Symantec™ Event Agent Implementation Guide

Symantec™ Event Agent Implementation Guide

Documentation version: 4.8

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Installing Symantec Event Agents

This chapter includes the following topics:

Preinstallation requirements

The prerequisites for installing the Symantec Event Agent are as follows:

- The host name should be resolvable from the computer on which you want to install Symantec Event Agent.
  The `/etc/hosts` file must have the IPv4 and IPv6 addresses listed against the host name.
- The install process stops if any previous installations of the agent are detected. You must uninstall all previous versions of the agent to continue.

Before you install the Symantec Event Agent, you should complete the following steps in the order presented:

- Uninstall any previous version of the agent.
  See "Uninstalling the Symantec Event Agent" on page 21.
- If you do not use a DNS server, ensure that the hosts file includes the following:
  - IP address
  - Host name information for the Information Manager server

  See the *Symantec Event Collectors Integration Guide*.
- Ensure that there is network connectivity between the system where the agent is installed and the Information Manager server.
- If there is a firewall between the agent computer and the Information Manager server, ensure that the following ports are open:
  - Depending on the user settings, at least one of the following ports must be open:
    TCP 10012
    TCP 10010
    TCP 443
  - The following port needs to only be open one way from the Information Manager server to the agent computer:
    TCP 5998
  - TCP 8086

See "Downloading and installing Symantec Event Agents on Windows, Linux, and Solaris" on page 13.

Supported platforms and operating systems

Table 1-1

Platform	Operating systems
Microsoft	■ Microsoft Windows Server 2003 (all editions) with Service Pack 2 or later (32-bit and 64-bit) ■ Microsoft Windows XP Professional ■ Microsoft Windows Vista Enterprise (32-bit and 64-bit) ■ Microsoft Windows Server 2008 Standard Edition (32-bit and 64-bit) ■ Microsoft Windows Server 2008 Enterprise Edition (32-bit and 64-bit) ■ Microsoft Windows Server 2008 R2 ■ Microsoft Windows 7 Enterprise (32-bit and 64-bit) ■ Microsoft Windows 7 Enterprise (32-bit and 64-bit) **Note:** For Agent communication with Information Manager over IPv6, Symantec recommends installing the Agent on Windows 7/Windows 2008, or Windows 2008 R2. You may observe intermittent connectivity issues when the Agent is installed on Windows 2003/Windows XP and communicates with Information Manager over IPv6. The connectivity issues are not observed in case of IPv4.
Linux	■ Red Hat Enterprise Linux 5.0 Advanced platform ■ Red Hat Enterprise Linux 5.0 Server (32-bit and 64-bit) ■ Red Hat Enterprise Linux 6.0 Server (32-bit and 64-bit) ■ Ubuntu 8.04 LTS 64-bit
Solaris	■ Solaris 10 (SPARC) ■ Solaris 11 (SPARC)

See “Supported deployments for Symantec Event Agent” on page 12.

Supported deployments for Symantec Event Agent

The following deployments are supported for Symantec Event Agent 4.8:

- 32-bit Symantec Event Agent on 32-bit OS (Windows, Linux , Solaris)
- 32-bit Symantec Event Agent on 64-bit OS (Windows, Linux , Solaris)
- 64-bit Symantec Event Agent on 64-bit OS (Windows, Linux , Solaris)
- 32-bit Symantec Event Agent communicating with 32-bit Information Manager server (4.7.4 and below)
- 64-bit Symantec Event Agent communicating with 32-bit Information Manager server (4.7.4 and below)
- 32-bit Symantec Event Agent communicating with 64-bit Information Manager server (4.8)
- 64-bit Symantec Event Agent communicating with 64-bit Information Manager server (4.8)

See "Supported platforms and operating systems" on page 11.

See "Downloading and installing Symantec Event Agents on Windows, Linux, and Solaris" on page 13.

Minimum system requirements

To install and run the console for the Symantec Security Information Manager agent, your computer must meet the following minimum requirements:

- Minimum screen resolution setting of 1024 x 768
  A setting of 1280 x 1024 is recommended.
- RAM minimum 512 MB, recommended 1 GB
- Minimum HDD requirements:
  - Windows Agent: 500 MB
  - Linux/Solaris Agent: 210 MB
- Connection to the same internal network as the Information Manager Server

Installing Symantec Event Agent for Ubuntu Platform

Ubuntu 8.04 LTS 64-bit is a supported platform for SSIM Linux agent. You can install both 32-bit and 64-bit versions of agent on a 64-bit Ubuntu server.

You must install the following packages on Ubuntu servers before installing the agent.

- openssh-server and openssh-client
- selinux-utils
- ia32-libs (to support 32-bit installation)
- glibc
- zlib (must include libz.so.1 under the /lib directory)
- libstdc++

You can install these packages using the following commands:

`sudo apt-get install pkgName`, where pkgName is any of the three packages listed.

The following are the prerequisites for installation:

- Ubuntu servers have static IP.
- Only root user can perform installation. Admin user can log on as root by running `sudo -s` command at the terminal prompt.
- You must run install script from bash shell. You can enter bash shell by running `bash` command on terminal prompt.

All the scripts must be run from bash shell. For example, for performing agent management operation, you must run `bash ./agentmgmt.sh` from agent installation directory.

Downloading and installing Symantec Event Agents on Windows, Linux, and Solaris

Symantec Event Agent must be installed before you install the collector component. A single installation of the Symantec Event Agent may host multiple collector installations. Also, the agent can send events to only one Information Manager server at a time.

Java Runtime Environment (JRE) 1.7.0.03 is automatically installed along with the agent into a subdirectory of the installation directory that is specified at installation. By default, the directory is C:\Program Files\Symantec\Event Agent\jre on Windows and /opt/Symantec/sesa/Agent/jre on UNIX and Linux. Only the collector component and the agent use the JRE; it does not interfere with any other JRE that is installed on the computer.

To download and install the Symantec Event Agent on a computer that runs Windows

1. On the remote computer, launch the at the following URL:

   https://*Information_Manager_Host_Name_or_IP_address*

   Symantec recommends that you use the Fully Qualified Domain Name of the Information Manager.

   https://*Information_Manager_IP_address*

2. From the Information Manager Web interface, click **System > Downloads > Downloads**.
3. Click **Symantec Event Agent 4.8 Installer for Windows**, and save the file to a directory on the remote computer.

   This option downloads a file that is named `symevtagent_windows_r4.8.0.*.exe`.

4. To install the Symantec Event Agent, double-click the file that you downloaded in step 3 and follow the prompts that are displayed on the Symantec Event Agent Installation Wizard .

   On a 64-bit computer, you are provided an option to either install a 32-bit version or a 64-bit version of the Symantec Event Agent.

5. Select the location to install Symantec Event Agent.
6. Enter the IP address or host name of the Information Manager server that Symantec Event Agent connects to.

   The IP address can be an IPv4 address or an IPv6 address.

7. Once the connectivity test is passed, install the third-party CA root certificate.

Note: For Agent communication with Information Manager over IPv6, Symantec recommends installing the Agent on Windows 7/Windows 2008, or Windows 2008 R2. You may observe intermittent connectivity issues when the Agent is installed on Windows 2003/Windows XP and communicates with Information Manager over IPv6. The connectivity issues are not observed in case of IPv4.

To download the Symantec Event Agent on a computer that runs Linux or Solaris (using GUI)

1. On the remote computer, launch the at the following URL:

   https://*Information_Manager_Host_Name_or_IP_address*

   Symantec recommends that you use the Fully Qualified Domain Name of the Information Manager.

2. From the , click **System > Downloads**.

3. Click and save the file to a directory on the remote computer.

   Click one of the following options:

   - **Symantec Event Agent 4.8 Installer for Linux**
   - **Symantec Event Agent 4.8 Installer for Solaris**

   This option downloads a .tar.gz file.

To download the Symantec Event Agent on a computer that runs Linux from the command line

1. Log in to the Linux computer on which you want to install the agent.

2. At the command prompt, type the following commands:

   scp db2admin@*<IM server_ip>*:/opt/Symantec/sesa/servletengine/webapps/imr/downloads/agent/linux/symevtagent_linux_r4.8*.tar.gz /tmp

3. When prompted, enter the password for the db2admin account on the Information Manager server and the agent then begins downloading to the /tmp directory.

To download the Symantec Event Agent on a computer that runs Solaris from the command line

1. Log in to the Solaris computer on which you want to install the agent.

2. At the command prompt, type the following commands:

   scp db2admin@*<IM server_ip>*:/opt/Symantec/sesa/servletengine/webapps/imr/downloads/agent/solaris/symevtagent_solaris_r4.8*.tar.gz /tmp

3. When prompted, enter the password for the db2admin account on the Information Manager server and the agent then begins downloading to the /tmp directory.

To install the Symantec Event Agent on a computer that runs Linux or Solaris

1. Navigate to the directory where you downloaded the .tar.gz file.
2. For Linux, at the command prompt, type the following command:

   `tar -zxvf symevtagent_linux_`*`version`*`.tar.gz`

   This command creates a subdirectory that is named `Agent`, and then unpacks the agent installation files into that directory.

   For Solaris, at the command prompt, type the following commands (if you have the SUNWgzip package installed):

   `gunzip symevtagent_solaris_`*`version`*`.tar.gz`

   `tar xvf symevtagent_solaris_`*`version`*`.tar`

   The first command ungzips the tar.gz file. The second command creates a subdirectory that is named `Agent`, and then unpacks the agent installation files into that directory.
3. At the command prompt, to run the install script, type the following commands:

   `cd Agent`

   `sh install.sh`
4. At the prompts, enter the appropriate information.

On a 64-bit computer, you are provided an option to either install a 32-bit version or a 64-bit version of the Symantec Event Agent. In case you install a 32-bit version of Symantec Event Agent on a 64-bit computer you should install the following dependent 32-bit packages along with the agent:

- **glibc**
- **zlib** (Must include `libz.so.1` under the `/lib` directory)
- **libstdc++**

Note: These packages should be 32-bit versions even if their 64-bit versions are already installed.

Running Symantec Event Agent as a non-root user

By default, the Symantec Event Agent is installed to run under the root user account and may not be desirable. The nonroot.sh script that is included with the Symantec Event Agent can be used to change this behavior.

To run the Symantec Event Agent as a non-root user

1. Make sure that the Agent is installed using root user credentials.
2. Install Collector using root user credentials.
3. While configuring Collector, change the syslog sensor port from 514 to a number higher than 1024, for example, 10514.
4. As the root user, edit the nonroot.sh script file with a text editor, such as vi. Perform the following steps:
   - Go to the line that reads:

     ```
     USERID=sesuser
     ```

     Change *sesuser* to the user name of the account you want to use to run the Symantec Event Agent.
   - Go to the line that reads:

     ```
     GROUPID=ses
     ```

     Change *ses* to the group name of the account that you want to use to run the Symantec Event Agent.

   If the user name and group name do not exist, the script creates them.
5. Run the nonroot.sh script.

   This script prepares the agent for running under a non-root user account. The agent must be installed before you run this script. The agent is restarted using the user and the group ID that is specified in the script. The user and group are automatically created if they do not already exist.

   If you want to perform LiveUpdate on any of the installed collectors after nonroot.sh had been executed, the non-root user must have permissions to read or update the file /etc/liveupdate.conf. It can be achieved by running the command `chown USERID:GROUPID /etc/liveupdate.conf` where USERID and GROUPID are the same as what is declared in nonroot.sh

Installing Symantec Event Agent silently

You can now install Symantec Event Agent silently by using the command line. This option can be used in Windows as well as on Linux operating systems.

- To install the agent silently on a computer that runs Windows, you must create the `installer.properties` file or edit the server and the path details in the `installer.properties` file.
  To create this file, refer to Sample installer.properties file.

Ensure to place the `installer.properties` file in the same location where the `symevtagent_windows_r4.8.0.*.exe` file is located and then run the following command:

`symevtagent_windows_r4.8.0.*.exe -i silent`

- To install the agent silently on a computer that runs Linux, edit the server and the path details in the `agent.settings` file.
  To create this file, refer to Sample agent.settings file
  The `agent.settings` file is present in the Agents directory when the downloaded `agent tar.gz` file is extracted. Run the following command:
  `symevtagent_windows_r4.8.0.*.exe -silent`

Sample installer.properties file

You can refer to this sample, while creating an `installer.properties` file for installing agent silently on a computer that runs Windows.

```
-------------------------------------------------------------------------

# Tue Dec 14 17:45:58 IST 2010

# Replay feature output

# --------------------

# This file was built by the Replay feature of InstallAnywhere.

# It contains variables that were set by Panels, Consoles or Custom Code.

#Choose Install Folder

#--------------------

USER_INSTALL_DIR=C:\\Program Files\\Symantec\\Event Agent

#SSIM Server Information

#----------------------

IP=127.0.0.1

IP_CONNECT=1

#INSTALLATION_TYPE=32 Bit Installation

INSTALLATION_TYPE=64 Bit Installation

#Install CA root certificates

#---------------------------

cacertspath="<PATH to Certificate1>,<PATH to Certificate2>
```

Sample agent.settings file

SESA Agent Installer properties

srcpath specifies the path to the agent files relative to the current # directory (where the .jar file is, which in our case is the current directory, ".") srcpath=.

modify paths here to override default install paths # Note: Any characters in the paths that contain ':', '\', '!', '=' or ' ' (space)

must be preceded by a '\' character. IE C:\SESA-Agent = C\:\\SESA-Agent

Do NOT use the '#' character in pathnames, CIMOM cannot handle this

In addition double quote characters should be avoided in specified paths

agentdirwin32=

agentdirunix=

If using Anonymous SSL (the default) the mserverip value MUST be in IP notation.

In turn, if the Agent is to use Authenticated SSL the host name must be specified. If an IPv6 address is provided for the mserverip field, the IP address must be enclosed in a square bracket. For example: [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx].

mserverip=127.0.0.1

mserverport=443

usessl=1

cacertenable=n

cacertpath=

the parameters that the JVM uses

Note: Precede ':', '\', '!', '=' or ' ' with a backslash

Note: -server option will not be used if agent installer detects that

its jre does not support server option

jvmparams=-server\ -XX\:NewRatio\=3\ -Xmx512m\ -Dnetworkaddress.cache.ttl\=300

the parameters that CIMOM uses

Note: Precede ':', '\', '!', '=' or ' ' with a backslash

cimomparams=-p\ 5998\ -auto

how long the service waits for CIMOM to start (in seconds)

cimomtimeout=300

This property is included for compatibility with N-1 integrating products.

New products should use cimomparams to specify the port number instead.

cimomport=

background task time allotment for service (in seconds)

agentpolling=300

servlet URL Prefix for the SESA servlets

servletprefix=/sesa/servlet/

service startup mode. can be auto or demand

startupmode=auto

flag to indicate whether service should be started immediately after installation

startimmediate=1

This property specifies the organizational unit distinguished name (DN) that this agent should belong to, which is where it will be bootstrapped.

If the value is left blank, the agent will be bootstrapped into the default

OrgUnit (ou=Default) within the domain being managed by the SES Management Server specified in "mserverip" above.

If the Agent should be bootstrapped into an OrgUnit other than Default, then the entry should contain the complete DN or the intended OrgUnit.

Ex. initialOrgUnitDn=ou\=Europe,ou\=Locations,dc\=SES,o\=symc_ses

The domain(s) (dc=) portion of the path should correspond to the domain managed by the SES Management Server (mserverip setting). If it doesn't a different domain that is managed by the Management Server should be selected, or the Management Server (mserverip) should be changed to one that does manage that domain.

initialOrgUnitDn=

leave agentdir/extdir blank. they will be set by the install program

agentdir=

extdir=

flag to indicate whether Java LiveUpdate should be installed installjlu=1

the following setting controls the installation of the TCPShim module

valid values are "no", "client" or "server" # "no" - do not install TCPShim

"client" - install TCPShim as a client for installation on servers

"server" - install TCPShim as a server for installation on clients

tcpshim=no

tcpshimpass=password

agentbit=64

Uninstalling the Symantec Event Agent

Uninstalling the Symantec Event Agent removes the Java application that performs communication functions between Information Manager and the collector.

If other products do not use the Symantec Event Agent, you must uninstall the Symantec Event Agent after you have uninstalled the collector component.

To uninstall the Symantec Event Agent

1 Navigate to the agent installation directory as follows:

- On Windows, the default installation directory on Windows is as follows:
  C:\Program Files\Symantec\Event Agent

  Note: When the Symantec Event Agent is uninstalled from a 64-bit Windows operating system, the entry for the Agent continues to be listed in the **Add/Remove** programs. Although the Agent gets uninstalled the entry is not cleared from the **Add/Remove** programs. To remove this entry completely from the **Add/Remove** programs, the Agent should be uninstalled once again.

- On Linux and Solaris, log on as superuser, and then navigate to the installation directory.
  The default installation directory on Linux and Solaris is as follows:
  /opt/Symantec/sesa/Agent

2 To uninstall the Symantec Event Agent, do one of the following tasks:

- On Windows, at the command prompt, type the following command:

  setup -u -debug

- On Linux, at the command prompt, type the following command:

  sh ./install.sh -u

- On Solaris, at the command prompt, type the following command:

./install.sh -u

3 Manually delete the Symantec Event Agent files in the following directories:

- On Windows, the default folder is as follows:
  C:\Program Files\Symantec\Event Agent
- On Linux and Solaris, the default folder is as follows:
  /opt/Symantec/sesa/Agent folder

Chapter 2

Managing Symantec Event Agents

This chapter includes the following topics:

Running the Agent Management utility

The Agent Management utility lets you manage the agent directly from the agent computer.

To run the Agent Management utility

1. Run the Agent Management utility.
   - On Windows, the default utility path is as follows: C:\Program Files\Symantec\Event Agent\agentmgmt.bat
   - On Linux and Solaris, the default utility path is as follows: /opt/Symantec/sesa/Agent folder/agentmgmt.sh
   - On Ubuntu server, run the utility from bash shell. For example, `bash ./agentmgmt.sh`
2. Select the option that you want.

   See "About the Agent Management utility" on page 24.

About the Agent Management utility

The following table lists the options that are available when you run the Agent Management utility.

See "Running the Agent Management utility" on page 23.

Table 2-1 Options available with the Agent Management utility

Option	Name	Information
Option 1	Show Agent Status	Shows the following information about the agent status: ■ Port to which it is connected ■ Connection status ■ Number of events received ■ Number of events sent ■ Name of the server it is connected to
Option 2	Flush Agent Queue	Forces the agent to reconnect and send data to the server. This option flushes the queue manually. By default, the queue is flushed when one of the following occurs: ■ Flush timeout occurs (by default, every 4 seconds) ■ The number of events in the queue is greater than the flush count size. If the agent is in disconnected mode, then flushing the queue resets the agent to connected mode and send events to the server.
Option 3	Reload Agent Configurations	Reloads the agent configuration from the Information Manager server without restarting the agent
Option 4	Force Agent to send its Software Inventory and state Updates	Forces the agent to send information about software inventory and state updates to LDAP directory.
Option 5	View log files	Opens the log files for viewing. Note: Selecting this option displays an error if UI is not supported on the Linux and Solaris terminal.

Table 2-1 Options available with the Agent Management utility *(continued)*

Option	Name	Information
Option 6	Force Re-Bootstrap of Agent to same or different server	Restarts the agent to the existing or different server, used to reconnect to the same server or different server.
Option 7	Gather data for Technical Support	Gathers the data such as logs, configurations which are added into a zip file named `sesa-<HostName>-<guid>.zip`.
Option 8	Enable or disable Collector Debug	Changes the log level to debug.
Option 9	Start the Agent	Starts the agent.
Option 10	Stop the Agent	Stops the agent.
Option 11	Restart the Agent	Restarts the Agent
Option 12	Quit the menu	Closes the menu.

Chapter 3

Verifying Symantec Event Agent Installation and Operation

This chapter includes the following topics:

Verifying Symantec Event Agent installation

To verify installation of the Symantec Event Agent, you can perform the following tasks in the order presented:

- Verify Symantec Event Agent connectivity from Information Manager.
  See "To verify Symantec Event Agent connectivity from Information Manager" on page 28.
- Verify the Information Manager IP address and Symantec Event Agent port.
  See "To verify the Information Manager IP address and the Symantec Event Agent port" on page 28.

To verify Symantec Event Agent connectivity from Information Manager

1. From a Windows computer that has the Information Manager Client installed, log on with an Information Manager user account with sufficient rights to view events.

   The Information Manager user must belong to a role that has rights to the Information Manager-integrated collector.
2. In the Information Manager console, in the left pane, click **System**.
3. On the **Administration** tab, expand the tree until you see Organizational Units.
4. Expand **Organizational Units >** [Default].

   [Default] is the name of the Organizational Unit where your agent is located.

   Note: Any Organizational Unit change is applied only after the agent restarts.
5. Verify that the name of the collector computer is listed.
6. Right-click the computer name, and then click **Properties**.
7. In the **Computer Properties** dialog box, on the **Services** tab, verify that the Agent Service displays Yes in the Started column.

To verify the Information Manager IP address and the Symantec Event Agent port

1. From the collector computer, navigate to the Symantec Event Agent installation folder.

   On Windows, the default location is C:\Program Files\Symantec\Event Agent

   On UNIX, the default location is /opt/Symantec/sesa/Agent

   On UNIX, you must become superuser.
2. In a text editor, such as Notepad on Windows or vi on UNIX, open the configprovider.cfg file.
3. Verify that the following options contain the correct settings for the collector product to which you want to send events:
   - MgmtServer contains the correct Symantec Security Information Manager IP address.
   - MgmtPort contains the correct Symantec Event Agent port number (default value is 443).

Verifying Symantec Event Agent operation

You can verify that the Symantec Event Agent is operating correctly by running the Show Agent Status script.

See "Verifying Symantec Event Agent installation" on page 27.

To run the Show Agent Status script Symantec Event Agent operation

1. On the collector computer, navigate to the agent directory as follows:
   - On Windows, the default location is C:\Program Files\Symantec\Event Agent.
   - On UNIX, the default location is /opt/Symantec/sesa/Agent.
     On UNIX, you must become superuser.
2. To access the Collector and Agent Management scripts, at the command prompt, do one of the following steps:
   - On Windows, type the following command:
     agentmgmt.bat
   - On UNIX, type the following command:
     sh agentmgmt.sh
3. At the **SSIM Collector / Agent Management Scripts** menu, select the following option:
   1. Show Agent Status

If the agent is not running, the following message appears:

```
Command: .\jre\bin\java -jar agentcmd.jar -status
The agent command cannot be executed.
Failed to make a connection to the agent.
The Symantec Event Agent is possibly not running.
Press any key to continue...
```

If the agent is running, something similar to the following message appears:

```
Symantec Event Agent (v 4.8.0.11) -
Copyright(c) 2002-2012 - Symantec Corporation
Symantec Event Agent status: running
Listening on: 127.0.0.1:8086
Sending on Port: 10012
SSL: Off
SSIM Server URL: http://127.0.0.1:80/sesa/servlet/
Outbound Thread State: CONNECTED
Java Version 1.7.0_03
```

```
Queue Status
  Total events accepted: 248
  Total events forwarded: 248
  Entries waiting in queue: 0
  Queue File: ./QueueFiles/filequeue.1333376838093.que
  Flush Size (KB): 2000
  Flush Count: 512
  Flush Time (sec): 4
  Spool Size (KB): 20000
  Max Queue Size (KB): 80000

HTTP forwarding statistics:
  Total number of HTTP post failures: 0
Event Acceptor HTTP ThreadPool:
  Thread 0 state = IDLE
  Thread 1 state = IDLE
  Thread 2 state = IDLE
  Thread 3 state = IDLE

Last state update time: Tue Apr 03 11:37:11 IST 2012
Last configuration download request time: none
Last configuration update invocation time: Tue Apr 03 11:37:09 IST 2012
Last configuration update completion time: none
```

Note: If Symantec Event Agent is installed on a computer that is assigned with an IPv6 address and an IPv4 address, the agent continues to listen on 127.0.0.1 IP address. This applies for the agents that are installed along with the Information Manager as well as for the agents that are installed separately.

Starting and stopping Symantec Event Agent services or daemons

If you install the collector on a Windows computer, the Symantec Event Agent runs as a service. If you install the collector on a UNIX computer, the Symantec Event Agent runs as a daemon. To start and stop the Symantec Event Agent, you start and stop the services or daemons as necessary.

To start and stop the Symantec Event Agent service

1. On the collector computer, navigate to the agent directory as follows:
   - On Windows, the default location is C:\Program Files\Symantec\Agent.
   - On UNIX, the default location is /opt/Symantec/sesa/Agent.

On UNIX, you must become superuser.

2 To access the Collector and Agent Management Scripts, do one of the following steps:

- On Windows, type the following command:

  agentmgmt.bat

- On UNIX, type the following command:

  sh agentmgmt.sh

3 At the **SSIM Collector / Agent Management Scripts** menu, select one of the following options:

10. Start the Agent

11. Stop the Agent