Symantec™ Security Information Manager 4.7.3 Release Notes

Symantec™ Security Information Manager 4.7.3 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 4.7.3

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND 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 SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 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

Overview

This chapter includes the following topics:

- Documentation
- About Symantec Security Information Manager

Documentation

The product disk of the Symantec Security Information Manager contains the following documentation:

Online Help for the Web configuration interface and the Information Manager console (client).	Contains the information on how to use the product. You can access the online Help by clicking the Help icon in any dialog box, or by pressing the F1 key.
Symantec Security Information Manager User Guide	Contains the information on how to use the product. The document is in the PDF format.
Symantec Security Information Manager Administrator Guide	Contains the information on how to manage the configuration and administrative tasks after the installation. The document is in the PDF format.
Symantec Security Information Manager Installation Guide	Contains the information on how to install and upgrade the product. The document is in the PDF format.
Symantec Security Information Manager Reporting Guide	Contains the information on how to use the reporting feature in the product. The document is in the PDF format.

Symantec Security Information Manager Release Notes	Contains a list of the known issues. The document is in the PDF format.

For the updated version of these documents, visit http://www.symantec.com/business/support/overview.jsp?pid=52517.

About Symantec Security Information Manager

Symantec™ Security Information Manager provides real-time event correlation and data archiving to protect against security threats and to preserve critical security data. The Information Manager collects and archives security events from across the enterprise. These events are correlated with the known asset vulnerabilities and current security information from the Global Intelligence Network. The resulting information provides the basis for real-time threat analysis and security incident identification. The Information Manager archives the security data for forensic and regulatory compliance purposes.

The Information Manager collects, analyzes, and archives information from security devices, critical applications, and services, such as the following:

- Firewalls
- Routers, switches, and VPNs
- Enterprise Antivirus
- Intrusion detection and Intrusion Prevention Systems
- Vulnerability scanners
- Authentication servers
- Windows and UNIX system logs

The Information Manager provides the following features to help you recognize and respond to threats in your enterprise:

- Normalization and correlation of events from multiple vendors.
- Event archives to retain events in both their original (raw) and normalized formats.
- Distributed event filtering and aggregation to ensure that only relevant security events are correlated.
- Real-time security intelligence updates from Symantec™ Global Intelligence Network to keep you apprised of global threats and to let you correlate internal security activity with external threats.

- Customizable event correlation rules to let you fine-tune threat recognition and incident creation for your environment.
- Security incident creation, ticketing, tracking, and remediation for quick response to security threats. Information Manager prioritizes incidents based upon the security policies that are associated with the affected assets.
- A powerful Event Viewer that lets you easily mine large amounts of event data and identify the machines and users that are associated with each event.
- A client-based console from which you can view all security incidents and drill down to the related event details, that includes affected targets, associated vulnerabilities, and recommended corrective actions.
- Predefined and customizable queries to help you demonstrate compliance with the security and the data retention policies in your enterprise.
- A Web-based configuration interface that lets you monitor and configure settings, manage licenses, and perform routine maintenance tasks such as backup and restore. You can also download various utilities and use the custom logs feature with the universal collectors to collect and map information from devices for which standard collectors are not available.

What's new in Symantec Security Information Manager 4.7.3

This chapter includes the following topics:

- New features

New features

Symantec Security Information Manager (SSIM) 4.7.3 has the following new features in addition to fixes to the issues in the older version.

Audit event for actions used in query execution

Automatically assigning incidents to the least busy member in a user group

Enhanced filter for user search

FIPS operational mode

Java LiveUpdate upgrade to version 3.7

New correlation rule based on Lookup Table Update rule type

New version of Symantec Event Agent

Selective backup, restore, and purge

Time zone retention for triggering a rule

2048-bit certificate requests

Audit event for actions used in query execution

Whenever you run a query or a report which contains a query, an audit event is generated. The audit event captures the details of the actions that are used to execute the query. The **Option1** field for the audit event that is generated is set as **Query Execution**.

From the **Event Details** dialog box, you can view the audit information of the actions that are used for the query execution. When you click the **Description** field in the **Event Details** box, the following details are displayed:

- Query execution date and time
- User who has run the query
- Type of query (Private/Published/System)
- Name of the query
- Parameters that are used to run the query, such as conditions, time range, and archives

Automatically assigning incidents to the least busy member in a user group

In Symantec Security Information Manager, an incident is created whenever an event matches a criterion that is specified in the rules and monitors. Based on the rules that are set, these incidents can be automatically assigned to a specific user group or an individual user. Now, rules or monitors can be set to assign incidents automatically to the least busy member in a user group. The incidents are automatically assigned based on the load factor of the users in a user group.

Incidents that are automatically assigned to the least busy member in a user group are listed against **SSIM** in the incident log.

Enhanced filter for user search

While assigning tickets and incidents to users or while creating a new user, you can now use the **Look in Group** filters when you search for a user. This option is available in the **Find Users** dialog box. Using the **Look in Group** filter, you can locate a user group and search for the user within that user group.

FIPS operational mode

The Federal Information Processing Standards (FIPS) operational mode is achieved in Symantec Security Information Manager 4.7.3. For more information see *Symantec Security Information Manager 4.7.3 FIPS 140-2 Operational Mode Guide*.

Java LiveUpdate upgrade to version 3.7

Symantec Security Information Manager use Java LiveUpdate to update various SSIM Components such as Collectors, Rules, Queries, GIN Content, and so on.

The existing certificate that is used by Java LiveUpdate expires on April 30, 2011. To use the new certificate, Java LiveUpdate has to be updated to version 3.7. When you upgrade Symantec Security Information Manager to 4.7.3, Java LiveUpdate gets updated to 3.7 on the Information Manager server.

To use LiveUpdate for Collectors that are installed with Symantec Event Agent on computers having Windows, Linux and Solaris, you must install Symantec Event Agent 4.7.1.

New correlation rule based on Lookup Table Update rule type

The **Lookup Table Update** rule is set to dynamically collect information in the lookup tables. Any rule can refer to this information to generate incidents and events. You can create a correlation rule which refers to an existing lookup table that gets dynamically updated. This rule is created only for updating the lookup table. Hence, conclusions are not created for the **Lookup Table Update** rule.

New version of Symantec Event Agent

A new version of the agent, Symantec Event Agent 4.7.1, is released with SSIM 4.7.3. Symantec Event Agent 4.7.1 contains fixes to the issues in the older version.

Refer to the Resolved issues section for the list of issues that are fixed in Symantec Event Agent 4.7.1.

Symantec Event Agent installed on the Symantec Security Information Manager server gets upgraded to version 4.7.1 when Symantec Security Information Manager server is upgraded to version 4.7.3. For agents that are installed on computers that run Windows, Linux, or Solaris, you must uninstall the older versions of agents and then install Symantec Event Agent 4.7.1.

See Installing Symantec Event Agent 4.7.1.

Selective backup, restore, and purge

Symantec Security Information Manager now lets you back up and restore data selectively from the Web Configuration Interface. Components can be selected for backup from the database and the LDAP. In addition, these components that are backed up can be selectively restored. During a discrepancy instead of restoring all the data to an earlier state, you can select and restore only those data items that you require. These data items can be selected for an immediate or a scheduled backup. Moreover backup files can be selected individually for purging.

Time zone retention for triggering a rule

If you use **Event Date** when you specify a rule condition, you can select the time zone from which an event has originated. This specification establishes the appropriate time of an event correlation. The **Server Time** is the default time zone that is considered for an event correlation. However, you can also choose either the **Source Network Time Zone** or the **Destination Network Time Zone** for the networks that are managed through Information Manager. The time zone that is associated with a network can be added when you create a new network or when you edit the network properties. The time zone must be entered in the **GMT +/- HH:MM** format.

- **Server Time**
  Server time is the default time zone that is considered for an event correlation. If this default time zone is retained, then the time zone of the Information Manager server is considered for an event correlation.
- **Source Network Time Zone**
  If you select this option, whenever an event occurs, the time zone of the source network is considered for an event correlation. The source network is derived from the IP source address in the event.
- **Destination Network Time Zone**
  If you select this option, whenever the event occurs, the time zone of the destination network is considered for an event correlation. The destination network is derived from the IP destination address in the event.

2048-bit certificate requests

Symantec Security Information Manager now lets you create and accept 2048-bit certificate requests.

Chapter 3

Installation and configuration

This chapter includes the following topics:

- Installing Symantec Security Information Manager 4.7.3
- Installing Symantec Event Agent 4.7.1

Installing Symantec Security Information Manager 4.7.3

Preinstallation requirements

Apply the Maintenance Pack only to the Information Manager servers running 4.7.1 or later versions of the software, as shipped by Symantec.

Before you install SSIM 4.7.3, make sure that 300 MB of free disk space is available in the / partition. Save all your work and close any Information Manager console sessions that are open.

Note: There is no facility to rollback or uninstall the Maintenance Pack.

Installing the Maintenance Pack

You must complete the preinstallation procedures before you install the pack.

The Primary SSIM Directory server must be updated first. After installation, restart must be completed before installing on other SSIM Servers. Any replica SSIM Directories must then be updated, followed by all other SSIM Servers.

Note: The installer must run only from the /tmp directory on the server. If you attempt to run the installer from any other location, the installer exits with an error.

To install the Maintenance Pack, do the following:

1. Connect to the appliance using an account with administrative or superuser privileges either by using an SSH client or by logging on locally.
2. Download the `Symantec_Security_Information_Manager_4.7.3_Linux_EN.tar.gz` and `.md5` files to the `/tmp` folder. If you install on other locations, the installation process fails. You must use **BINARY** mode when transferring the files to the server. Some FTP utilities use **ASCII** mode by default, which corrupts the installation file.
3. Verify the integrity of the downloaded `.tar.gz` file by using a file verification tool such as **md5sum**, which is included with the Linux installation. If you use md5sum, execute the following command:

   ```
   md5sum -c
   Symantec_Security_Information_Manager_4.7.3_Linux_EN.tar.gz.md5
   ```

   Both the `.tar.gz` and `.md5` files must be present in the same directory for md5sum to execute correctly.

   For more information on **md5sum**, see the Linux man pages.
4. Unpack the Maintenance Pack by executing the following command:

   ```
   tar -xvzf
   Symantec_Security_Information_Manager_4.7.3_Linux_EN.tar.gz
   ```
5. Change directories to the Maintenance Pack folder by executing the following command:

   ```
   cd MaintenancePack473
   ```
6. Execute the following command:

   ```
   sh install.sh
   ```

Note: The installer automatically stops and restarts services as necessary and restarts the server when done. The SSIM installation history file is updated with the SSIM Maintenance Pack number. The SSIM installation history file is located at /etc/ssim-history.

Installing Symantec Event Agent 4.7.1

When you install Symantec Security Information Manager 4.7.3, Symantec Event Agent 4.7.1 is installed. For agents that are installed on computers that run Windows, Linux, or Solaris, you must uninstall the older versions of agents and then install Symantec Event Agent 4.7.1.

For more information on preinstallation requirements, supported platforms, minimum system requirements, and uninstalling the agent, refer to *Symantec Event Agent 4.7 Implementation Guide*.

Downloading and installing Symantec Event Agents

The Symantec Event Agent sends the data that is collected by the Symantec event collector to the Information Manager server. The agent must be installed before installing the collector component. You must sometimes install agents on the same computer as the security product for which it collects events; in other cases you can install the collector on a separate computer from the security product for which it collects events. This computer must have network access to the Information Manager server.

The Symantec Event Agent sends the data that is collected by the collector to the Information Manager server.

If you want to install and use a Universal collector on a remote computer, you must download and install the Symantec Event Agent on the same computer as the collector component.

Note: 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.

Note: Java Runtime Environment (JRE) 1.6 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.

When you complete the Symantec Event Agent operation, you can verify installation by completing the following procedures:

- Verify Symantec Event Agent installation

- Verify Symantec Event Agent operation
- Starting and stopping Symantec Event Agent services and daemons

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

1 On the remote computer, launch the Information Manager Configuration Web site 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 Information Manager Configuration Web page, click **Downloads**.

3 Click **Symantec Event Agent 4.7.1 Installer for Windows**, and save the file to a directory on the remote computer.

This option downloads a file that is named `install.exe`.

4 To install the Symantec Event Agent, double-click the `install.exe` file that you downloaded in step 3, and then follow the prompts.

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

1 On the remote computer, launch the Information Manager Configuration Web site 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 Information Manager Configuration Web site, click **Downloads**.

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

To download Symantec Event Agent Installer for Linux, click **Symantec Event Agent 4.7.1 Installer for Linux®**.

This option downloads a file that is named symevtagent_linux_r4.7.1.x.tar.gz file.

To download Symantec Event Agent Installer for Solaris, click **Symantec Event Agent 4.7.1 Installer for SolarisTM**.

This option downloads a file that is named symevtagent_solaris_r4.7.1.x.tar.gz file.

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

1. Login 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_r4.7.1*.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. Login 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_r4.7.1*.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_4.7.1*.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_4.7.1*.tar.gz
   ```

   ```
   tar -xvf symevtagent_solaris_4.7.1*.tar
   ```

   The first command unzips 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.

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 `install.exe` file is located and then run the following command:

  ```
  install.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. The agent.settings file is present in the Agents directory when the downloaded agent tar.gz file is extracted.Run the following command:

  ```
  run install.sh -silent
  ```

Sample installer.properties file

You can refer to this sample, while creating an `installer.properties` file.

# <date>

# Replay feature output

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

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

# Choose Install Folder

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

#Installation directory of the agent.

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

```
#SSIM Server Information

#Bootstrap server

IP=127.0.0.1

IP_CONNECT=1

#Install CA root certificates

#Third party certificates path information. Uncomment and provide a valid path
#if you want to install any third-party certificate.

#cacertspath="<PATH to Certificate1>,<PATH to Certificate2>..."

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

Issues

This chapter includes the following topics:

Known issues

The following are the known issues for the version 4.7.3 release of Information Manager:

- In the Information Manager console, when you select a local event archive from **Events > Local Event Archives**, the **Help** icon gets repositioned to the left side of the screen.
- When **Assign to least busy user** option is selected, the incidents generation rate is slightly slower than when the option is not selected. However, none of the incidents that are created when **Assign to least busy user** option is selected are lost. Symantec recommends you to use this option judiciously.
- Warning messages are not displayed when a lookup table that is associated with a **Lookup Table Update** rule is deleted. However, the corresponding warning message gets listed in the `simcm.log` file. The Rule gets deactivated but not reflected in the Information Manager console.
- Whenever the LDAP backup files are restored on a newly set Information Manager server, links of events associated with incidents that are generated before the LDAP restoration are broken. Symantec recommends performing the LDAP restore operation immediately after the Information Manager server is newly setup.
- If a Network File System (NFS) mounted directory is used for the LDAP and database backup through selective backup and restore, and if the NFS server

is not running during the selective restore or purge of those backup files, the system may fail to respond.

- If disk space is full in the /dbsesa partition, simdbmu service may stop and the user cannot log on to the Information Manager Web Configuration Interface.
- When you back up a role and then assign it to a user, after restoration of that role, the role is no longer associated with that user. The same is the case with groups.
- If you specify a custom path for backup file storage, then you must ensure that the db2admin user is given full permission and the sesuser is given read and execute permission.
- In case the folder path where Symantec Event Agent is installed has Double Byte Character Set (DBCS), the agent does not install properly. You must ensure that the folder path has ascii characters.
- When the schedule for an existing backup job is updated, a backup is triggered immediately in case the user updates the schedule with the date and time that is earlier than the current date and time.

Resolved issues

Symantec Security Information Manager (SSIM) 4.7.3 includes the following resolved issues:

- Accurate results are now displayed for an event query when the **Last 5 minutes** time filter is used.
- The **Restart** option is provided for agentmgmt.sh / agentmgmt.bat script. This option now lets agentmgmt.sh / agentmgmt.bat to restart Symantec Event Agent.
- When install.sh detects an already running agent, a command is now displayed that can be used to uninstall the already running agent.
- Agent failover functions smoothly even when there are a large number of agents in a system.
- Agent failover is not skipped if one of the servers in the specified sequence is recognized as erroneous.
- Agent failover to a server is successful even if agents are assigned with multiple IP addresses.
- SSIM Statistics Event erroneously displayed the product version as 1.0 for the agent status event. Now the appropriate product version is displayed.

- When reports are emailed, the report names that are in localized characters are now displayed appropriately.
- Visualizer now displays accurate Max Queue Size and Total Events in the table view.
- SESA certificate is used to sign and verify the archives. Previously there was an option to delete the SESA certificate which created an error during archive validation. This option is removed and the user cannot delete the SESA certificate.
- **Rotate data** option is now working for reports having TopN and TrendTopN queries.
- A user who has read-only access for the main Lookup Table cannot edit or delete the main Lookup Tables.
- The event archives purge only after the limit that is set in the storage rules is reached.
- Information Manager server now uses a new method to derive the queue size and thus the statistic information is accurately represented.
- Trending reports now displays the last day of the month.
- Agent Manager does not restart the agent erroneously after every 5 minutes in case **Bandwidth throttle** feature is used.

Third-party Legal Notices

This appendix includes the following topics:

Introduction

The Third-Party Legal Notices for the third-party software that are distributed, embedded, or bundled with the Symantec product can be accessed by clicking the Third-Party Legal Notices link from Help > About Symantec Security Information Manager.

In addition to this, the following are the Third-Party Legal Notices.

Third-party Legal Notices

Network Security Services Netscape Communications Corporation/the Initial Developer The Original Code is the Netscape security libraries. The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by the Initial Developer are Copyright (C) 1994-2000 the Initial Developer. All Rights Reserved.

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.

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 an 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