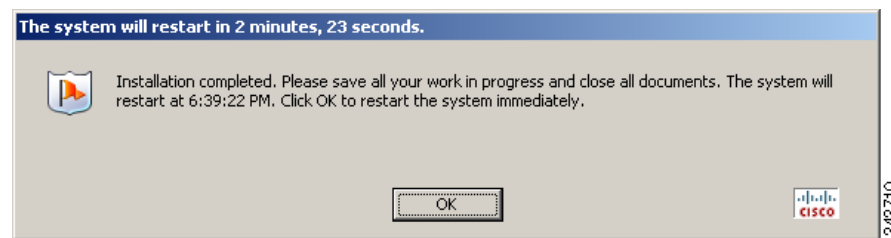
**Note**

When the CSA MC installation completes, an agent installation automatically begins. It is recommended that an agent protect the CSA MC system. (You may uninstall the agent separately if you choose, but this is not the recommended configuration.)

If an agent is already installed on a system to which you are installing CSA MC, that agent will automatically be upgraded by the CSA MC agent installation.

When the MC and agent installs are complete, if you selected to have the system reboot automatically, you are prompted that the automatic reboot will occur within 5 minutes. If you selected not to have the system reboot automatically, it is required that you manually reboot the system at this time.

Figure 2-14 Automatic Reboot Prompt



Once the system reboots, you should login to the MC and copy the license key file(s) you received from Cisco Systems to your CSA MC. CSA MC ships with and automatically uses a license for the MC and local agent. See [Uploading a License, page 2-4](#) for more information.

Microsoft SQL Server 2005 and 2000 Local Installation Notes

**Note**

The following instructions are only intended for administrators choosing to install CSA MC and Microsoft SQL Server 2005(or 2000) to the same system. These instructions are not for administrators using CSA MC with a remote database. If you are choosing to use Microsoft SQL Server 2005 as a remote database, information is provided in the section titled [Installing CSA MC with a Remote Database, page 2-21](#). All instructions apply to both Microsoft SQL Server 2005 and 2000 unless otherwise specified.

**Note**

No additional database should be present on the server running CSA MC.

**Caution**

CSA MC supports Microsoft SQL Server 2005 with Service Pack 0, Service Pack 1, or Service Pack 2. You should note that if you install a SQL Server 2005 build that is lower than build number 2153 (released after SP1), the service “SQL Server Integration Services” will fail upon system reboot. You can manually start the service or you can upgrade to Microsoft SQL Server 2005 SP1 build number 2153 or higher.

For local database installations exceeding 1,000 agents, it is recommended that you install Microsoft SQL Server 2005 instead of using the Microsoft SQL Server Express Edition that is provided with the product. Microsoft SQL Server Express Edition has a 4 GB limit. SQL Server 2005 must be licensed separately and it must be installed on the local system before you begin the CSA MC installation.

In order for Microsoft SQL Server 2005 to function properly with CSA MC, you must select certain settings during the installation. Those settings are listed here. (Refer to your Microsoft SQL Server 2005 manual for detailed installation information.)

**Note**

You should not change the default instance name of “MSSQLSERVER” for the SQL Server 2005 database. If you change this, the CSA MC installation will not detect the database.

When installing Microsoft SQL Server 2005, choose the default settings except in the following instances:

- In the **Setup Type** installation window, choose the **Typical** radio button and in the **Destination Folder** section, click the various **Browse** buttons to install SQL Server on the system.
- In the **Components to Install** dialog box, select **SQL Server Database Services** and **Analysis Services**.
- In the **Instance Name** dialog box, select **Default Instance**.
- In the **Service Account** installation dialog box, choose **Use the built-in System Account** radio button and specify **Local System**. In the **Start Services at the End of Setup** area, select **SQL Server** and **Analysis Services**.
- In the **Authentication Mode** dialog box, select **Windows Authentication Mode**.
- (For Microsoft SQL Server 2000 only) In the **Choose Licensing Mode** installation window, select the **Per Seat for** radio button and then increment the **devices** number field to a positive value—at least 1 or 2.

(For Microsoft SQL Server 2005 only) Reboot the system.

(For Microsoft SQL Server 2000 only) Reboot the system and install the most recent service pack for SQL Server 2000. CSA MC has been qualified with Service Pack 4. When installing the service pack, choose the default settings except in the following instances

- When you install the service pack, in the **Installation Folder** screen, you should select a drive that has at least 140 MB of free space. For the service pack installation, choose the default settings in all instances.
- In the **SA Password Warning** installation screen, select the **Ignore the security threat warning, leave the password blank** radio button.
- In the **SQL Server 2000 Service Pack Setup** installation screen, select the **Upgrade Microsoft Search and apply SQL Server 2000 SP4 (required)** checkbox.

Microsoft SQL Server Express Manual Installation Settings

Because Microsoft SQL Server Express is provided on the CD separately, during a local database MC installation, you might be tempted to install Microsoft SQL Server Express yourself manually. This is not recommended. If you install it yourself, you must select specific non-default settings for the database to work with CSA MC. Those settings are provided here. But again, this is not the recommended deployment.

**Caution**

If you are installing both CSA MC and the database to the same machine with the provided Microsoft SQL Server Express database, you should install Microsoft SQL Server Express Edition as part of the CSA MC installation. The CSA MC installation runs the Microsoft SQL Server Express installation program choosing the Microsoft SQL Server Express settings the MC needs. During the MC installation, if you want to install the database on a different system drive from the MC, the install prompts allow you to do this.

During the Microsoft SQL Server Express manual installation, you can simply leave all the default settings except in the following cases:

- **Registration information** dialog - UNCHECK the “Hide advanced configuration options” option.
- **Instance name** dialog - Choose the “Default instance” option.

Service Account - Select “User the built-in system account” and from the drop down menu, select “Local System”.

Installing CSA MC with a Remote Database

If you are installing one or two CSA MCs and their corresponding database to different machines, you must first install and properly configure Microsoft SQL Server 2005 or Microsoft SQL Server 2000 on the remote system according to Microsoft’s instructions. You should restrict access to this database machine as much as possible using any access control systems you already have in place on your network.

**Caution**

It is recommended that all installed CSA MCs and remote databases be placed on a private LAN. If you cannot provide a private LAN, then you should follow Microsoft’s recommendations for securing communication between database servers and application servers.

**Caution**

It is important that the time on the database server system closely match the time on the CSA MC system. Both systems must be in the same time zone and you should make sure both times are set correctly.

**Caution**

You must install a Cisco Security Agent on this remote database. This agent should be in the Servers–CSA Management Center– Secured Remote Database group. This group is hidden by default, you will need to change the visibility view on the Groups list page to “Show all items” to expose this group. You should install this agent after the last CSA MC has been installed and rebooted.

Microsoft SQL Server 2000 Remote Database Setup

**Note**

The following section contains overview information for setting up the Microsoft SQL Server 2000 database to work correctly with CSA MC. More detailed SQL Server configuration information should be obtained from your Microsoft documentation.

In order to enter the requested remote database information during the CSA MC installation, you must first setup the SQL Server database system by doing the following. (Note that these steps may be performed by your database administrators. The procedure is detailed after the bullet list.)

- Create an empty database.
- You must configure a new login ID and password and associate it with a new user ID which has the standard access rights on the CSA MC database, including db_ddladmin, db_datareader, and db_datawriter. **Note that the login ID and user ID must be identical.** (db_owner privileges are not required.)
- Make sure the default language is set to English. Note that you should not change the language default after CSA MC is installed. The SQL Server collision string must contain **Latin1_General**.
- Make sure that the database is configured to accept SQL Server authentication.
- You also need to create a Filegroup for the database called “analysis” and it must have at least one file attached.

More specifically, use the following procedure as a guideline to create a remote database on MS SQL Server 2000:

-
- Step 1** Right click your SQL Server. Select the **Security** tab and set “Authentication” to **SQL Server and Windows**. Then click **OK**.
- Step 2** Stop and start sql server.
- Step 3** Create new database “CSAMC601”.
- Step 4** Inside the DB properties, click **Filegroups** and create a new filegroup called ANALYSIS. Inside the DB properties, click **Data Files** and in the **File Name** field, type “csamcanalysis”, and in the Filegroup field type “ANALYSIS”. Then click **OK**.
- Step 5** Expand the “security” + and right-click Logins. Then create a new login. Use SQL Server Authentication. Set Defaults -> Database = csamc60 database.



Note Do not click anything under “server roles”.

- Step 6** In the “database access” section, permit access to csamc60 and give the role of db_ddladmin. db_datareader and db datawriter permissions must also be provided. Click **OK**.
- Step 7** Restart the server.

Microsoft SQL Server 2005 Remote Database Setup



Note

The following section contains overview information for setting up the Microsoft SQL Server 2005 database to work correctly with CSA MC. More detailed SQL Server configuration information should be obtained from your Microsoft documentation.

**Caution**

CSA MC supports Microsoft SQL Server 2005 with Service Pack 0, Service Pack 1, or Service Pack 2. You should note that if you install a SQL Server 2005 build that is lower than build number 2153 (released after SP1), the service “SQL Server Integration Services” will fail upon system reboot. You can manually start the service or you can upgrade to Microsoft SQL Server 2005 SP1 build number 2153 or higher.

In order to enter the requested remote database information during the CSA MC installation, you must first setup the SQL Server database system by doing the following. (Note that these steps may be performed by your database administrators. The procedure is detailed after the bullet list.)

- Create an empty database.
- You must configure a new login ID and password and associate it with a new user ID which has the standard access rights on the CSA MC database, including db_ddladmin, db_datareader, and db_datawriter. Note that the login ID and user ID must be identical. (db_owner privileges are not required.)
- Right-click on the server name and view Properties. On the left side of the Properties panel, click Permissions. In the table containing the logins and roles, click on the user id that has been created for CSA MC. In the explicit permissions list for the user, for the permission “View Server State”, check the box for “Grant”.
- Expand the created CSA MC Database tree and click Security. In the Security pane for your database, right-click Schemas and create a new schema with a name that is identical to the user id and login id. Click the Search button and locate the user. Attach this user to the new schema and click OK. Return to the Users in the database. Double-click the user id and select the newly created schema as the default schema.
- Make sure the default language is set to English. Note that you should not change the language default after CSA MC is installed. The SQL Server collision string must contain **Latin1_General**.
- Make sure that the database is configured to accept SQL Server authentication.
- You also need to create a file group for the database called “analysis” and it must have at least one file attached.

Use the following procedure as a guideline for creating a database on MS SQL 2005:

- Step 1** In the Object Explorer column on the left, right-click the name of your SQL Server and select **Properties**.
- Step 2** In the Server Properties dialog box, in the left hand column, select **Security**. Select the **SQL Server and Windows Authentication** radio button in the Server authentication area. Click **OK**.
- Step 3** In the Object Explorer column on the left, right-click the name of your SQL Server and select **Restart** to restart the SQL Server service.
- Step 4** In the Object Explorer column on the left, click **Databases** for your SQL server. In the Databases pane, right-click in the background and select **New Database**. Give the database a name such as “CSAMC601”. Click **OK**.
- Step 5** In the Databases pane, right-click the database you just created and click **Properties**.
- Step 6** Select **Filegroups** in the left column and then click **Add**. Name the new Filegroup **ANALYSIS**.
- Step 7** In the Database Properties dialog, click **Files** (or Data Files) and then click **Add**. Give the File a Logical Name, for example, **csamc601_analysis**. Click the Filegroup column for the file and select **ANALYSIS** from the list box. The Filegroup designation must be ANALYSIS. Click **OK**.

Step 8 Create an SQL Server Login:

- a. Under the name of your SQL server in the left hand column, select **Security**.
- b. Right-click **Logins** and click **New Login**.
- c. Specify a **Name** for the new user. Select the **SQL Server authentication** radio button and enter a **Password** for the new user. Specify the name of your new database as the **Default database**.
- d. Click **OK**.



Note Do not click anything under “server roles”.

Step 9 Configure the SQL Server Login:

- a. In the Object Explorer column on the left, right-click your SQL Server and select **Properties**.
- b. Click **Permissions** in the Server Properties dialog box.
- c. In the **Logins or roles** window, select the SQL Server login you just created.
- d. In the **Explicit permissions for Login Name** window, select **View server state**. Select **Grant** and click **OK**.

Step 10 Create a database user:

- a. In the left hand column, expand **Databases** and then expand the tree for your new database. Click **Security**.
- b. In the Security pane for your database, right-click **Users** and click **New User**.
- c. Specify a **User name** and a **Login name** for the new user. Make these names the same as the name of the SQL Server user.
- d. In the **Schemas owned by this user** field, select **db_datareader**, **db_datawriter**, and **db_ddladmin**.
- e. In the Database role membership field, select **db_datareader**, **db_datawriter**, and **db_ddladmin**.
- f. Click **OK**.

Step 11 Create a database schema:

- a. In the Security pane for your database, right-click **Schemas** and select **New Schema**.
- b. In the **Schema name** and **Schema owner** fields, enter the name of the database user you created in the previous step.
- c. Click **OK**.

Step 12 In the Security pane for your database, double-click **Users**. Right-click the name of the database user you created and select **Properties**. In the Default schema field, enter the name of the database schema you created. Click **OK**.

Step 13 Restart the SQL server.

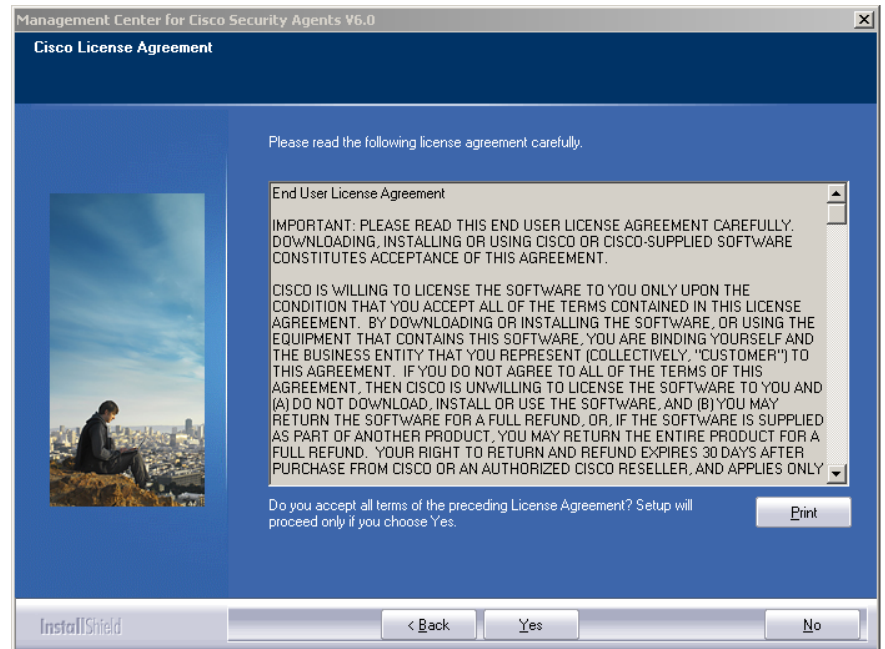
Installing CSA MC Using the Remote Database

Before beginning, exit any other programs you have running on the system where you are installing CSA MC. To install the CSA MC, do the following:

Step 1 Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.

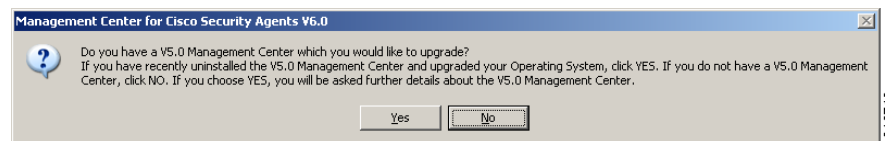
- Step 2** Management Center for Cisco Security Agents CD into the CDROM drive. The welcome screen appears. Click **Next** to begin the installation. (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)
- Step 3** The Management Center for Cisco Security Agents appears. After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.
- Step 4** When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See [Figure 2-15](#).

Figure 2-15 CSA MC End User License Agreement



- Step 5** The installation asks if you are upgrading from a V5.0 Management Center. In this case, click **No** to continue. See [Figure 2-16](#). (If you are upgrading from a V5.0 Management Center, click **Yes** and refer to [Installing CSA MC with a Previous Version's Database \(Same System Installation\)](#), page 2-31.)

Figure 2-16 Upgrade Question Window



- Step 6** The install begins by prompting you to choose a database setup type. In this case, you will select the **Remote Database** radio button and click the **Next** button.

When you select the Remote Database radio button, you are next prompted to enter the following information for the remote SQL Server database (see [Figure 2-17](#)):

- Name of the server
- Name of the database
- Login ID
- Password

Figure 2-17 *Remote Database Information*

Management Center for Cisco Security Agents V6.0

Please enter the database details

Server Name

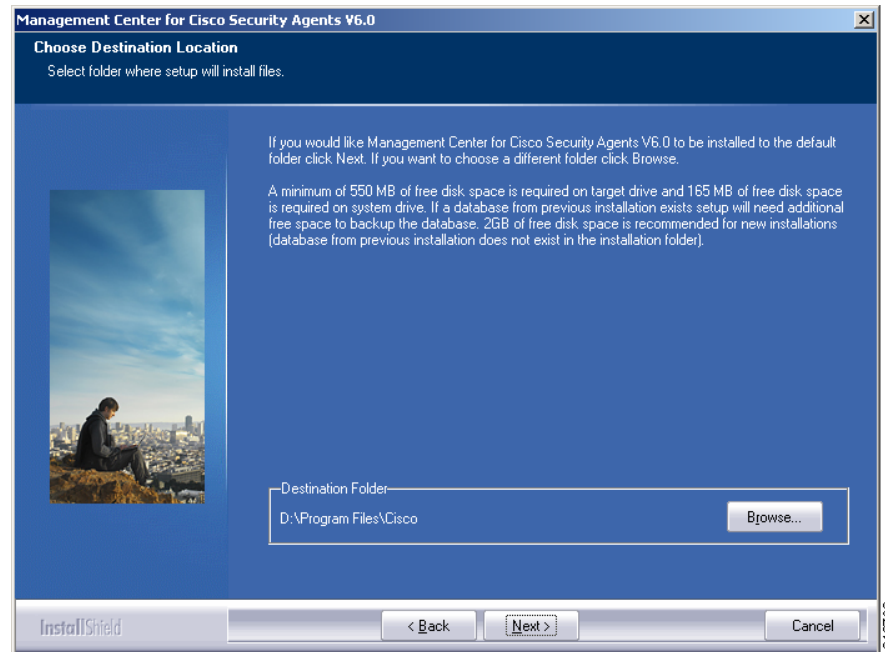
Database Name

User Name

Password

InstallShield < Back Next > Cancel

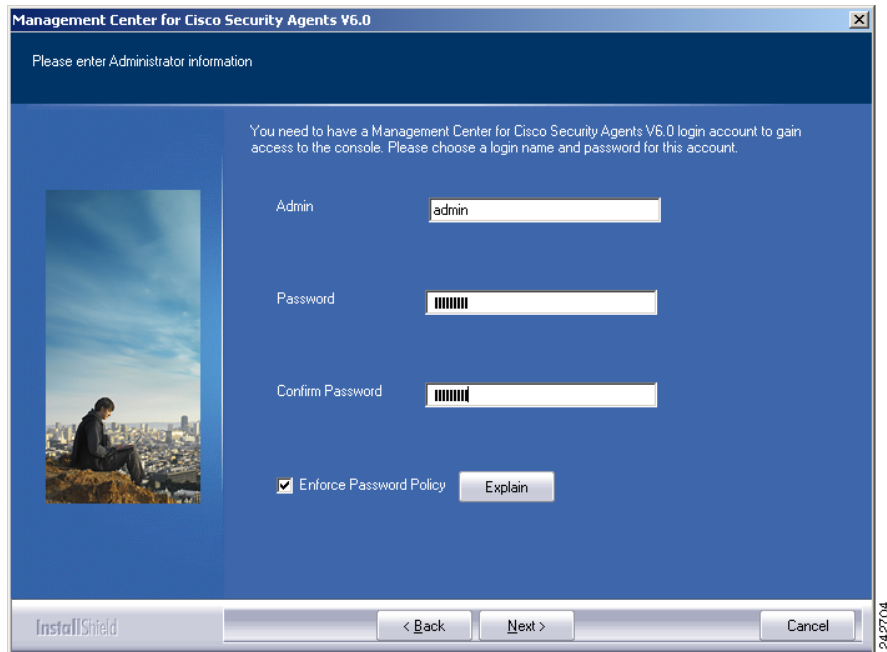
- Step 7** Once you enter the database information and click **Next**, the installation attempts to locate the database and verify that it is configured appropriately. If the database is not setup correctly, you are prompted with this information and the installation will not continue. Otherwise, the installation proceeds.
- Step 8** You are next prompted to select a CSA MC directory installation path. Either accept the default installation path or browse to a different path.

Figure 2-18 *Installation Directory*

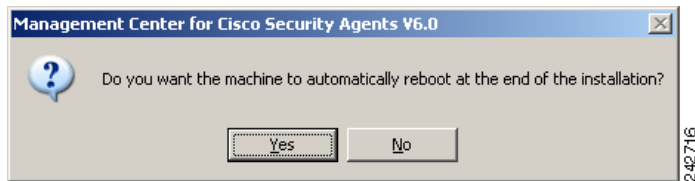
Step 9 You are next prompted to enter Administrator Name and Password information. This is the user name and password you will use to login in to CSA MC. Checking the **Enforce password policy** checkbox places these constraints on the password you enter:

- Password cannot be the same as, or contain, the login name
- Password must be between 6 and 32 characters long
- Password must contain characters from at least three of the following classes:
 - lower case letters
 - upper case letters
 - digits
 - non-alphanumeric characters.

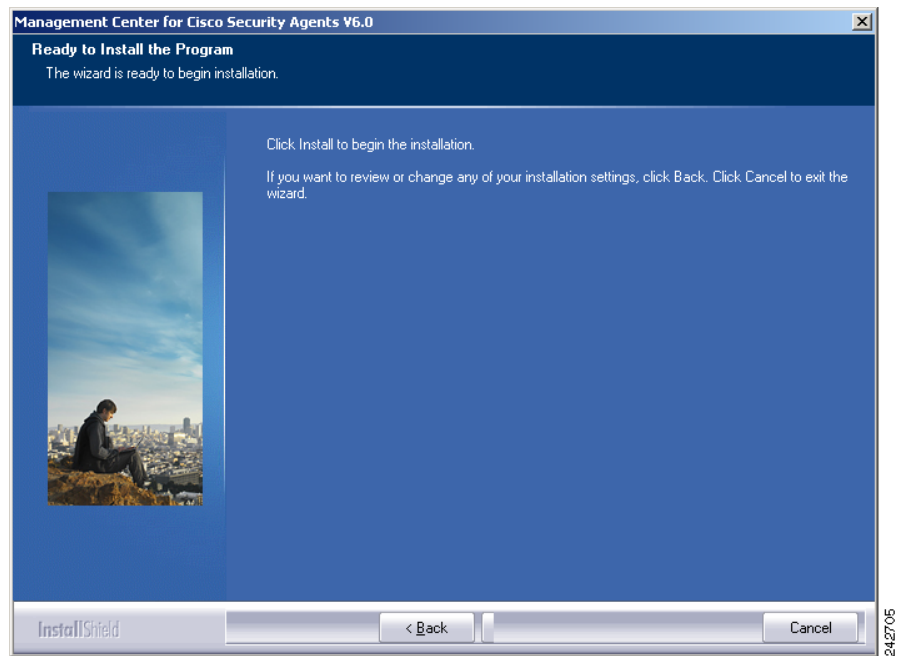
See [Figure 2-19](#). Enter this information and click **Next**.

Figure 2-19 Enter Administrator Name and Password

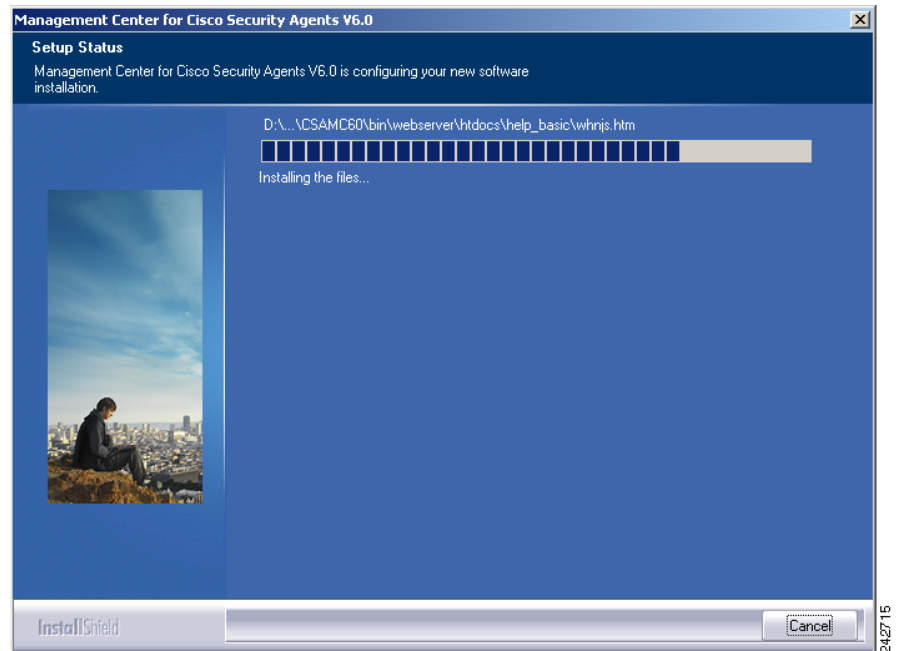
- Step 10** You are next prompted to select whether or not you want the system to automatically reboot once the installation is complete (see [Figure 2-20](#)). It is recommended that you reboot the system after the installation is complete whether you select Yes to have it done automatically or you choose to manually reboot at the end.

Figure 2-20 Automatic Reboot Option Prompt

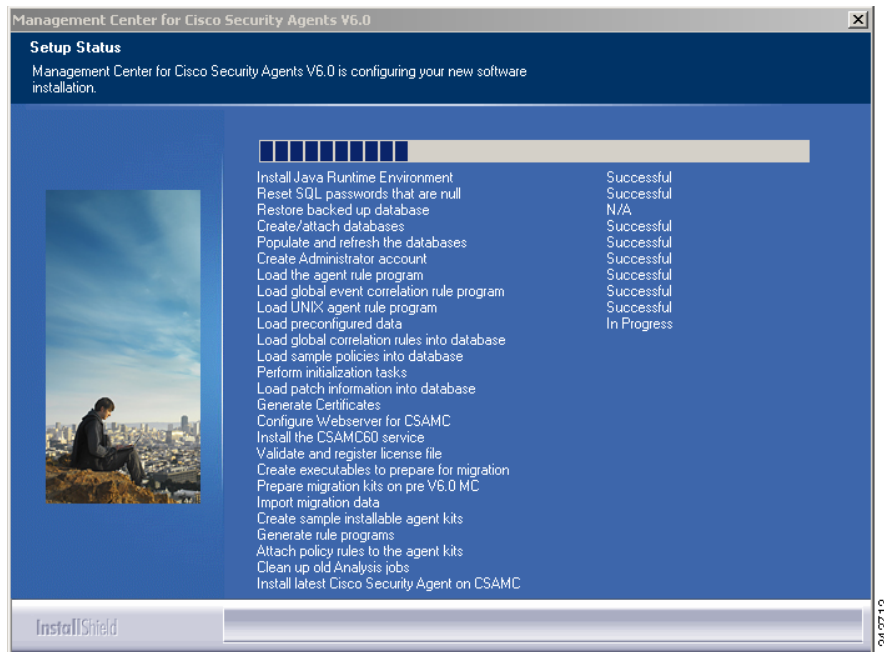
You are next prompted to begin the installation. Click the **Install** button. (See [Figure 2-21](#).)

Figure 2-21 *Begin Install*

The install then proceeds copying the necessary files to your system (see [Figure 2-22](#)).

Figure 2-22 *Copy Files*

Once the copying is complete, the installation begins configuration and setup tasks. See [Figure 2-23](#).

Figure 2-23 *Installation Proceeds***Note**

When the CSA MC installation completes, an agent installation automatically begins. It is recommended that an agent protect the CSA MC system and this is done automatically for you. (You may uninstall the agent separately if you choose, but this is not the recommended configuration.)

When the MC and agent installs are complete, if you selected to have the system reboot automatically, you are prompted that the automatic reboot will occur within 5 minutes. If you selected not to have the system reboot automatically, it is recommended that you manually reboot the system at this time.

Once the system reboots, should login to the MC and copy the license key file(s) you received from Cisco Systems to your CSA MC. CSA MC ships with and automatically uses a license for the MC and local agent. You must manually import all other licenses through the MC **Maintenance>License** Information window. See [Uploading a License, page 2-4](#) for license import instructions.

Information for Installing Multiple CSA MCs on Separate Systems

A CSA installation with two or more CSA MCs and a remote database is referred to as a “Distributed Configuration” or a “3 Tier System.”

If you are installing a distributed configuration, follow this procedure:

- Step 1** Install the remote database and the first CSA MC using the [Installing CSA MC with a Remote Database, page 2-21](#) procedure and reboot the system. This becomes the Polling CSA MC.
- Step 2** Stop the CSA MC service on the Polling CSA MC.
 - a. Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - b. Open a command prompt window and type `net stop csamc60` and press **Enter**.

- Step 3** Install the second (and subsequent) CSA MCs using the [Installing CSA MC Using the Remote Database, page 2-24](#) and use the same remote database information for the additional. After the system reboots, stop the CSA MC service before installing the next Configuration CSA MC.
- Step 4** Start the CSA MC service on the Polling CSA MC and all configuration CSA MCs.
- Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - Open a command prompt window and type `net start csamc60` and press **Enter**.

**Caution**

When installing two CSA MCs, the first MC you install automatically becomes the Polling and logging MC. The second MC acts as the Configuration MC. During the installation process, the CSA MCs know the order in which the MCs were installed and direct polling, logging, and management tasks to the appropriate MC.

**Caution**

The CSA MC service must be stopped on the Polling CSA MC before the configuration CSA MC can be installed. The CSA MC service must also be stopped on both the polling and configuration CSA MCs before either CSA MC is upgraded or uninstalled.

**Caution**

In a distributed configuration, when installing or updating, you **must** install the CSA MC software update on **all** MC's.

Installing CSA MC with a Previous Version's Database (Same System Installation)

This section addresses the procedure for backing up and importing a 5.0 database as part of CSA MC V6.0.1 same system installation.

In order to perform this type of migration, you must install a V5.1 MC along with the V6.0.1 MC. You must use V5.1 to migrate your V5.0 hosts and data to the V6.0.1 product schema. V5.1 is provided as an interim tool for bringing all your data into V6.0.1 correctly. The V6.0.1 installation installs both MCs, first 5.1 and then 6.0.1, with one reboot at the end.

**Note**

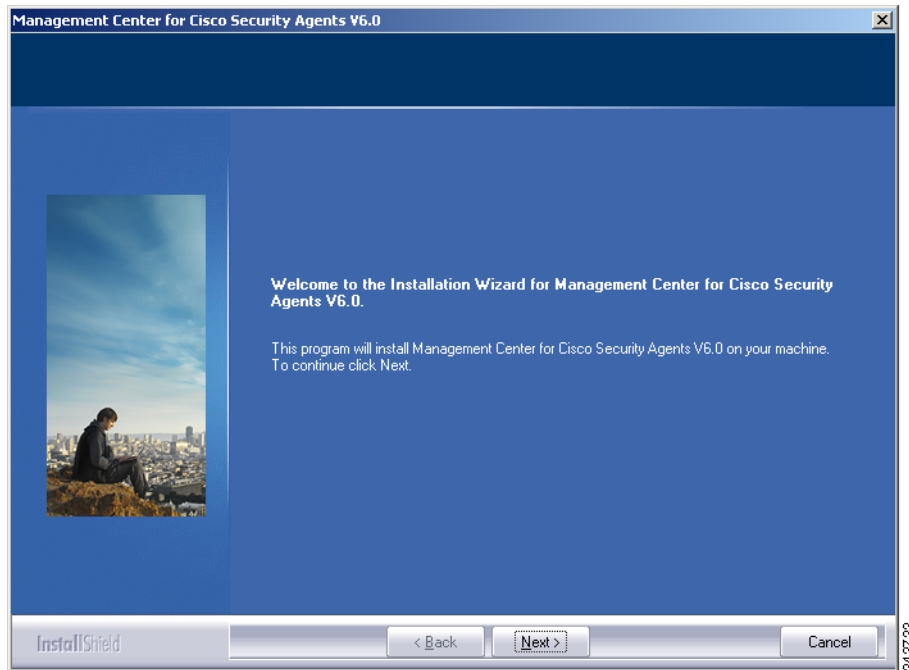
If you are migrating from CSA MC V4.x in a same system installation scenario, you must first upgrade to CSA MC V5.0. Refer to the CSA MC V5.0 Installation Guide for that procedure. Once you've completed that upgrade, you can use the following procedure.

- Step 1** Uninstall CSA MCV5.0 per the instructions in your CSA MC V5.0 Installation Guide. (If V5.0 uses a local database, during the CSA MC V5.0 uninstall procedure, when prompted, make sure to select to backup the database. When the uninstall completes, move the backed-up database to a different, network accessible system.)
- Step 2** Re-install that same system with the Windows 2003 R2 operating system.

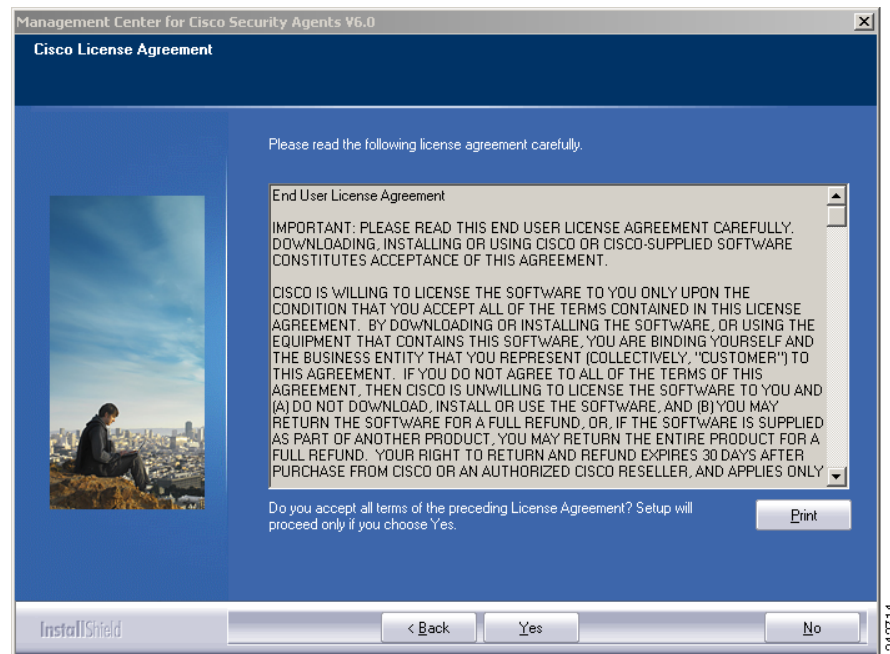
Install CSA MC V6.0.1 as follows:

- Step 1** Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
- Step 2** Place the Management Center for Cisco Security Agents CD into the CDROM drive. The welcome screen appears. Click Next to begin the installation. See [Figure 2-24](#). (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)

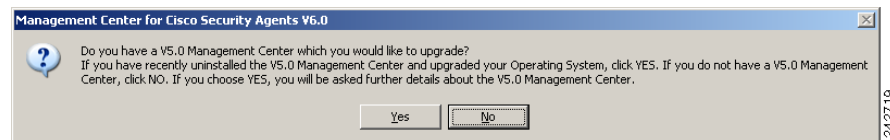
Figure 2-24 CSA MC Installation Welcome Screen



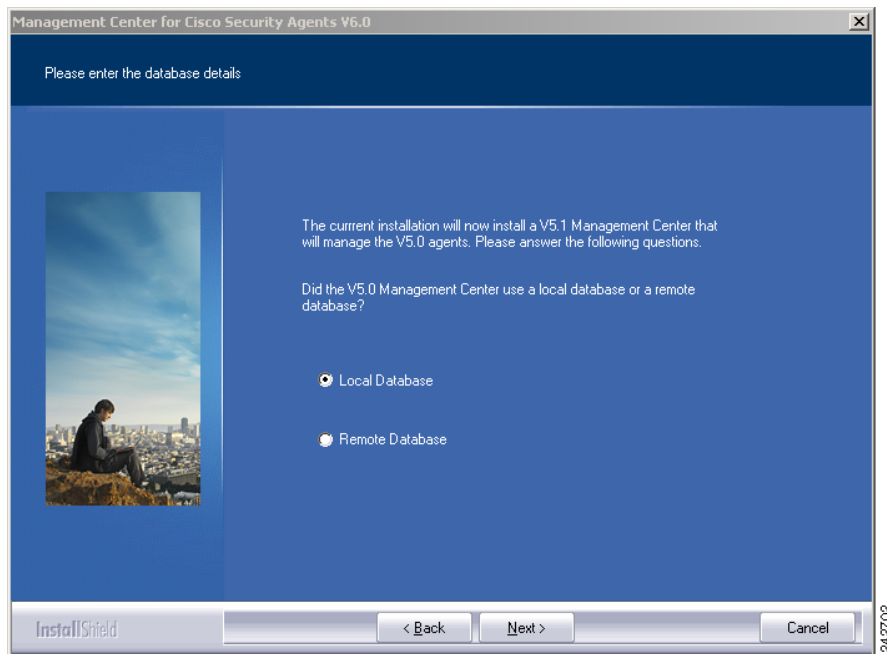
- Step 3** After you click **Next** in the welcome screen, various system checks are performed before the system installation continues.
- Step 4** When the initial system checks are complete, you are prompted to accept the license agreement. Accept the agreement by clicking **Yes**. See [Figure 2-25](#).

Figure 2-25 CSA MC EULA License Agreement

Step 5 The installation asks if you are upgrading from a V5.0 Management Center. In this case, click **Yes** to continue. See [Figure 2-26](#).

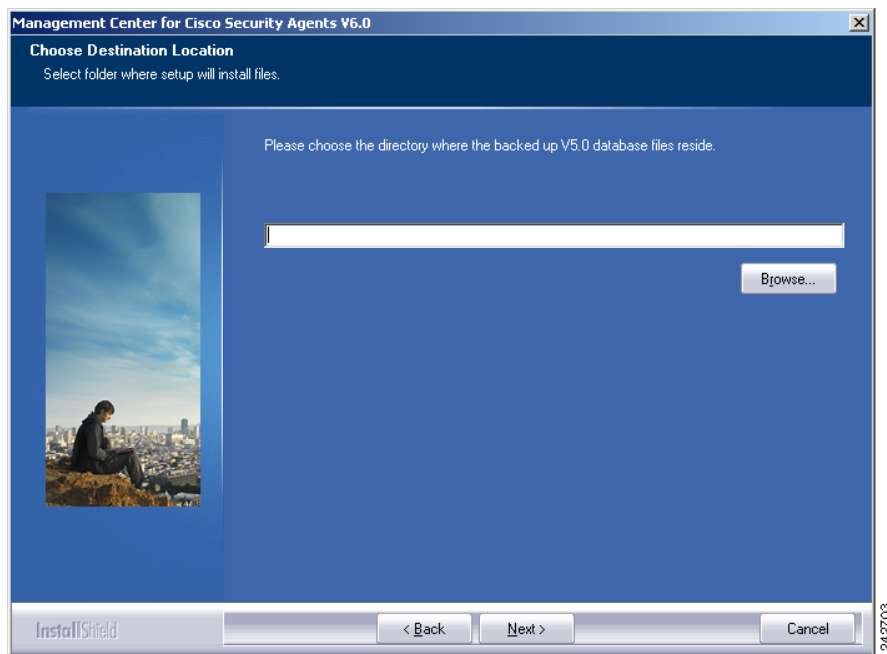
Figure 2-26 Upgrade Question Window

Step 6 Select whether your V5.0 installation used a local or a remote database. See [Figure 2-27](#).

Figure 2-27 Select V5.0 Database Type

Step 7 If you select Local Database, you are next asked to browse to the location of the backed-up V5.0 database. Once you've located the database, click **Next** to continue. See [Figure 2-28](#).

If you select Remote Database, you are asked to enter data for accessing the remote database. This remote database entry screen is the same as [Figure 2-17](#).

Figure 2-28 Browse to Backed-up V5.0 Database

Step 8 Once the V5.0 local or remote database is located, the installation will proceed to install CSA MC V5.1.

- Step 9** You must create a user name and password to login into the CSA MC V5.1. See [Figure 2-29](#). (You will later create another user and password for CSA MC V6.0.1).

Figure 2-29 Username and Password Creation for V5.1

From here, you can continue by following the procedures detailed in [Installing CSA MC with a Local Database, page 2-12](#) or [Installing CSA MC with a Remote Database, page 2-21](#) depending on how you are installing the product. As stated earlier, the installation will proceed by first installing V5.1 and then directly begin the V6.0.1 installation with one reboot at the end of the procedure. For both V5.1. and V6.0.1 installations, you must select a database type and setup usernames and passwords as explained in the procedures referenced above.

Installation Log

The installation of CSA MC produces a log file. This log file, called “CSAMC-Install.log” and located in the CSAMC60\log directory, provides a detailed list of installation tasks that were performed. If there is a problem with the installation, this text file should provide information on what task failed during the install.



Note

The installation of the agent produces a similar file called “CSAgent-Install.log” and is located in the Cisco\CSAgent\log directory on agent host systems.

Accessing Management Center for Cisco Security Agents

When the installation has completed and you’ve rebooted the system, a Management Center for Cisco Security Agents [version number] shortcut icon is placed on your desktop. Double-clicking this icon launches the MC in your default browser.

Local Access

To access CSA MC locally on the system hosting the CSA MC software, double-click the shortcut icon added to your desktop during the installation. This launches the management console login screen in your default browser.



Note

See [Initiating Secure Communications, page 2-41](#) if you cannot connect to CSA MC.

Remote Access

To access CSA MC from a remote location, launch a browser application on the remote host and enter the following in the Address or Location field (depending on the browser you're using) to access the Login view:

`https://<management center system hostname>.<domain>`

For example, enter `https://stormcenter.cisco.com`



Note

In this example, CSA MC is installed on a host system with the name stormcenter.



Note

This is the preferred method of accessing the CSA MC.

Figure 2-30 *CSA MC Login Window*

Management Center for
Cisco Security Agents

Version: 6.0

Running on: client221

Username:

Password:

Login

Please log in

© 2008 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

[[Get root certificate](#)] [[Agent Kits](#)]

242707

Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1

Take this approach, when upgrading from CSA 6.0 to CSA 6.0.1:

-
- Step 1** Upgrade the CSA MC from CSA6.0 to 6.0.1 using [Upgrading CSA MC with a Local or Remote Database from CSA V6.0 to V6.0.1, page 2-37](#) or [Upgrading Multiple CSA MCs with a Remote Database from CSA V6.0 to V6.0.1, page 2-38](#) procedure.
- Step 2** Update existing agents with CSA 6.0.1 software by scheduling software updates. See “Scheduling Software Updates” in the CSA MC online help or in Chapter 3, of *Using Management Center for Cisco Security Agents*, for more information.
- Step 3** Compare the CSA 6.0.1 default policies with the CSA 6.0 default policies.
- a. In the **Things to Do** section of the Home Page, users with configure or deploy roles, viewing CSA MC in Advanced Mode, will see an alert stating “At least one mandatory policy is obsolete” and it will provide links to **Update mandatory policies: Linux, Solaris, Windows**. (Mandatory policies are those connected to the auto-enrollment groups: <All Windows>, <All Linux>, and <All Solaris>.)
- Clicking the link for an operating system opens the compare tool and displays the differences between, for example, the <All Windows> auto-enrollment group and the **All Windows** prototype group. Use the compare tool to review the new and updated policies in the prototype group to those in the auto-enrollment group.
- After comparing the policies, attach the new or updated policies in the prototype group to the auto-enrollment groups and detach outdated policies from the auto-enrollment group.
- b. In addition to the auto-enrollment groups be sure to review changes to the CSA MC, Desktops, and Servers groups.
- Though there is not an alert in the **Things to Do** section for every group or policy; however, you can still use the compare tool to compare your existing policies to those provided in the latest release.
- See “Comparing Configurations” in the CSA MC online help or in Chapter 5 of *Using Management Center for Cisco Security Agents*, for more information.
- Step 4** Pilot new policies. If you want to test the new policies before you deploy them, add the new policies to a small test group and add a limited number of hosts to the group.
- Step 5** When you are ready to adopt the CSA 6.0.1 default policies, move hosts out of the groups running the 6.0 policies and into the groups using the 6.0.1 policies. See “Host Managing Tasks” in Chapter 3, of *Using Management Center for Cisco Security Agents*, for more information.

Upgrading CSA MC with a Local or Remote Database from CSA V6.0 to V6.0.1

-
- Step 1** Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
- Step 2** Put the Management Center for Cisco Security Agents CD into the CDROM drive. The Welcome screen appears. Click **Next** to begin the installation. (If the installation does not start automatically, browse to the setup.exe file on the CD and double click to begin the installation.)
- If you have downloaded the updated release from Cisco.com, save the kit on the same system on which CSA 6.0 is running and double-click the setup.exe file. At the Welcome screen, click **Next** to begin the installation.

- Step 3** The install shield will attempt to stop the CSA 6.0 agent running on the CSA MC. When you receive the message, “An attempt is being made to disable security for Cisco Security Agent. Do you wish to Allow this?” Select **Yes**, provide a brief explanation in the **Please explain** field, and click **Apply**.
- Step 4** Respond to the security challenge in the Cisco Security Agent Challenge pop-up dialog box and click **OK**.
- Step 5** When asked if you want to reboot at the end of the upgrade; click **Yes**. The installation continues and you see a Setup Stratus similar to that in [Figure 2-13](#).
- Step 6** After the installation has finished, you receive a pop-up message indicating that you have five minutes until the reboot takes place. Click **OK** if you want to restart the system immediately.

**Note**

Wherever CSA 6.0.1 policies are exactly the same as they were in CSA 6.0, the 6.0 policy is replaced by the 6.0.1 policy. The group details page may show a group from 6.0 with 6.0.1 policies.

**Note**

Any rules that you changed or policies you added to 6.0 will be maintained in the correct group for 6.0.1.

- Step 7** See [Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1, page 2-37](#) and continue with steps 2-5 to upgrade agents in your deployment.

Upgrading Multiple CSA MCs with a Remote Database from CSA V6.0 to V6.0.1

In this configuration there is a Polling CSA MC, at least one Configuration CSA MCs, and a remote database. This is referred to as a “Distributed Configuration” or a “3 Tier System.”

There are two procedural items to note when installing a software update in a distributed configuration with multiple MC’s.

- In a distributed configuration, you **must** install the software update on **all** MC’s.
- In a distributed configuration, when installing, upgrading, or uninstalling any MC, the service must be stopped on the other MCs. For example, in a configuration with 2 MCs, you must first stop the service on one MC before you install the software update on the other MC. Then restart the services.

This is the approach of the upgrade:

- Step 1** Stop the CSA MC service on all Configuration CSA MCs in the configuration:
- a. Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - b. Open a command prompt window and type `net stop csamc60` and press **Enter**.
- Step 2** Upgrade the Polling CSA MC from CSA V6.0 to CSA V6.0.1 using [Upgrading CSA MC with a Local or Remote Database from CSA V6.0 to V6.0.1, page 2-37](#). After the system reboots, stop the CSA MC service on the newly upgraded Polling CSA MC.
- Step 3** Start the CSA MC service on the next Configuration CSA MC you want to upgrade.
- a. Log on as a local Administrator on your Microsoft Server Windows 2003 R2 Standard or Enterprise system.
 - b. Open a command prompt window and type `net start csamc60` and press **Enter**.

- Step 4** Upgrade the Configuration CSA MC from CSA V6.0 to CSA V6.0.1 using [Upgrading CSA MC with a Local or Remote Database from CSA V6.0 to V6.0.1, page 2-37](#). After the system reboots, stop the CSA MC service on the newly upgraded Configuration CSA MC.
- Step 5** Repeat step 4 until all your Configuration CSA MCs have been upgraded.
- Step 6** Start the CSA MC service on all CSA MCs where the service is stopped, starting with the Polling CSA MC.
- Step 7** See [Upgrading Your Deployment from CSA V6.0 to CSA V6.0.1, page 2-37](#) and continue with steps 2-5 to upgrade agents in your deployment.

Migration Instructions

The following section contains information for migrating to CSA MC V6.0.1 from a previous version installed on the same system and for a previous version installed on a separate machine. Both scenarios are covered here.



Note

If you install 6.0.1 on the same system where you have 5.2 installed, the majority of this migration is done automatically.

If you intend to migrate 5.2 Solaris agents, please read [Solaris and Linux Agent Migration, page 2-41](#) before starting your upgrade.

To migrate to V6.0.1, do the following:

- Step 1** Install the Management Center for Cisco Security Agents V6.0.1. See previous sections for instructions.
- If you're installing CSA MC V6.0.1 on the same machine running CSA MC V5.2, an xml file containing V5.2 configuration items and several .dat files containing host information are automatically generated by the installation and ready for importing once the install is complete.
 - If you're installing CSA MC V6.0.1 on a different machine from the system running V5.x or V4.x, after installing V6.0.1, you must copy and manually run an executable file on the V5.x or V4.x machine to create the xml and dat files needed for importing V5.x or V4.x configurations and host information to V6.0.1.
- Step 2** If you have installed V6.0.1 on the same machine as V5.2, you can skip to Step 8. Otherwise, once you have installed CSA MC V6.0.1 and rebooted the system, navigate to the **Cisco Systems\CSAMC\CSAMC60\migration** directory. Copy the appropriate file (named `prepare_<version>_migration.exe` depending on the version you are migrating from, for example `prepare_52_migration.exe`) to your V5.x or V4.x system. (You can copy it to any place on the system.)
- Step 3** On your V5.x or V4.x system, disable agent security and run the `prepare_<version>_migration.exe` file that you copied from the V6.0.1 system. (You must disable security in order to run the executable file and create the import xml data.) This launches a command prompt which displays the progress of the migration.
- Step 4** When the `prepare_<version>_migration.exe` file is finished, on the V5.x or V4.x system, navigate to the **Cisco Systems\CSAMC\CSAMC52\migration\export** or **CSCOpX\CSAMC50\migration\export** directory (the directory name depends on the version you're migrating from) and locate several newly created files. Your configuration data is now in a file named `migration_data_export.xml`. Your host data (hosts and distinct host groupings) are now in several files, depending on how many distinct host groupings existed, named `migration_host_data<number>.dat`.

Using the data that is now wrapped up in these files allows you to import your existing policy configurations and your current host groupings, thereby preserving the policy tuning and host group configurations for your new V6.0.1 installation.

Step 5 Next, copy the `migration_data_export.xml` and all the `migration_host_data<number>.dat` files from the V5.x or V4.x system to your V6.0.1 system. These files must exist together in the same directory on the V6.0.1 system (although the directory name and location does not matter).

Step 6 From the V6.0.1 system, run the **webmgr import utility** from a command prompt to pull the data into the new MC. You cannot use the CSA MC UI Import utility to do this. That utility does not allow you to import the .dat files that are associated with the .xml file as one grouping.

For example, from a command prompt window on the V6.0.1 system, change to the directory in the following example and run the command as follows:

```
%system\Cisco\CSAMC\CSAMC60\bin>webmgr import %path_to_xml_file%\migration_data_export.xml
```

Because the host .dat files are associated with the .xml file, this command imports both the configuration and host data with the `migration_data_export.xml` file.

Step 7 You must generate rules once the import is complete. If you do not generate rules at this point, you cannot upgrade agent host software as described in the next section.



Note

CSA MC V6.0.1 ships with policies that contain new V6.0.1 functionality. This new functionality does not match all V5.x or V4.x configurations. CSA MC configuration item names are labeled with the release version number to distinguish them from older (or newer) configuration items or items created by administrators. When you import your older configuration, new V6.0.1 items are not overwritten. You will likely have items from both versions in your CSA MC V6.0.1. If the import process finds that two items have the exact same contents and the only difference is the V6.0.1 appended name field, the older item is not imported and the newer V6.0.1 item is used in its place.

Step 8 To upgrade migrated V5.x or V4.x agents to V6.0.1, schedule V6.0.1 software updates for older agents. You schedule this upgrade from the V5.x or V4.x system.

To schedule the update, mouseover the **Systems** menu in the V5.x or V4.x CSA MC and select **Software Updates > Scheduled Software Updates**. For instructions on how to schedule the software update, select **Help > Online help**.

Once the older agents receive the scheduled software update, they will point to and register with the new CSA MC V6.0.1. The update contains the appropriate new certificates to allow this to occur. After the hosts have registered with the new CSA MC, they will need to be moved into groups with the 6.0.1 security policies. Take the same upgrade approach, starting with step 3, as outlined in [Upgrading from CSA V6.0 to CSA V6.0.1, page 2-7](#). The difference, of course, is that you will be moving hosts out of 5.x or 4.x groups into 6.0.1 groups.



Note

Agent kits are configuration items that do not migrate to the new version. Because host migration does not relate to agent kits, old agents kits are not considered to be necessary migration items.

Also, configuration items that are not used (not attached to any group) do not migrate to the new version.

**Caution**

When upgrading V5.x or V4.x agents to software version 6.0.1, the upgrade program disables the system network interfaces to ensure a secure upgrade process. The agent service is also stopped to allow the update to occur. Once the update is complete, the agent service is restarted and the network interfaces are enabled. (Note, that secure upgrades are not supported for Windows NT systems.)

Once you have migrated all old agents to the newer version, you can uninstall the old version of CSA MC. See [Uninstalling Management Center for Cisco Security Agents, page 2-46](#).

Solaris and Linux Agent Migration

**Caution**

Solaris agent versions 4.0.3.736 or later can be upgraded to version 6.0.1 Earlier Solaris agents cannot be upgraded.

Only Linux agent version 4.5.1.638 or later can be upgraded to version 6.0.1 Earlier Linux agents cannot be upgraded.

You should note that the Solaris host migration process is a bit different than Windows and Linux migration.

Once scheduled, Solaris software upgrades must be launched manually by accessing the **csactl** command line tool on the Solaris systems and typing in the software update command. When the update is complete, network connectivity is disabled and remains disabled until the system automatically reboots within 5 minutes. This reboot *cannot* be stopped. Therefore, once you launch the Solaris software update, you must understand that the system will reboot when the update completes.

Upgrade Note

Newer versions of policies are not automatically attached to the auto-enrollment groups during upgrade. If you want to update the mandatory policies, you can use the CSA MC Compare tool to synchronize the existing auto-enrollment groups with the new updated auto-enrollment groups added by the upgrade.

Initiating Secure Communications

CSA MC uses SSL to secure all communications between the CSA MC user interface (locally and remotely) and the Management Center for Cisco Security Agents server system itself. This way, all configuration data travels over secure channels irrespective of the location of the CSA MC host system.

During installation, CSA MC generates private and public keys to be used for secure communications between any system accessing the CSA MC user interface and the CSA MC itself.

When your browser connects to the server, it receives the server's certificate. You are then prompted to accept this certificate. It is recommended that you import it into your local certificate database so that you are not prompted to accept the certificate each time you login. The following sections show the process of importing certificates into Internet Explorer and Netscape Web browsers.

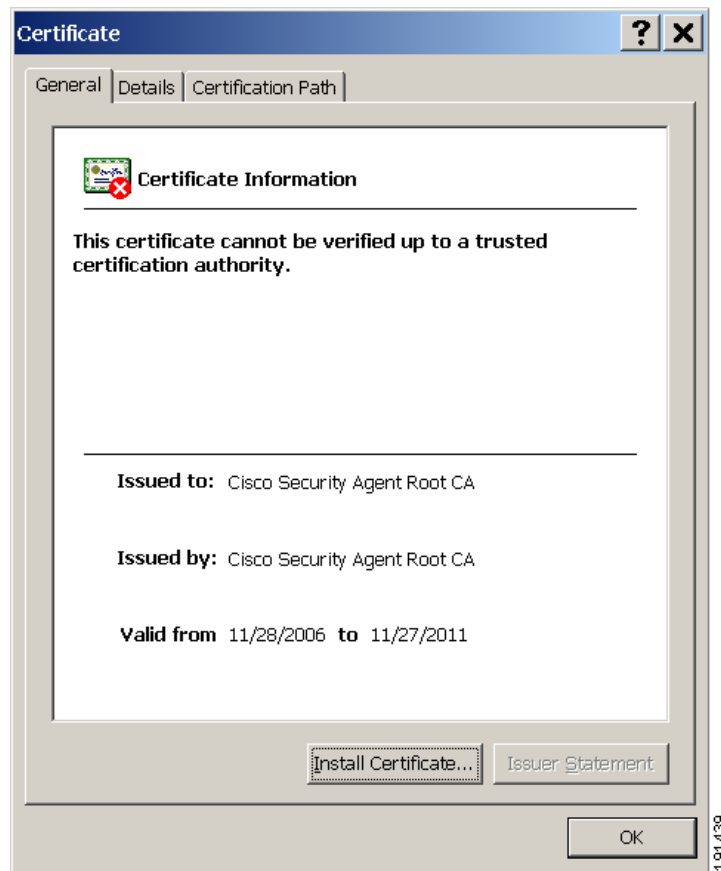
Internet Explorer: Importing the Root Certificate


Note

If you are using Internet Explorer 7.0, you see an “Invalid Certificate” screen when you first attempt to open a CSA MC browser window. See the end of this section for further information.

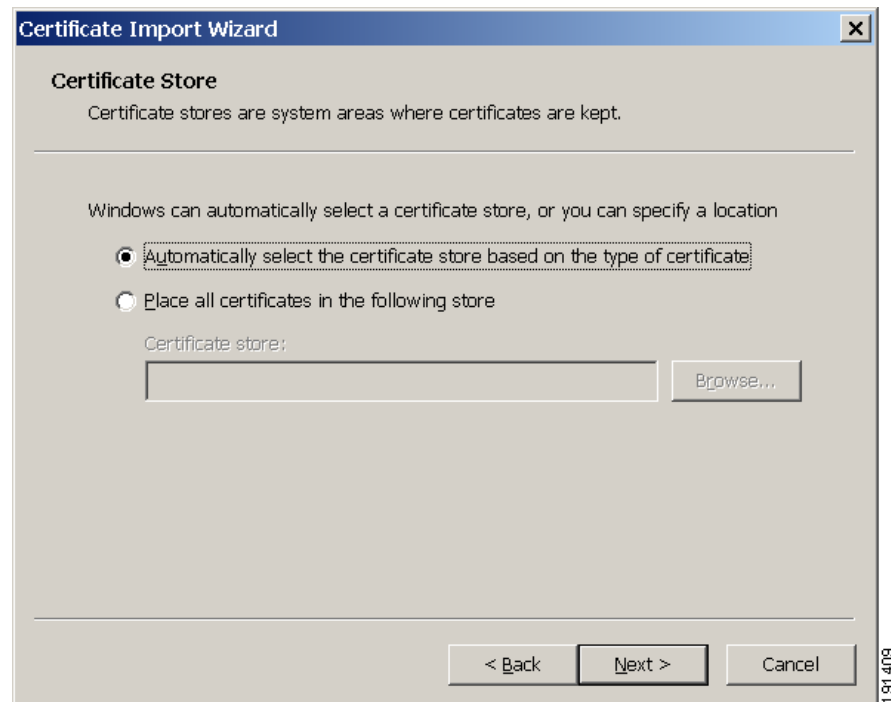
- Step 1** You import the certificate from the CSA MC login window. Click the **Get root certificate** link. See [Figure 2-30](#).
- Step 2** Select the **Open** (this file from its current location) button and click **OK**.
- Step 3** The certificate information box appears (see [Figure 2-31](#)). It contains information on the system the certificate is issued to and it displays expiration dates. Click the **Install Certificate** button to start the Certificate Manager Import Wizard.

Figure 2-31 Certificate Information



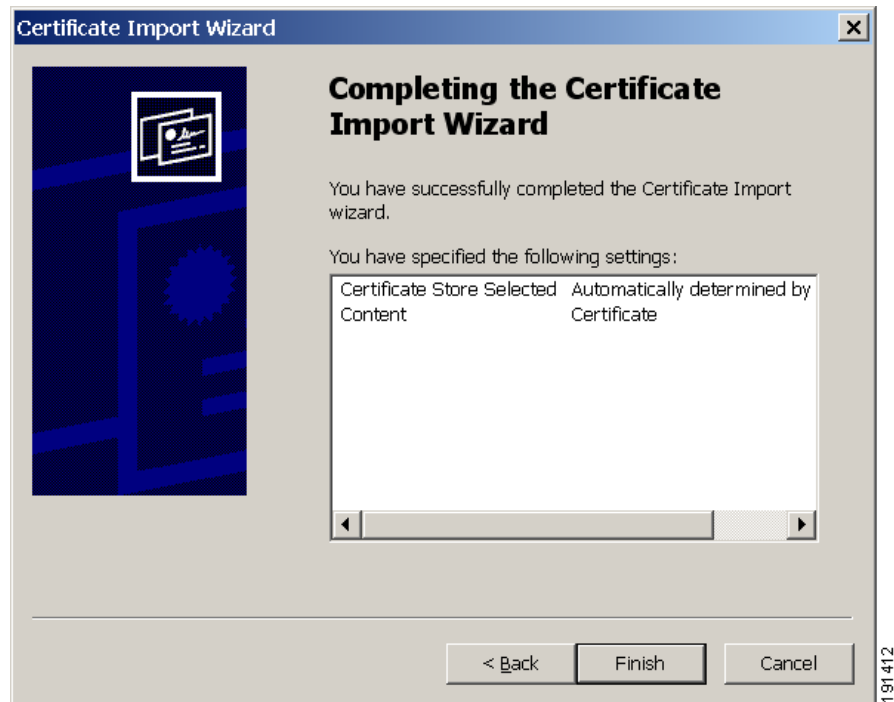
- Step 4** The first Certificate Manager Import page contains an overview of certificate information. Click **Next** to continue.
- Step 5** From the Select a Certificate Store page, make sure the **Automatically select the certificate store based on the type of certificate** radio button is selected. Click **Next**.

Figure 2-32 Certificate Wizard



Step 6 You've now imported your certificate for the server. Click the **Finish** button (Figure 2-33) to continue.

Figure 2-33 Certificate Wizard Finish Page



Step 7 Now, you must save the certificate. Click the **Yes** button in the Root Certificate Store box.

Step 8 You are next prompted with a confirmation box informing you that your certificate was created successfully.

**Note**

You must perform this certificate import process the first time you login to CSA MC from any remote machine. Once the certificate import is complete, you can access the login page directly for all management sessions. To access the login page remotely, enter the URL in the following format.

```
http://<management center system hostname>.<domain>
```

For example, enter `http://stormcenter.cisco.com`

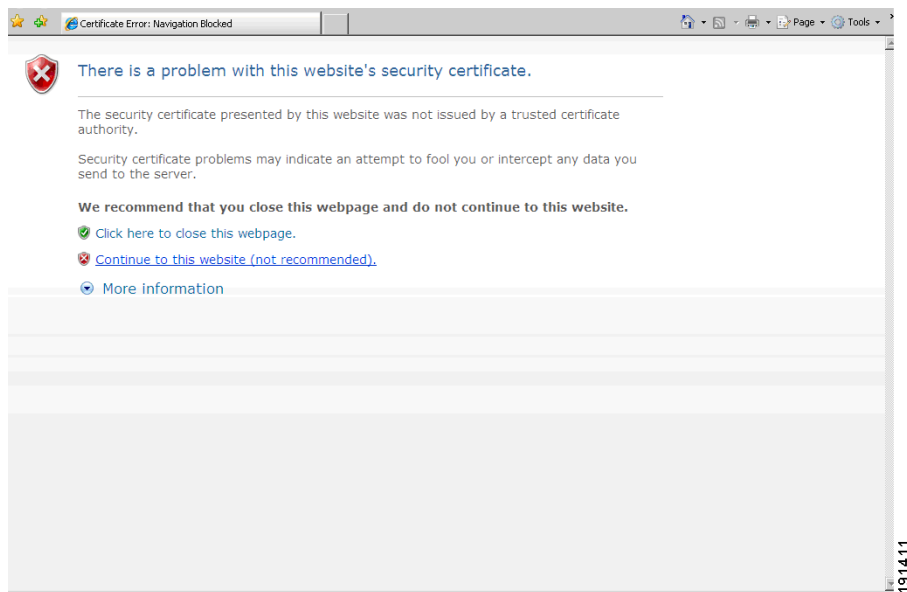
**Caution**

If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Refer back to [page 2-2](#) for further licensing information.

Internet Explorer 7.0: Importing the Root Certificate

If you are using Internet Explorer 7.0, you see an “Invalid Certificate” screen when you first attempt to open a CSA MC browser window. When that screen appears, click the **Continue to this website (not recommended)** link, see [Figure 2-34](#). Then you can continue by following instructions in [Internet Explorer: Importing the Root Certificate, page 2-42](#).

You will only see this screen the first time you access the CSA MC browser in IE 7.0. Once you follow the instructions and import the root certificate, the screen should not appear again.

Figure 2-34 Internet Explorer 7.0 Certificate Screen

Uninstalling Management Center for Cisco Security Agents

Uninstall the CSA MC software as follows:

- Step 1** Click the uninstall CSA MC option on the system from **Start > Programs > Cisco > Uninstall Management Center for Cisco Security Agents**. This launches the uninstall program.
- Step 2** You must respond to uninstall confirmation and database back-up prompts during the uninstall process. The CSA MC uninstall also removes the Cisco Security Agent on the MC system.



Tip If you are running a local database, click **Yes** when prompted to backup your CSA MC database configuration. Store the backup in a location other than the Program Files\Cisco\CSA MC directory. If you are uninstalling and reinstalling CSA MC, this will give you an easy way to restore your CSA MC's configuration.

- Step 3** Reboot when prompted.



Note

Uninstalling CSA MC does not uninstall the Microsoft SQL Server Desktop Engine (database). You must uninstall this separately from the **Control Panel>Add/Remove Programs** window if you are completely removing the product from your system.



Caution

If you are upgrading to a new version of CSA MC, or if you are reinstalling the product on the same system, and you want to preserve your current configuration, you should select to **Backup the Database** during the uninstall when you are prompted to do so. If you do not backup the database, the uninstall removes all program files and configurations. (Note that this only applies to local database installations. CSA MC does not provide a backup mechanism for remote databases.)

Hotfix Information

After a hotfix is installed, administrators must clear the cache of the browsers they use to reach the updated CSA MC.

Clearing the cache in Internet Explorer

- Step 1** From the Tools menu of Internet Explorer, select **Internet Options**.
- Step 2** In the Temporary Internet files section click **Delete Files**.
- Step 3** In the Delete Files dialog box, select **Delete all offline content**.
- Step 4** Click **OK** to delete the content.
- Step 5** Click **OK** to close the Internet Options dialog box.

Clearing the cache in Mozilla Firefox.

- Step 1** From the Tools menu of Mozilla Firefox, click **Clear Private Data**.
- Step 2** Make sure that **Cache** is selected.
- Step 3** Click **Clear Private Data Now**.



CHAPTER 3

Quick Configuration & Deployment

Overview

This chapter provides the basic setup information you need to start using the Management Center for Cisco Security Agents to configure some preliminary groups and build agent kits. The goal of this chapter is to help you quickly configure and distribute Cisco Security Agent kits to hosts and have those hosts successfully register with CSA MC. Once this is accomplished you can configure some policies and distribute them to installed and registered Cisco Security Agents.

For detailed configuration information, you should refer to the User Guide.

This section contains the following topics.

- [Logging on to the CSA MC, page 3-2](#)
 - [Access Management Center for Cisco Security Agents, page 3-2](#)
 - [Simple View and Advanced View Modes, page 3-3](#)
 - [Visible, Hidden, and Read-only Components on CSA MC, page 3-3](#)
- [Cisco Security Agent Policies, page 3-4](#)
- [Piloting the Product, page 3-4](#)
 - [Running a Pilot Program, page 3-4](#)
- [Quick Configuration and Deployment, page 3-5](#)
 - [1. Update your Licenses, page 3-5](#)
 - [2. Pick your Policies, page 3-5](#)
 - [3. Update the Agent Kits, page 3-6](#)
 - [4. Distribute and Install the Kits, page 3-6](#)
 - [5. Create Exceptions as Necessary, page 3-6](#)
- [View Registered Hosts, page 3-7](#)
- [Policy Tuning and Troubleshooting, page 3-7](#)
 - [Overall Guidelines, page 3-7](#)
 - [Creating Policies for Your Special Applications, page 3-8](#)
 - [Using Audit Mode, page 3-9](#)
 - [Disabling Specific Rules, page 3-9](#)
 - [Caching and Resetting Query Responses, page 3-9](#)

- [Setting Up Exception Rules, page 3-10](#)
- [Configuring Your Own Policies, page 3-11](#)
- [Distributing Agent Kits Using a Third Party Tool, page 3-11](#)
 - [Setup.exe Command Switches, page 3-12](#)
 - [Command Examples, page 3-14](#)

Logging on to the CSA MC

Use the procedures in this section to access the CSA MC from a browser. After logging on you reach CSA MC's Home Page. For a description of the CSA MC interface, see "Interface Overview of Management Center for Cisco Security Agents" in *Using Management Center for Cisco Security Agents*.

Access Management Center for Cisco Security Agents

An initial administrator account was created as part of the CSA MC installation process. Use that administrator account to log into CSA MC.

Administrators can access CSA MC locally or remotely from a supported Web browser. No more than 12 users may be logged on to the CSA MC at the same time.

**Note**

We recommend connecting to the CSA MC through a browser on a remote machine rather than through a browser installed directly on the CSA MC server.

Remote Access

To access CSA MC from a remote location, launch a browser application and enter

```
https://<system hostname>.<domain>
```

For example, enter `https://stormcenter.cisco.com`

Local Access

To access CSA MC locally on the system hosting CSA MC software, double-click the CSA MC desktop icon created during the installation.

Enter the administrator name and password created during the CSA MC installation.

**Note**

When you login to the CSA MC system, you are presented with the CSA MC Home page. Various messages or warnings may appear in the Things to Do area. See the description of the **Home Page** in *Using the Management Center for Cisco Security Agents* for more information.

**Tip**

Once you have logged on, look at the global command buttons in the top right corner of the Home Page. One will indicate "All OSES," "Windows," or "UNIX." Click the command button to view the components relevant to the operating system you choose. Clicking UNIX displays components for both Solaris and Linux operating systems.

**Caution**

If you have not obtained a valid license from Cisco, when you login to CSA MC, you'll receive a warning informing you that your license is not valid. Any newly deployed agents will not be able to register with the unlicensed CSA MC. Refer back to [Licensing Information, page 2-2](#) for further licensing information.

Simple View and Advanced View Modes

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

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

Visible, Hidden, and Read-only Components on CSA MC

What you see on component list pages and on the Host Security page depends on your user configuration and whether or not the component is hidden or visible. What you can edit on list pages or through the Host Security page depends on your user configuration.

Some components are “hidden” by default other components are “Read-only” by default. Users are not expected to have to configure these components in a deployment that uses the groups, policies, and other components, supplied with this release.

Before you begin your pilot, view the system in Advanced Mode and, from the menu bar, navigate **Maintenance > Administrators > Account Management**. From the account list page, click the login ID you intend to use to manage your pilot. The details page shows the user's preferences.

Here you can configure users viewing mode, their ability to see hidden objects, and their permissions to edit read-only objects. Configure your users with the permissions they will need to conduct the pilot. See **Configuring Role Based Administration** in the **Management Center for Cisco Security Agents Administration** chapter of *Using Management Center for Cisco Security Agents*.

From the menu bar, navigating **Configuration > Host Security** brings up the Host Security page. From this page you can configure groups and create agent kits. The groups and policies appear on this page because their Simple Mode Settings are set to expose the component on the page.

If there are other groups or policies you want to manage through the Host Security page, you can configure them to be displayed if your user account allows you to edit read-only components. See “Configuring Groups” and “Configuring a Policy” in the User Guide for instructions on exposing these components on the Host Security page.

Cisco Security Agent Policies

CSA MC default Cisco Security Agent kits, groups, policies, and configuration variables are designed to provide a high level of security coverage for desktops and servers. These default Cisco Security Agent kits, groups, policies, rule modules and configuration variables cannot anticipate all possible local security policy requirements specified by your organization's management, nor can they anticipate all local combinations of application usage patterns. Cisco recommends deploying agents using the default configurations and then monitoring for possible tuning to your environment.

If you are using shipped policies, you can also use shipped, pre-built agent kits. Therefore, if you're not creating your own configurations, you can simply refer to the chapters on **Management Center for Cisco Security Agents Administration** and **Event Logging and Alerts** in *Using Management Center for Cisco Security Agents* for information on deploying kits to end users and viewing the event log.

**Note**

Each pre-configured rule module, policy, and group page has data in the expandable **+Detailed** description field explaining the item in question. Read the information in these fields to learn about the items described and to determine if the item in question meets your needs for usage.

As a jumping off point for creating your own configurations, the following sections in this manual take you through the step by step process of configuring some of the basic elements you need to initiate server/agent communications and to begin the distribution of your own policies.

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 in a CSA upgrade situation, a short pilot program will be beneficial.

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

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

The following sections provide a guideline for conducting a pilot of CSA and deploying the product on a large scale.

Running a Pilot Program

Your pilot program should proceed in the following manner:

- *How large should a pilot program be?* Select a logical, manageable, sample of systems on which agents will be installed. A good rule of thumb is to make your pilot approximately 1% the size of what the entire deployment will be.

Details:

- If your entire deployment will be very small, be sure to pilot at least 15-20 systems.
- If your entire deployment will be very large, roll out your pilot in steps. For example, do not pilot 1,000 systems initially and all at once. Start with a smaller sample and gradually expand the pilot.

The pilot should include machines that you can access readily (either yourself or through a responsive end-user). If you will eventually be installing agents on multiple, supported operating systems, your pilot should include machines running those operating systems. Again, systems in your pilot should be representative of the whole deployment to which you intend to scale.

- *How long should a pilot program run?* The policies in CSA 6.0 are designed to be used as they are or with only minimal tuning. Still, deploying and tuning policies is an iterative process. Initially, you will have some event log noise to parse. You must examine the data coming in and fine tune your policies accordingly.

Although every site is different, it would not be unusual to run a pilot program for approximately one to two weeks after you feel you have tuned your policies to your satisfaction. All possible application usage should take place within the pilot time frame. It is important to note that this recommended time frame allows you to exercise applications, their deployment and usage, within an entire fiscal quarter. The idea being, every application you use and every manner in which you use it will occur during this piloting period.

Quick Configuration and Deployment

The Management Center for Cisco Security Agents (CSA MC) comes preconfigured with downloadable kits for desktop and server hosts. Here's how to get your pilot program up and running in five easy steps:

1. Update your Licenses

CSA MC comes with a few free agent licenses for servers so you can install the CSA MC and get started quickly. Before deploying agents throughout your network, you must install a more comprehensive license for desktops and servers. If you want the added protection of the Data Loss Prevention feature, you will need to upload a separate license for that.

For a procedure on how to update your licenses and to learn more about Data Loss Prevention update your licenses, see [Licensing Information, page 2-2](#).



Note

You can proceed through step 3 without loading a license, but make sure to load a license before proceeding to step 4.

If you need help getting your formal CSA MC license file(s) from Cisco, see the Product Licensing Information section of the *Documentation and Licensing Overview for Management Center for Cisco Security Agents 6.0*. If you need keys for a product evaluation, and you are a registered user of Cisco.com, you can go to the Cisco Product License Registration page and download the **Cisco Security Agent 6.x Demo License**.

2. Pick your Policies

To pick policies for your desktops, mouse-over the **Configuration menu** on the CSA MC and click **Host Security**, then follow this procedure:

Step 1

Click the “Desktops” group for the appropriate operating system. You will see a list of policies - you can click on a policy name to see a description of the policy.

- Step 2** Click the checkbox for each policy you want enforced on your desktops. If you want a policy's rules to be logged but not enforced, click the policy's "**Audit Mode**" checkbox. If you are unsure of what to check, just keep the defaults. If you change a checkbox from its default state, press the **Save** button when done.
- Step 3** If a policy displays a red [warning] link, click the link to show the items that require customization. Customize each item by clicking its link in the Policy Warning dialog box and editing the pop-up provided. If you customize something, press the **Save** button when done.

**Tip**

If you want to take the deployment a little slower, enable one policy at a time and tune that policy before turning on the next policy. This will help you match specific outcomes with specific policies.

3. Update the Agent Kits

Policies are bundled together into downloadable, installable agent kits. If you made changes in the previous step, you must update these kits by clicking **Generate rules** at the bottom of your browser window, then pressing the **Generate** button to confirm the action. (If you didn't change anything, then you can skip this step.)

You can see a list of all your agent kits by mousing-over **Systems** in the menu and selecting **Agent kits**.

4. Distribute and Install the Kits

To see the agent kit corresponding to your desktop group's policies, go to the **Host Security** page and click on the appropriate **Desktops** group. You should see the text "Available kits for this group" followed by a link. Click the link to pop up the name of the kit, and click on this name to see the kit's details dialog box.

On this dialog, under the heading **Download**, there will be a URL. The URL references the executable that installs CSA with the appropriate policies. E-mail this URL to your users who should install CSA. Alternatively, you can click on the URL, save the resulting executable, then use systems-management software (like SMS) to push the executable to your endpoints for installation.

When an agent kit is downloaded and installed, the agent will register with the CSA MC, start enforcing your policies and generating events.

Once you have completed steps 1-4 for desktops, repeat them for the servers you want to protect with CSA.

5. Create Exceptions as Necessary

If CSA denies an action that you wish to allow, you can create a policy exception to permit the action.

- Step 1** Open the Event Log by navigating **Events > Event Log** from the menu bar.
- Step 2** Locate the event corresponding to the denied action in the Event Log.
- Step 3** For the appropriate event, click the Wizard link to launch the exception wizard.
- Step 4** Follow the steps given in the wizard to make the agent more permissive. Take the default settings offered by the wizard.

View Registered Hosts

Once you have distributed agent kits to your pilot hosts, you can see which hosts have successfully registered using any of these methods:

- In Simple or Advanced Mode, mouse-over **Configuration** in the menu bar and select **Host Security**. For a particular group, click the number of hosts in the hosts column to see which hosts have registered as a member of that group.
- In Advanced Mode, mouse-over the **Systems** menu and select **Hosts**. This takes you to the **Hosts list** page. On the right side of this page is a column that displays varying types of information on each host. Use the pulldown menu for this column to view hosts that are Active.
- To search for specific hosts based on more status data, use the **Search** option in CSA MC. Search for Hosts using available status information such as:
 - Active hosts—A host is active if it polls into CSA MC at regular intervals.
 - Not active hosts—A host is inactive if it has missed a certain number polling intervals or if it has not polled into the server for at least one hour.

Policy Tuning and Troubleshooting

Once you have started your CSA pilot, you may need to tune the policies to suit your needs and troubleshoot any problems that occur. Beyond creating exceptions you may need to tune rules to deny or allow user actions or prevent false positives. Tuning policies is best done using Advanced Mode.

Overall Guidelines

This section presents some overall guidelines for tuning and troubleshooting your CSA pilot. Please read through this section carefully and consider the specific needs and requirements of your pilot before moving on to actually using the techniques. Here are the most important guidelines to follow when tuning and troubleshooting policies:

- *Never directly modify one of the supplied groups, policies, or rule modules unless you are using the links provided through the Home page or Host Security page.* The groups, policies, rule modules provided are designed to work in your enterprise with minimal or no tuning. Using the links provided on the Home page and Host Security page will direct you to the areas that require your attention. If you need to dramatically change a group, policy, or rule module, make sure you *clone and rename* it first so you preserve it for use later. Modifying the supplied groups, policies, and rule modules directly makes it difficult to back out of any inadvertent mistakes.
- Policies displaying a red [warning] link on the Host Security page may need your attention. Click the warning link to display the Policy Warning dialog box. In the box you will find links to one or more items that may have already been customized but may require occasional updates. Customize each item by clicking its link in the Policy Warning dialog box and editing the pop-up provided.
- Use the supplied groups and if necessary define additional groups for *each distinct desktop and server type* in your network. In your pilot, you should have some participants that are using each desktop and server type so you can tune and troubleshoot all policies before deployment.

Group membership is cumulative, which can be useful in tuning and troubleshooting. For example, at the beginning of a pilot, participating hosts that are Windows desktops would be attached to the **All Windows** and **Desktops** groups. Once you are satisfied with the performance of these basic policies, you could define a new group for a specific department's applications, attach hosts to the new group, and pilot those policies.

- If you are running your pilot with policies or groups in Audit Mode, examine the event log (**Events -> Event Log** menu) for possible tuning and troubleshooting needs before moving to enforcement mode (also known as live mode). With the current release, you can place *individual policies within a group* in audit mode or a *single rule module* in audit mode. Therefore, as you tune and troubleshoot, you can incrementally move rule modules to enforcement mode if need be. Keep in mind when using audit mode that the area under test is completely vulnerable from a security standpoint.
- Policy tuning and troubleshooting is an *iterative* process. Focus on a single policy for improvement at a time and then verify that the tuning and troubleshooting techniques did what you expected before deploying the improved policy.
- *Prioritize* the security features you want to implement with CSA policies. You can also prioritize applications and groups. By having clear priorities and working through a single policy improvement at a time, you can manage the complexity of deploying large policy sets in large networks. For example, based on priorities, you can keep a specific rule module in audit mode while the rest of the rule modules in the policy are in live mode.
- Large policy sets can generate enormous numbers of log messages. Another advantage of piloting one policy at a time is that you can focus on the just the events the new policy has generated. Otherwise, you need to use the tools provided that help *filter out* extraneous information and *isolate* the specific policy to be improved or behavior to be studied. For example, you can log only the events that result in Deny actions or create an exception rule that stops logging a specific event to reduce the overall number of log messages. In addition, host diagnostics can be used to filter rules based on the user state (that is, the user and group) the host is in, such as only logging the behavior of the rules used by members of the Administrator group. Monitor policies can be used in clever ways to focus in on specific behavior without interrupting applications and services.
- Set up *separate agent kits* to support the different features of your pilot. For example, you might have some desktop kits that have all policies in audit mode, some desktop kits with a basic set of well-tested policies in live mode plus one experimental policy in audit mode, and so forth. Labelling these kits clearly will help your pilot participants download the right set of policies you want to test and give you clear feedback on areas needing improvement.

Creating Policies for Your Special Applications

Once you have distributed and piloted a generic Desktops or Servers agent kit, you are ready to create and pilot policies that address the needs of special applications you in use in your enterprise.

The Application Behavior Investigation tool allows you to understand the behavior of these special applications.

Prioritize the applications that you want to protect and begin your analysis with the highest priority application. From the menu bar, navigate **Analysis -> Application Behavior Investigation > Behavior Analyses** to launch the Behavior Analyses tool. Using this tool will allow you to understand the behavior of the application, craft a policy, place it in audit mode on the pilot machines, and examine the event log. Use the techniques in the rest of this section to tune/troubleshoot that application's policy, re-examine the event log, and if you are satisfied with the result, place the application's policy in live mode on the pilot machines. You repeat these steps with each application on your prioritized list.

Using Audit Mode

CSA policies can execute in *live mode*, where they enforce rules by denying or allowing events, or *audit mode*, where they indicate in the event log what the action would have been to the given event. All entries in the event log for rules in audit mode begin with the label `AuditMode:` to make it easy to scan for events relating to rules under test. In general, you start a pilot in audit mode and gradually change over to live mode as you examine the performance of each policy. You can place an entire group, individual policies within a group, or individual rule modules within a policy, in audit mode.

See the **Rule Module Configuration** chapter in *Using Management Center for Cisco Security Agents* and review the **Using Audit Mode** section for a complete discussion of how to use audit mode.



Note

When running your pilot, explain to participants the difference between audit mode and live mode, clearly label whether agent kits are for audit mode or live mode, and tell participants which kits to download and use during various phases of the pilot.

Audit mode is *not* intended to be used indefinitely because the area under test is completely vulnerable from a security standpoint. Groups and rule modules in audit mode should move to live mode in a timely fashion. Once the pilot is over, you need to carefully control which hosts if any are in audit mode. You can remove the audit mode kits to ensure they do not get downloaded during deployment and periodically monitor hosts involved in the audit to ensure that all pilot participants have migrated to live mode agent kits. You want to avoid the situation where a security hole exists after deployment because some groups or rule modules were inadvertently left in audit mode.

Disabling Specific Rules

When you examine the event log with the **Events -> Event Log** menu, the description of each event references the *rule number*. If you find a consistent pattern of false positives with the same specific rule number, you can disable that rule if desired. There are two different approaches to disabling rules:

- You can disable the rule *temporarily*. At a later time, you can go back and modify the rule, set up a query with a cached response, or set up an exception rule.
- You can disable the rule *permanently* if the rule protects a resource that you don't need protected as part of your security policy.

The easiest way to disable a rule is by clicking on the rule number at the bottom of the event description in the event log. On the rule page, you click on the Enabled checkbox to uncheck it and disable the rule. Once you generate the rules, this rule will be disabled.

Caching and Resetting Query Responses

Rules can be configured with enforcement actions of allow, deny, terminate, or query the user. In some cases, there are rules that already query the user but do so repeatedly instead of caching the user's response to make it persistent. In other cases, there are rules that are generating a mix of false positives and valid enforcements in the event log and need to be modified so they query the user and cache the user's response for the false positives.

You set up a query and cache the answer with *different* CSA MC menus:

- To set up a query, you display the rule you wish to modify by clicking on the rule number in the event log. You then select **Query User** from the action popup menu.

- To cache the response for a query, select the **Configuration -> Variables -> Query Settings** menu option, and then select the desired query from the page. Then, click on the **Enable “don’t ask again” option** checkbox if it is not already checked. When users receive the query and indicate they don’t want to be asked this query again, their answer is cached.

**Note**

One trade-off of setting up a cached query response is that users can answer the query inappropriately and then the inappropriate response becomes persistent. After setting up a cached query response, review the event log to make sure users are responding appropriately to the query. If some users give inappropriate responses, you can reset their agents and then give the users more information about responding to the query.

If a user has responded to a query inappropriately and the response is being cached, you can reset the user’s cache by doing the following:

1. Select the **Systems -> Hosts** menu option.
2. Click on the **<hostname>**.
3. Click the **Reset Cisco Security Agent** link in the Tasks menu.

Setting Up Exception Rules

In some cases, you need two or more different rules to completely specify the desired actions to a specific event. For example, you could have one rule that denies all applications from writing to the `//blizzard/webdocs` directory and another rule that allows the WebGuru application with authenticated user webmaster to write to the `//blizzard/webdocs` directory. The second rule allowing write access for WebGuru is considered *an exception rule* because it overrides a small part of the overall deny rule for the `//blizzard/webdocs/` directory. The MC manipulates the precedence of exception rules so that they are evaluated before the rules that they override.

Although you can create exception rules with the MC rule pages, the easiest way to create exception rules is using the Event Management Wizard from the event log. The wizard tailors its behavior to the event from which you launch it. You can use the wizard to create two general types of exception rules:

- Exception rules that under certain conditions allow an event that was denied
- Exception rules that stop logging similar events

To launch the wizard:

1. Select **Events -> Event Log**.
2. Click on the **Wizard** link at the bottom of the desired event’s description.

The wizard asks you questions about the following:

- Whether the exception rule applies to the user/state conditions of the triggering rule or the user/state conditions of the specific event where you launched the wizard. If you want the exception to apply to all users, you typically want the user/state conditions of the triggering rule (the default). If you want to create an exception rule only for the user specified in the event, you need to explicitly select the **specific user state conditions** radio button
- Whether the description of the proposed exception rule looks correct. Keep in mind that if you need to make some small changes to the rule, such as the applications specified, you can do so later. After the wizard finishes, you can still modify the exception rule further before saving it.

- Whether you want to put this new exception rule in a separate exception rule module (the default) or modify the rule module that triggered the event. In most cases, you want to put this in a separate exception rule module so you can preserve the supplied rule modules.
- Whether you want the exception rule based on the application specified in the event or whether you want to base it on a new application class.

After you click Finish in the wizard, the MC displays the new exception rule. At this point, you should do the following:

1. Change the **Description** field to an appropriate name.
2. Examine the details in the **when** box. If necessary, you can change these details to expand or narrow the conditions for the exception.
3. Click the **Save** button.

Configuring Your Own Policies

Creating a complete custom set of policies requires a team of network security experts who have assembled a detailed list of security features and studied the many supplied rule modules. The experts use the **Behavior Analyses** tool to thoroughly study the applications for which they will write rules. Then, the experts will craft custom policies by selecting the desired rule modules and rules. With this custom approach, consider conducting a small pilot of a few systems in a test lab and then expanding to a larger and more thorough pilot.

To create a set of custom policies these are the tasks you need to complete after you have assessed your application's vulnerabilities and decided on your security needs:

-
- | | |
|---------------|---|
| Step 1 | Familiarize yourself with the CSA MC user interface in Advanced Mode. See the chapter on Management Center for Cisco Security Agents Administration in <i>Using Management Center for Cisco Security Agents</i> (this is also referred to as the <i>User Guide</i>) for more information. |
| Step 2 | Select an existing rule module or create your own. See the chapter on Rule Module Configuration in the <i>User Guide</i> for more information. |
| Step 3 | Add existing rules to the rule modules or create your own rules and add them to the rule module. |
| Step 4 | Create a policy and associate rule modules with the policy. See the chapter on Building Policies in the <i>User Guide</i> for more information. |
| Step 5 | Associate the policy with a group you create or an existing group that you select. See the chapter on Configuring Groups and Managing Hosts in the <i>User Guide</i> for more information. |
| Step 6 | Create an agent kit to distribute the policy. See Configuring Groups and Managing Hosts in the <i>User Guide</i> for more information. |
| Step 7 | Monitor events created by the new policy, then tune and configure the policy. See the chapter on Event Logging and Alerts in the <i>User Guide</i> and Policy Tuning and Troubleshooting, page 3-7 . |

Distributing Agent Kits Using a Third Party Tool

Agent kits can be distributed using third party software distribution tools. After the agent has been downloaded and installed it will attempt to register with the CSA MC.

**Note**

The agent kit is a self-extracting executable file that contains several files (16 total) such as cab files, hdr, and setup files. In order to distribute agent kits using a third party software distribution tool, you must first extract the files manually from the agent kit and then run a script or a command from a command shell applying certain switches. The switches are referenced AFTER the extracted setup.exe.

This distribution methodology is for Windows agents only.

Step 1 Download the agent kit from CSA MC.

Step 2 Extract the files in the agent kit. If the agent kit is named **CSA-Desktops-setup-abc123.exe**, run this command from a command prompt:

```
c:\>CSA-Desktops-setup-abc123.exe -x
```

This will extract all the files to the directory

```
C:\{D933754D-B870-45b7-BFAA-1BDD2A7D4B80}
```

Step 3 Connect to the directory {D933754D-B870-45b7-BFAA-1BDD2A7D4B80}:

```
c:\>cd {D933754D-B870-45b7-BFAA-1BDD2A7D4B80}
```

Step 4 Run the extracted setup.exe with the necessary parameters for mass deployment.

This command is run as a local user:

```
setup.exe /s --targetdir=f:\installfolder\ --disable_net=0 --reboot=0
```

Notice the use of f2 in the next example. This will allow you to specify where the Installshield log directory will be written, just in case it cannot write to the drive where the setup.exe is located. This is useful if you are installing over a network:

```
setup.exe /s /f2"c:\setup.log" --autolevel=3 --reboot=0 --nshim=1 --startagent=0
```

Setup.exe Command Switches

The following are the switches for the agent setup.exe in versions 5.0.0.x and later

--autolevel

--autolevel switches define the amount of user interaction with the installation.

--autolevel=1 no questions are asked. The default actions are taken.

--autolevel=2 no warnings are displayed

--autolevel=3 suppresses all warnings and error messages

--autolevel=4 which makes the install completely silent (not even the message saying "Installing CSA" is displayed)

--reboot

--reboot=0 The agent install finishes silently and the host is not rebooted.

--reboot=1 The agent reboots automatically at the end of the install. (This is the default.)

--rebootdelay

--rebootdelay=x Specifies in seconds what the reboot delay is if reboot=1.



Note

If this parameter is missing and you set the machine to reboot (reboot=1), the default is 300 seconds (five minutes).

--startagent

This switch is applicable only if reboot=0.

startagent=0 The agent is not started after the installation is finished.

startagent=1 This agent is started after the installation is finished. This is the default setting.



Warning

The agent will provide NO security until the agent service is MANUALLY started or the machine is rebooted.

--disable_net

This switch is used to suspend agent security and prevent further connections to and from the machine.

--disable_net=0 We do not prevent network connections.

--disable_net=1 We do prevent any network connections. This is the default setting.



Warning

During an upgrade, the agent service is stopped. If this switch is set to 0, the machine is unprotected during the time of the upgrade.

--targetdir

This switch allows you to install the agent to a directory of your choice)

--targetdir=<path>

setup.exe /s --targetdir=c:\Path\To\Directory



Note

The <path> should NOT have quotes, even if the path contains spaces.

If the path does not exist, the installation will create it. Also, if the path is invalid (invalid driver letter or encrypted directory, for example), the installation aborts.

The default path, if no command line targetdir is specified, is

<PROGRAMFILES>\Cisco

--mt

This switch is used to uninstall CSA

--mt=removeall

for example:

```
C:\{D933754D-B870-45b7-BFAA-1BDD2A7D4B80}>setup.exe --mt=removeall
```

Command Examples

Example 3-1 *Install silently, no errors displayed, reboot at the end of install*

```
setup.exe /s --autolevel=3 --reboot=1
```

The reboot=1 will show the 5 minute countdown prior to reboot - this box cannot be suppressed at this time)

Example 3-2 *Install silently, do not log errors, force a reboot after 10 seconds*

```
setup.exe /s --autolevel=3 --reboot=1 --rebootdelay=10
```

Example 3-3 *Silent installation, install on f:\targetfolder, do not disable the NIC and do not reboot:*

```
setup.exe /s --autolevel=3 --targetdir=f:\installfolder\ --disable_net=0 --reboot=0
```

Example 3-4 *Silent uninstallation, no user interaction*

```
setup.exe /s /f1"%PROGRAMFILES%\InstallShield Installation  
Information\{DE499746-67B9-11D4-97CE-0050DA10E5AE}\setup.iss" --mt=removeall  
--autolevel=4
```

You will then need to reboot eventually, there is no forced reboot.

Example 3-5 *Silent uninstallation from the Installshield Installation Information folder:*

Change directories to:

```
*:\Program Files\InstallShield Installation  
Information\{DE499746-67B9-11D4-97CE-0050DA10E5AE}
```

Then run:

```
setup.exe /s /f1"D:\Program Files\InstallShield Installation  
Information\{DE499746-67B9-11D4-97CE-0050DA10E5AE}\setup.iss" --mt=removeall  
--autolevel=4
```

Example 3-6 *Drive independent uninstallation*

If you do NOT want the uninstall to be drive dependent, then you can wildcard the program files"

```
setup.exe /s /f1"%PROGRAMFILES%\InstallShield Installation  
Information\{DE499746-67B9-11D4-97CE-0050DA10E5AE}\setup.iss" --mt=removeall  
--autolevel=4
```



APPENDIX **A**

Cisco Security Agent Installation and Overview

Overview

This chapter describes the Cisco Security Agent and provides information on the agent user interface. It also includes installation information for Windows, Linux, and Solaris agents. (This information, with additional details, also appears in a similarly titled Appendix A in the User Guide.)

Once the agent is installed, there is no configuration necessary on the part of the end user in order to run the agent software. Optionally, as the administrator, you can ask users to enter individualized contact information into the fields provided. If required, the agent user interface makes it easy for the user to enter this data and send it to CSA MC.

This section contains the following topics.

- [Downloading and Installing, page A-1](#)
- [The Cisco Security Agent User Interface, page A-3](#)
- [Installing the Solaris Agent, page A-4](#)
- [Installing the Linux Agent, page A-6](#)

Downloading and Installing

Once you build an agent kit on CSA MC, you deliver the generated URL, via email for example, to end users so that they can download and install the Cisco Security Agent. They access the URL to download and then install the kit. This is the recommended method of agent kit distribution. But you may also point users to a URL for the CSA MC system. This URL will allow them to see all kits that are available. That URL is:

```
https://<system name>/csamc60/kits
```

If you are pointing users to the “kits” URL and you have multiple agent kits listed here, be sure to tell users which kits to download.



Note

Note that the Registration Control feature also applies to the <system name>/csamc60/kits URL. If the Registration Control feature (see the User Guide for details on the feature) prevents your IP address from registering, it also prevents you from viewing the agent kits URL.

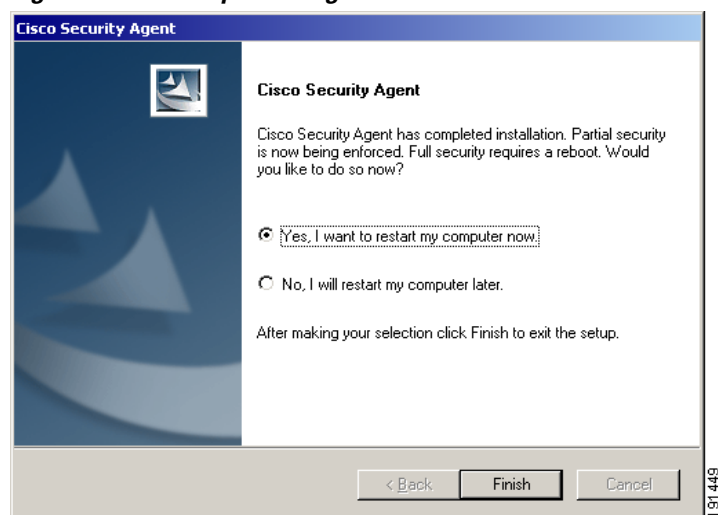


Note

Cisco Security Agent systems must be able to communicate with the Management Center for Cisco Security Agents over HTTPS.

Once users install agents on their systems, they can optionally perform a reboot (if Force reboot is not selected). See [Figure A-1](#). Whether a system is rebooted or not, the agent service starts immediately and the system is protected.

Figure A-1 *Optional Agent Reboot*



If a system is not rebooted following the agent installation, the following functionality is not immediately available. (This functionality becomes available the next time the system is rebooted.)

Windows agents

- Network Shield rules are not applied until the system is rebooted.
- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Data access control rules are not applied until the web server service is restarted.

Solaris and Linux agents, when no reboot occurs after install, the following caveats exist

- Network access control rules only apply to new socket connections. Network server services should be stopped and restarted for full network access control security without a system reboot.
- Buffer overflow protection is only enforced for new processes.
- File access control rules only apply to newly opened files.
- Data access control rules are not applied until the web server service is restarted.

After installation, the agent automatically and transparently registers with CSA MC. To see which hosts have successfully registered, switch to Advanced Mode, from the **Systems** menu select **Hosts**. This displays the hosts list view. All registered host system names appear here.

The Cisco Security Agent User Interface

**Note**

The Cisco Security Agent user interface does not run on Solaris systems.

**Note**

If the **Agent UI control rule** is not present (available on Windows and Linux only) for the system group, no agent UI appears on the end user system.

To open the Cisco Security Agent user interface on Windows and Linux systems, users can double-click on the flag icon in their system trays. The user interface opens on their desktop.

As the administrator, you decide which agent UI options to provide to the end user. These options are controlled by the Agent UI control rule. Available options are as follows:

- **Allow user to reset agent UI default settings**—Selecting this checkbox in the Agent UI control rule causes the end user to have a product reset option available from the **Start>Programs>Cisco>Cisco Security Agent** menu. Selecting the “Reset Cisco Security Agent” option puts all agent settings back to their original states and clears almost all other user-configured settings. This does not clear configured Firewall Settings or File Protection settings. But if these features are enabled, they are disabled as this is the default factory setting. The information entered into the edit boxes for these features is not lost.
- **Allow user interaction**—Selecting this checkbox in the Agent UI control rule causes the end user to have a visible and accessible agent UI, including a red flag in the system tray.
- **Allow user access to agent configuration and contact information**— Selecting this checkbox in the Agent UI control rule provides Status, Messages, and Contact Information features, including the ability to manually poll the MC.
- **Allow user to modify agent security settings**—Selecting this checkbox in the Agent UI control rule provides System Security and Untrusted Applications features.
- **Allow user to modify agent personal firewall settings**—Selecting this checkbox in the Agent UI control rule provides Local Firewall Settings and File Protection features.

The options available to the user in the agent UI depend upon the features selected in the Agent UI control rule governing the agent in question. All possible agent features are described in Appendix A of the User Guide.

Uninstall Windows Cisco Security Agent

To uninstall the Cisco Security Agent, do the following:

From the **Start** menu, go to **Programs>Cisco>Cisco Security Agent>Uninstall Cisco Security Agent**. Reboot the system when the uninstall is finished.

**Note**

You can also uninstall the agent from the **Start>Settings>Control Panel> Add/Remove Programs** dialog.

Installing the Solaris Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Solaris systems. After you download the agent kit from CSA MC, do the following to unpack and install it. (Note that you can put the downloaded tar file in any temp directory. Do not put it in the opt directory; however, as you may then experience problems with the installation.)



Note

See also **UNIX Agent csactl Utility** in Appendix A of *Using Management Center for Cisco Security Agents* for information on a Solaris agent utility which allows you to manually poll to CSA MC and perform other tasks.

Step 1 You must be super user on the system to install the agent package.

```
$ su
```

Step 2 Untar the agent kit. (In the following example, **CSA-Server_6.0.1.100-setup.tar** is the name of the agent kit.)

```
# tar xf CSA-Server_6.0.1.100-setup.tar
```

Step 3 Install the agent package. (Use the command listed below when you install. This command forces the installation to use a package administration file to check the system for the required OS software agent dependencies. If the required dependencies are not present, such as the “SUNWlibCx” library, the install aborts.)

```
# pkgadd -a CSCOcsa/reloc/cfg/admin -d . CSCOcsa
```

When the install is complete, the following is displayed:

```
The agent installed cleanly, but has not yet been started. The
command: /etc/init.d/ciscosec start will start the agent. The agent
will also start automatically upon reboot. A reboot is recommended to
ensure complete system protection.
```

Step 4 Optionally, reboot the system by entering the following.

```
# shutdown -y -i6 -g0
```



Note

If the Solaris system is not rebooted following the agent installation, the following functionality is not immediately available: Buffer overflow protection is only enforced for new processes, network access control rules only apply to new socket connections, file access control rules only apply to newly opened files, and data access control rules are not applied until the web server service is restarted. (This functionality becomes available the next time the system is rebooted.)



Note

On Solaris 10, when you reboot the system after upgrading the agent, the system will perform the reboot once, display these messages, and reboot, automatically, again.

```
svc.startd[7]:system/csaservice : default failed: transitioned to maintenance (see 'svcs
-xv for more details')
```

```
svc.startd[7]:system/webconsole :console failed: transitioned to maintenance (see 'svcs
-xv for more details')
```

After second reboot, you will not receive any other messages and regarding CSA and CSA will be fully functional.

The agent installs into the following directory:

```
/opt/CSC0csa
```

Some files are put into additional directories such as
`/kernel/strmod/sparcv9`, `usr/lib/csa`, `/etc/init.d` and `/etc/rc?.d`.

**Note**

If you are upgrading the Solaris agent and you encounter the following error, “There is already an instance of the package and you cannot install due to administrator rules”, you must edit the file `/var/sadm/install/admin/default`. Change “instance=unique” to “instance=overwrite” and then proceed with the upgrade.

**Note**

See also **Manual Agent Data Filter Installation**, in chapter 12 of *Using Management Center for Cisco Security Agents*, if you are installing a web server on the same server as the Solaris agent.

Uninstalling Solaris Agent

When uninstalling the Solaris Agent you must be in a session which has permission to disable CSA. The Agent Service Control rules in the **Base - CSA service control (Solaris)** rule module provided with this release, define the sessions given permission to disable CSA.

While running the default **Base - CSA service control (Solaris)** rule module, booting directly into multi-user mode using the **Command Line Login** option or booting directly into single-user mode gives you the permission to uninstall CSA.

**Note**

When running Solaris 10, if you boot into multi-user mode and then switch to single-user mode, you do not have permission to disable CSA.

To uninstall CSA:

- Step 1** Boot directly into **multi-user mode** using the **Command Line Login** option or boot directly into **single-user mode**.
- Step 2** Login as the **root** user.
- Step 3** At the prompt, enter the following command:

```
# pkgrm CSC0csa
```
- Step 4** Reboot the machine.

**Note**

If an agent is running a policy which contains an Agent self protection rule, the agent cannot be uninstalled unless your session has the permission to disable it. (Administrators can generally do this through a remote management session if the default policies applied to the CSA MC/VMS system are not changed to restrict this access.)

A shipped UNIX policy allows secured management applications to stop the agent service. For example, after having logged in by selecting Command Line Login in the options menu of the login screen, all login applications are considered secure management applications. You can now run the `pkgrm` command to uninstall the agent.

Installing the Linux Agent

This section details the commands you enter and the subsequent output that is displayed when you install the Cisco Security Agent on Linux systems.

Step 1 Move the tar file downloaded from CSA MC to a temporary directory, for example:

```
$ mv CSA-Server_V5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959a30b2.tar /tmp
```

Step 2 Untar the file, for example:

```
$ cd /tmp
$ tar xvf CSA-Server_V5.2.0.218-lin-setup-1a969c667ddb0a2d2a8da3e7959a30b2.tar
```

Step 3 Connect to the CSCOCsa directory where the rpm package is located, for example:

```
$ cd /tmp/CSCOCsa
```

Step 4 Run script `install_rpm.sh` as root, for example:

```
# sh ./install_rpm.sh
```

The package will be installed to `/opt/CSCOCsa`, with some files being put into directories such as `/lib/modules/CSCOCsa`, `/lib/csa`, `/etc/init.d` and `/etc/rc?.d`.

As the installation proceeds, you receive these messages:

```
If you wish to install the CSA data filters Apache 2.0, you will need to run the
install script by hand:
```

```
cd /opt/CSCOCsa/app_plugins/apache
./i.csafilter install
```

```
Warnings about non-GPL modules are to be expected and can be ignored The Agent UI may
have to be added to customized Gnome/KDE session files manually
(gnome-session-properties for GNOME). To do this, add /opt/CSCOCsa/bin/ciscosecui to
the startup programs list.
```

```
If this system is running a web server, the csa service module must be installed.
Execute /opt/CSCOCsa/app_plugins/apache/i.csafilter to copy the module and modify the
httpd configuration appropriately. The web server will be restarted automatically.
```

For more information about installing data filters, see “Manual Agent Data Filter Installation” in chapter 12 of *Using Management Center for Cisco Security Agents*.

Step 5 After a successful installation, you receive the message “The installation has completed successfully. For Full protection to be enabled, it is recommended that the machine be rebooted.”

Step 6 Reboot the host after the installation is complete.



Note

CSAagent rpm packages are not relocatable.



Caution

If a system is not rebooted following the agent installation, the following functionality is not immediately available: Buffer overflow protection is only enforced for new processes, network access control rules only apply to new socket connections, file access control rules only apply to newly opened files, and data access control rules are not applied until the web server service is restarted. (This functionality becomes available the next time the system is rebooted.)

**Note**

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/CSCOcsc/bin/ciscosecui`) manually (using “gnome-session-properties” utility) to make the agent UI auto-start.

**Caution**

On Linux systems, if you upgrade the kernel version or boot a different kernel version than the initial version where the agent was installed, you must uninstall and reinstall the agent.

Uninstalling Linux Agent

You can uninstall Linux agents from the command line or by using the GUI.

Uninstalling Cisco Security Agent from a command line

- Step 1** Log on to the host as the root user.
- Step 2** CD to the directory: `/opt/CSCOcsc/bin`
- Step 3** At the prompt enter: `./uininstall`
- Step 4** When warned that CSA is being disabled, select **Yes** to allow the action, type an explanation in the “Please Explain” field and then click **Apply**.
- Step 5** When you have successfully uninstalled CSA, you receive the message, “Cisco Security Agent has been uninstalled. Press Enter to exit...” Press **Enter**.
- Step 6** Restart the computer.

Uninstalling Cisco Security Agent using the GUI

- Step 1** Log on to the host as the root user.
- Step 2** From the Applications menu, select Cisco Security Agent > Uninstall Cisco Security Agent.
- Step 3** When warned that CSA is being disabled, select **Yes** to allow the action, type an explanation in the “Please Explain” field and then click **Apply**.
- Step 4** When you have successfully uninstalled CSA, you receive this message in a terminal window: “Cisco Security Agent has been uninstalled. Press Enter to exit...” Press **Enter**.
- Step 5** Restart the computer.

**Caution**

If an agent is running a policy which contains an Agent self protection rule, the agent cannot be uninstalled unless this rule is disabled. (Administrators can generally do this through a remote management session if the default policies applied to the CSA MC system are not changed to restrict this access.) See **Agent self protection** in the User Guide for details on this rule type.

You can uninstall the linux agent regardless of policies if you login using single user mode.



APPENDIX **B**

Open Source License Acknowledgements and Third Party Copyrights

Cisco Security Agent utilizes third party software from various sources. Portions of this software are copyrighted by their respective owners as indicated in the copyright notices below.

The following acknowledgements pertain to this software license.

- [OpenSSL/Open SSL Project, page B-1](#)
- [Apache \[version 2.0.59\], page B-3](#)
- [TCL license, page B-6](#)
- [Perl, page B-6](#)
- [Socket6, page B-7](#)
- [libpcap, page B-7](#)
- [CMU-SNMP Libraries, page B-8](#)
- [Open Market FastCGI, page B-8](#)
- [CGIC License, page B-9](#)
- [Mozilla 1.xx \(libcurl\), page B-9](#)
- [MICROSOFT SOFTWARE LICENSE TERMS, page B-9](#)
- [.Net Framework 2.0, page B-12](#)
- [MarshallSoft Computing SMTP/POP3 Email Engine, page B-13](#)
- [Jasper Reports V1.2.0 and JFreeChart V1.0.5, page B-13](#)
- [iText version 1.3.1, page B-20](#)
- [Java Runtime Environment JRE 1.5.0.06, page B-26](#)
- [The GNU General Public License \(GPL\), page B-29](#)

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Apache [version 2.0.59]

Xerces 2.7 and AxisCpp 1.6

Copyright © 2000-2005 The Apache Software Foundation. All rights reserved.

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a

cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the tradenames, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work

(including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

TCL license

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that the existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. Government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARS. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

Perl

Copyright 1987-2005, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the GNU General Public License, which may be found in the Perl 5 source kit.

Complete documentation for Perl, including FAQ lists, should be found on this system using ``man perl'` or ``perldoc perl'`. If you have access to the Internet, point your browser at <http://www.perl.org/>, the Perl Home Page.

Socket6

Copyright (C) 2000-2005 Hajimu UMEMOTO <ume@mahoroba.org>. All rights reserved.

Socket6.pm and Socket6.xs are based on perl5.005_55-v6-19990721 written by KAME Project.

gai.h, getaddrinfo.c and getnameinfo.c are based on ssh-1.2.27-IPv6-1.5 written by KIKUCHI Takahiro <kick@kyoto.wide.ad.jp>.

Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

libpcap

Copyright (c) 1993, 1994, 1995, 1996, 1997, 1998, The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of California, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CMU-SNMP Libraries

This product contains software developed by Carnegie Mellon University. Copyright 1998 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Open Market FastCGI

This FastCGI application library source and object code (the "Software") and its documentation (the "Documentation") are copyrighted by Open Market, Inc ("Open Market"). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here. If modifications to this Software and Documentation have new licensing terms, the new terms must be clearly indicated on the first page of each file where they apply.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION,

INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS". OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

CGIC License

CGIC, copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Thomas Boutell and Boutell.Com, Inc.. Permission is granted to use CGIC in any application, commercial or noncommercial, at no cost. HOWEVER, this copyright paragraph must appear on a "credits" page accessible in the public online and offline documentation of the program. Modified versions of the CGIC library should not be distributed without the attachment of a clear statement regarding the author of the modifications, and this notice may in no case be removed. Modifications may also be submitted to the author for inclusion in the main CGIC distribution.

Mozilla 1.xx (libcurl)

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2007, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2005 EXPRESS EDITION

MICROSOFT SQL SERVER 2005 EXPRESS EDITION WITH ADVANCED SERVICES

MICROSOFT SQL SERVER 2005 EXPRESS TOOLKIT

MICROSOFT SQL SERVER 2005 MANAGEMENT STUDIO EXPRESS

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.

1. INSTALLATION AND USE RIGHTS.

- a. **Installation and Use.** You may install and use any number of copies of the software on your devices.
- b. **Included Microsoft Programs.** The software contains other Microsoft programs. These license terms apply to your use of those programs.

2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

- a. **Distributable Code.** You are permitted to distribute the software in programs you develop if you comply with the terms below.
 - i. **Right to Use and Distribute.** The software is "Distributable Code."
 - **Distributable Code.** You may copy and distribute the object code form of the software. You may not modify the software, and your programs must include a complete copy of the software, including set-up.
 - **Third Party Distribution.** You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.
 - ii. **Distribution Requirements.** For any Distributable Code you distribute, you must
 - add significant primary functionality to it in your programs;
 - require distributors and external end users to agree to terms that protect it at least as much as this agreement;
 - display your valid copyright notice on your programs;
 - indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs; and
 - if the software is Microsoft SQL Server 2005 Management Studio Express or Microsoft SQL Server 2005 Express Toolkit, distribute it with either:
 - Microsoft SQL Server 2005 Express Edition or
 - Microsoft SQL Server 2005 Express Edition with Advanced Services.
 - iii. **Distribution Restrictions.** You may not
 - alter any copyright, trademark or patent notice in the Distributable Code;
 - use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
 - distribute Distributable Code to run on a platform other than the Windows platform;
 - include Distributable Code in malicious, deceptive or unlawful programs; or

- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
 - the code be disclosed or distributed in source code form; or
 - others have the right to modify it.
3. **INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the software. It may change or cancel them at any time.
 4. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not
 - disclose the results of any benchmark tests of the software to any third party without Microsoft's prior written approval;
 - work around any technical limitations in the software;
 - reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
 - make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
 - publish the software for others to copy; or
 - rent, lease or lend the software.
 5. **BACKUP COPY.** You may make one backup copy of the software. You may use it only to reinstall the software.
 6. **DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.
 7. **TRANSFER TO A THIRD PARTY.** The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.
 8. **EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
 9. **SUPPORT SERVICES.** Because this software is "as is," we may not provide support services for it.
 10. **ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.
 11. **APPLICABLE LAW.**
 - a. **United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
 - b. **Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY.** THE SOFTWARE IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES.** YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

.Net Framework 2.0

End-User License Agreement

MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

MICROSOFT .NET FRAMEWORK 2.0

Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows operating system software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use a copy of this supplement with each validly licensed copy of the software.

The following license terms describe additional use terms for this supplement. These terms and the license terms for the software apply to your use of this supplement. If there is a conflict, these supplemental license terms apply.

By using this supplement, you accept these terms. If you do not accept them, do not use this supplement. If you comply with these license terms, you have the rights below.

1. **SUPPORT SERVICES FOR SUPPLEMENT.** Microsoft provides support services for this supplement as described at www.support.microsoft.com/common/international.aspx.
2. **MICROSOFT .NET FRAMEWORK BENCHMARK TESTING.** This supplement includes the .NET Framework component of the Windows operating systems (".NET Component"). You may conduct internal benchmark testing of the .NET Component. You may disclose the results of any benchmark test of the .NET Component, provided that you comply with the following terms: (1) you must disclose all the information necessary for replication of the tests, including complete and accurate details of your benchmark testing methodology, the test scripts/cases, tuning parameters applied,

hardware and software platforms tested, the name and version number of any third party testing tool used to conduct the testing, and complete source code for the benchmark suite/harness that is developed by or for you and used to test both the .NET Component and the competing implementation(s); (2) you must disclose the date (s) that you conducted the benchmark tests, along with specific version information for all Microsoft software products tested, including the .NET Component; (3) your benchmark testing was performed using all performance tuning and best practice guidance set forth in the product documentation and/or on Microsoft's support web sites, and uses the latest updates, patches and fixes available for the .NET Component and the relevant Microsoft operating system; (4) it shall be sufficient if you make the disclosures provided for above at a publicly available location such as a website, so long as every public disclosure of the results of your benchmark test expressly identifies the public site containing all required disclosures; and (5) nothing in this provision shall be deemed to waive any other right that you may have to conduct benchmark testing. The foregoing obligations shall not apply to your disclosure of the results of any customized benchmark test of the .NET Component, whereby such disclosure is made under confidentiality in conjunction with a bid request by a prospective customer, such customer's application(s) are specifically tested and the results are only disclosed to such specific customer. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the .NET Component, provided it complies with the same conditions above.

MarshallSoft Computing SMTP/POP3 Email Engine

License for Use and Distribution

MarshallSoft Computing, Inc. grants the registered user of SEE4C the right to use one copy of the SEE4C DLL's on a single computer in the development of any software product. The user may not use the library on more than one computer at the same time.

However, the registered DLLs (SEE16.DLL and SEE32.DLL) may be distributed without royalty with the user's compiled application, provided that the value of the keycode is not revealed.

The "student" (\$73.50) registered DLL's may not be distributed under any circumstances, nor may they be used for any commercial purpose.

The "professional" (\$105) registered DLL's may be distributed (without royalty) in object form only, as part of the user's compiled application. The registered DLL's may NOT be distributed as part of any software development system (compiler or interpreter) without our express written permission.

When you register, you will be sent a "key code" which enables access to the registered DLL's. You may NOT distribute or make known this key code.

Registered DLLs do NOT expire. Registered users may download free updates for a period of one year from the date of purchase.

[END]

Jasper Reports V1.2.0 and JFreeChart V1.0.5

jTDS version 1.2

JFreeChart version 1.0.5

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be

introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

iText version 1.3.1

MOZILLA PUBLIC LICENSE Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant. The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant. Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

- (a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and
- (b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).
- (c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.
- (d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License. The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code. Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications. You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

- (a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a

recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations. Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices. You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions. You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works. You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABILITY, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the

parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____. Portions created by _____ are Copyright (C) _____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [_____] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [_____] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

Java Runtime Environment JRE 1.5.0.06

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA SE RUNTIME ENVIRONMENT (JRE) VERSION 6 SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT.

INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. **DEFINITIONS.** "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java Platform, Standard Edition (Java SE) on Java-enabled general purpose desktop computers and servers.

2. **LICENSE TO USE.** Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. **RESTRICTIONS.** Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. **LIMITED WARRANTY.** Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. **DISCLAIMER OF WARRANTY.** UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. **LIMITATION OF LIABILITY.** TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. **TERMINATION.** This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at <http://www.sun.com/policies/trademarks>. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government primecontractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against

any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

D. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

E. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

F. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

G. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at <http://java.com/data/>.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

The GNU General Public License (GPL)

The source code needed to build our Clam AntiVirus components is provided with the CSA MC kit. These Clam AntiVirus components are **csaclamutil**, which was developed by Cisco to scan files, and its supporting libraries: **ClamAV** and **GMP**. The source code is stored in the **\OpenSource** directory in the **sources.zip** file.

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and a brief idea of what it does.

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.



INDEX

Symbols

.Net Framework 2.0 license acknowledgement [B-12](#)

A

Active hosts [3-7](#)

Agent

 optional reboot after install [A-2](#)

 user interface [A-3](#)

Agent (Linux)

 installing [A-6](#)

Agent (Solaris)

 installing [A-4](#)

 migrating from V4.x [2-41](#)

Agent installation, automatic [2-30](#)

agent kits

 distributing with 3rd party tool [3-11](#)

Agent migration [2-40](#)

Agent-server size ratio [1-20](#)

Apache [A-6](#)

Apache license acknowledgement [B-3](#)

auto-enrollment groups [2-37](#)

B

Browser requirements [1-9](#)

C

Certificate import [2-42, 2-45](#)

CGIC License acknowledgement [B-9](#)

Cisco Security Agent Analysis

 license [2-3](#)

Cluster support [1-11](#)

CMU-SNMP Libraries license acknowledgement [B-8](#)

Content engine [1-21](#)

CSA agent

 about [1-2](#)

CSA MC [1-4](#)

 about [1-2](#)

 browser requirements [1-9](#)

 changing the CSA MC server's hostname [2-10](#)

 environment requirements [1-9](#)

 Language setting [1-11](#)

 logging in [2-35](#)

 login locally [2-36](#)

 login remotely [2-36](#)

 Policies [3-4](#)

 Required Regional Language Options [1-11](#)

 System Locale [1-11](#)

 system requirements [1-4](#)

 User Locale setting [1-11](#)

CSA MC configuration

 Single server [1-19](#)

 Three servers, multi-tiered [1-19](#)

 Two servers [1-19](#)

D

Data Loss Prevention [2-3](#)

 license [2-3](#)

Deployment overview [1-2](#)

Detailed description [3-4](#)

Directory paths to CSA Versions [2-10](#)

DLP Desktop Agent Upgrade [2-3](#)

DNS environments [1-9](#)

F

File Integrity Check

on CSA software delivered on CD [2-6](#)

on downloaded CSA software [2-5](#)

File Integrity check [2-5](#)

Firefox [1-9](#)

clearing cache [2-47](#)

G

GNU General Public License [B-29](#)

Groups

No user interaction [A-3](#)

H

Hosts

active [3-7](#)

not active [3-7](#)

search [3-7](#)

view [3-7](#)

Hotfix information [2-47](#)

HTTPS [A-2](#)

I

Import migration data [2-40](#)

Import Root Certificate [2-42](#)

Inactive hosts [3-7](#)

Installing Microsoft SQL Server 2000

as a remote database [2-21](#)

Installation

agent [A-1](#)

certificate (IE) [2-42](#)

with 3rd party tool [3-11](#)

Installation Log [2-35](#)

Installing CSA MC [2-10](#)

3 tier system [2-30](#)

configuration options [2-10](#)

distributed configuration [2-30](#)

installation options [2-10](#)

license information [2-2](#)

using remote database [2-24](#)

with local database [2-10, 2-12](#)

with previous version's database [2-31](#)

with remote database [2-10](#)

with remote remote database [2-21](#)

Installing Microsoft SQL Server 2000 [2-21](#)

as remote database [2-21](#)

Installing Microsoft SQL Server 2005

as remote database [2-22](#)

Installing Microsoft SQL Server 2005 or 2000

local installation [2-19](#)

Installing Microsoft SQL Server Express [2-14, 2-20](#)

manual installation [2-20](#)

Internationalization support [1-12](#)

Windows 2000 [1-13](#)

Internet Explorer

clearing cache [2-47](#)

version support [1-9](#)

iText version 1.3.1 license acknowledgement [B-20](#)

J

Jasper Reports version 1.2.0 license
acknowledgement [B-13](#)

Java Runtime Environment JRE 1.5.0.06 license
acknowledgement [B-26](#)

JFreeChart, version 1.0.5 license acknowledgement [B-13](#)

L

libpcap license acknowledgement [B-7](#)

License types [2-2](#)

- Cisco Security Agent Analysis [2-3](#)
- Data Loss Prevention (DLP) [2-3](#)
- server platforms [2-3](#)
- workstation platforms [2-3](#)
- Licensing import information [2-30](#)
- Licensing information [2-2](#)
 - license file contents [2-3](#)
 - license types [2-2](#)
 - PAK certificates [2-2](#)
 - troubleshooting [2-4](#)
 - uploading a license [2-4](#)
- Local database install [2-10](#)
- Log
 - installation [2-35](#)
- Logging in to CSA MC
 - locally [2-36](#)
 - remotely [2-36](#)
- logging in to CSA MC [2-35](#)
- Logging on to CSA MC
 - maximum concurrent CSA MC users [3-2](#)

M

- MarshallSoft Computing SMTP/POP3 Email Engine license acknowledgement [B-13](#)
- MICROSOFT SOFTWARE LICENSE TERMS [B-9](#)
- Microsoft SQL Server 2000
 - installing as remote database [2-21](#)
- Microsoft SQL Server 2005
 - installing as remote database [2-22](#)
- Microsoft SQL Server 2005 and 2000 [2-19](#)
 - local installation [2-19](#)
- Microsoft SQL Server Express [2-20](#)
 - manual installation [2-20](#)
- Microsoft SQL Server express installation [2-12](#)
- Migrating [2-7](#)
 - migration scenarios [2-8](#)
 - to CSA V6.0.1 from V5.2 and earlier [2-39](#)
 - upgrading from CSA V6.0 to V6.0.1 [2-7](#)

- Migrating from CSA 5.2 and earlier [2-7](#)
- migration_data_export.xml [2-40](#)

N

- Not active hosts [3-7](#)
- No user interaction [A-3](#)

O

- Open Market FastCGI license acknowledgement [B-8](#)
- OpenSSL - Open SSL Project [B-1](#)
- Operating system changes, agent [1-6, 1-8](#)
- Operating systems sample [3-5](#)
- Overview of product [1-1](#)

P

- Perl license acknowledgement [B-6](#)
- Pilot Program
 - recommendations [3-4](#)
 - size of pilot [3-4](#)
 - time frame of pilot [3-5](#)
- Policies
 - exception rules [3-10](#)
 - pre-configured modules [3-4](#)
 - query responses [3-9](#)
 - Test Mode as a tool [3-9](#)
 - tuning and troubleshooting [3-7](#)
 - updating mandatory policies [2-37](#)
- Polling interval recommendation [1-21](#)
- ports [1-10](#)
 - agent kit caching [1-10](#)
 - agents communicating with csamc [1-10](#)
 - Application Analysis jobs [1-10](#)
 - https [1-10](#)
 - SNMP traps [1-10](#)
 - SQL Server [1-10](#)

VPN and VMS [1-10](#)
 ports...-mail alerts [1-10](#)
 prepare__migration.exe [2-39](#)
 Product overview [1-1](#)
 prototype groups [2-37](#)

Q

Quick start setup [3-1](#)

R

Reboot optional
 agent [A-2](#)
 Registered hosts
 view [3-7](#)
 Remote access [3-2](#)
 Remote access to CSA MC [2-36](#)
 Remote database install [2-11](#)
 Requirements
 agent [1-6](#)
 cluster support [1-11](#)
 DNS and WINS [1-9](#)
 port availability [1-10](#)
 server [1-4](#)
 time and date settings [1-10](#)
 web browsers [1-9](#)
 Root certificate import [2-42, 2-45](#)

S

Scalability
 hardware sizing [1-19](#)
 server configurations [1-19](#)
 Scalable deployment [1-19](#)
 configuration recommendations [1-21](#)
 content engines [1-21](#)
 hardware sizing [1-19](#)

polling interval [1-21](#)
 software considerations [1-20](#)
 three servers [1-19](#)
 Secure communications [2-41](#)
 Socket6 license acknowledgement [B-7](#)
 Solaris agent install directory [A-5](#)
 Solaris host migration [2-41](#)
 Solaris requirements
 agent [1-7](#)
 SSL [2-41](#)
 System requirements [1-4](#)
 CSA MC on VMWare ESXi [1-4](#)
 minimum CSA MC [1-4](#)
 Windows agent [1-6](#)

T

TCL license acknowledgement [B-6](#)
 Terminal services [1-6](#)
 third party installation tools [3-11](#)
 Time settings
 remote db and CSA MC system [2-21](#)

U

Uninstall CSA MC [2-46](#)
 UNIX agent install directory [A-5](#)
 Update mandatory policies [2-37](#)
 Upgrade naming conventions [2-40](#)
 Upgrading
 CSA V6.0 to CSA V6.0.1 [2-7](#)
 from CSA V6.0 to V6.0.1 [2-37](#)
 migrating from CSA V5.2 and earlier [2-7](#)
 upgrade scenarios [2-8](#)
 Upgrading CSA MC
 3 tier system [2-38](#)
 distributed configuration [2-38](#)
 with local or remote database [2-37](#)

V

Version labels [2-40](#)
Virtual machine support [1-11](#)
VMWare ESXi [1-4, 1-11](#)

W

Web-based user interface [1-2, 1-3](#)
Web browser
 requirements [1-9](#)
WEPOS 1.1 [1-6](#)
Windows Cluster support [1-11](#)
Windows requirements
 agent [1-6](#)
WINS environments [1-9](#)

