

Symantec™ Event Collector 4.3 for Symantec Endpoint Protection 11.0 Quick Reference

Symantec™ Event Collector for Symantec Endpoint Protection 11.0 Quick Reference

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.

Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support	4
Chapter 1	
Introducing Symantec Event Collector for Symantec Endpoint Protection 11.0	9
About this quick reference	10
Compatibility requirements for Symantec Endpoint Protection 11.0 Event Collector	10
System requirements for the Symantec Endpoint Protection 11.0 Event Collector computer	11
About the installation sequence for Symantec Endpoint Protection 11.0 Event Collector	11
Setting the SQL Server security mode to mixed authentication	13
Downloading database drivers	14
Installing database drivers on a remote computer	15
Installing database drivers on an Information Manager appliance	15
Creating read-only database users	16
Creating a read-only database user account for Microsoft SQL Server 2000	16
Creating a read-only database user account for Microsoft SQL Server 2005	17
Creating a read-only database user account for Microsoft SQL Server 2000 Desktop Engine (MSDE)	19
Creating a read-only database user account for Sybase	20
Configuring the SQL Server instance to listen on a non-dynamic port	21
Configuring an SSL connection for the Microsoft SQL Server 2005 JDBC driver 1.2	21
Importing sensor settings	23
About Symantec Endpoint Protection 11.0 logs	24
Installing Symantec Endpoint Protection 11.0 Event Collector queries on the Information Manager appliance	25
Adding Symantec Endpoint Protection 11.0 domain or group information to events	28
Sensor properties for Symantec Endpoint Protection 11.0 Event Collector	30

	Enabling Assets table population on Symantec Security Information Manager	31
	About Assets table population for Symantec Endpoint Protection 11.0 Event Collector	33
	Running LiveUpdate for collectors	34
Chapter 2	Implementation notes	39
	Product ID for Symantec Endpoint Protection 11.0 Event Collector	39
	Event example	39
	Schema packages	42
	Event mapping for Information Manager	43
Chapter 3	Event filtering and aggregation	47
	Event filtering and aggregation for Symantec Endpoint Protection 11.0 Event Collector	47

Introducing Symantec Event Collector for Symantec Endpoint Protection 11.0

This chapter includes the following topics:

- [About this quick reference](#)
- [Compatibility requirements for Symantec Endpoint Protection 11.0 Event Collector](#)
- [System requirements for the Symantec Endpoint Protection 11.0 Event Collector computer](#)
- [About the installation sequence for Symantec Endpoint Protection 11.0 Event Collector](#)
- [Setting the SQL Server security mode to mixed authentication](#)
- [Downloading database drivers](#)
- [Installing database drivers on a remote computer](#)
- [Installing database drivers on an Information Manager appliance](#)
- [Creating read-only database users](#)
- [Configuring the SQL Server instance to listen on a non-dynamic port](#)
- [Configuring an SSL connection for the Microsoft SQL Server 2005 JDBC driver 1.2](#)
- [Importing sensor settings](#)

- [About Symantec Endpoint Protection 11.0 logs](#)
- [Installing Symantec Endpoint Protection 11.0 Event Collector queries on the Information Manager appliance](#)
- [Adding Symantec Endpoint Protection 11.0 domain or group information to events](#)
- [Sensor properties for Symantec Endpoint Protection 11.0 Event Collector](#)
- [Enabling Assets table population on Symantec Security Information Manager](#)
- [Running LiveUpdate for collectors](#)

About this quick reference

This quick reference includes information that is specific to Symantec™ Event Collector for Symantec Endpoint Protection 11.0. General knowledge about installing and configuring collectors is assumed, as well as basic knowledge of Symantec Endpoint Protection 11.0.

For detailed information on how to install and configure event collectors, please see the *Symantec Event Collectors Integration Guide*.

For information on Symantec Endpoint Protection 11.0, see your product documentation.

Compatibility requirements for Symantec Endpoint Protection 11.0 Event Collector

The collector is compatible with Symantec Endpoint Protection 11.0.

The collector runs on the following operating systems:

- Microsoft Windows 2000 with Service Pack 4 or later
- Microsoft Windows Advanced Server 2000 with Service Pack 4 or later
- Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1 or later
- Microsoft Windows Server 2003 Standard Edition with Service Pack 1 or later
- Windows XP with Service Pack 2 or later
- Red Hat Enterprise Linux AS 3.0
- Red Hat Enterprise Linux AS 4.0

Note: You can install version 4.3 collectors on both 32-bit and 64-bit versions of Windows Server 2000/2003.

System requirements for the Symantec Endpoint Protection 11.0 Event Collector computer

Minimum system requirements for a remote collector installation are as follows:

- Intel Pentium-compatible 133-MHz processor (up to and including Xeon-class)
- 512 MB minimum, 1 GB of memory recommended for the Symantec Event Agent
- 35 MB of hard disk space for collector program files
- 95 MB of hard disk space to accommodate the Symantec Event Agent, the JRE, and the collector
- TCP/IP connection to a network from a static IP address

About the installation sequence for Symantec Endpoint Protection 11.0 Event Collector

The collector is preinstalled on the Information Manager 4.6 appliance. You can also install this collector on a remote computer or on an Information Manager 4.5 appliance.

Remote connections are not allowed with a Sybase database. If you use Symantec Endpoint Protection 11.0 with a Sybase database, you must install the collector on the same computer that runs the Sybase database. On-appliance installations are supported only if you use a Microsoft SQL Server database.

The collector installation sequence is as follows:

- Complete the preinstallation requirements.
For these procedures, see the *Symantec Event Collectors Integration Guide*.
- Configure Symantec Endpoint Protection 11.0 to work with the collector.
- Close the Symantec Security Information Manager Client console.
- Register the collector for all off-appliance collector installations.
If you use Information Manager 4.6, the collector is pre-registered. You do not have to register it.
For this procedure see the *Symantec Event Collectors Integration Guide*

- Install the Symantec Event Agent on the collector computer.
You must install the agent for all remote installations.
Symantec Event Agent 4.5.0 build 12 or later is required.
- Run LiveUpdate on earlier collectors.
If you install a 4.3 collector on a computer that has an earlier collector on it, you must first run LiveUpdate on all components of the earlier version of the collector. You must update the earlier collector before you install the 4.3 collector.
See [“Running LiveUpdate for collectors”](#) on page 34.
- Install the collector component.
The collector is preinstalled on the Information Manager 4.6 appliance. If you want to use the collector on a remote computer, you must install it on the remote computer.
You can install the collector on the Information Manager 4.5 appliance. However, you must first apply Information Manager 4.5.1 with Maintenance Release 1 (or later) upgrade package on the appliance.
If you use Symantec Endpoint Protection 11.0 on the appliance, you must use a Microsoft SQL Server database and not a Sybase database.
For procedures on how to install the collector on a remote computer or on an appliance, see the *Symantec Event Collectors Integration Guide*.
- Symantec Endpoint Protection 11.0 can use a Microsoft SQL Server database or a Sybase database. If you use a Microsoft SQL Server database, you must make sure that the database installation is set to mixed authentication mode if you use a Microsoft SQL Server database with Symantec Endpoint Protection 11.0.
See [“Setting the SQL Server security mode to mixed authentication”](#) on page 13.
- Download and extract the required database driver.
Symantec Endpoint Protection 11.0 can use a Microsoft SQL Server database or a Sybase database to collect events.
If you use Microsoft SQL Server, the Microsoft SQL Server JDBC database driver is preinstalled on Information Manager 4.6.
You must install the database driver on the collector computer for all remote installations.
See [“Downloading database drivers”](#) on page 14.
- Create a read-only database user account.
See [“Creating read-only database users”](#) on page 16.
- Configure the SQL Server instance to listen on a non-dynamic port, optional.
See [“Configuring the SQL Server instance to listen on a non-dynamic port”](#) on page 21.

- Install the queries.
See [“Installing Symantec Endpoint Protection 11.0 Event Collector queries on the Information Manager appliance”](#) on page 25.
- Add DOMAIN or GROUP information to events, optional.
See [“Adding Symantec Endpoint Protection 11.0 domain or group information to events”](#) on page 28.
- Configure the sensor.
See [“Sensor properties for Symantec Endpoint Protection 11.0 Event Collector”](#) on page 30.
- Import the sensor settings.
If you use an alternate database, you can import the sensor settings with the configuration that is supplied.
See [“Importing sensor settings”](#) on page 23.
- Configure an SSL connection for the Microsoft SQL Server 2005 JDBC driver 1.2
See [“Configuring an SSL connection for the Microsoft SQL Server 2005 JDBC driver 1.2”](#) on page 21.
- Enable Assets Table population.
See [“Enabling Assets table population on Symantec Security Information Manager”](#) on page 31.
- Run LiveUpdate.
See [“Running LiveUpdate for collectors”](#) on page 34.

For all procedures that are not covered in the quick reference, see the *Symantec Event Collectors Integration Guide*.

Setting the SQL Server security mode to mixed authentication

If you use a Microsoft SQL Server database, you must make sure that the database security mode is set to mixed authentication mode. The security mode is selected when SQL Server is installed. You can change the security mode at any time.

Symantec Endpoint Protection 11.0 can use a Microsoft SQL Server database or a Sybase database.

To set the SQL Server security mode to mixed authentication

- 1 From the Start menu, click **Programs > Microsoft SQL Server > SQL Enterprise Manager**.

With SQL Server 2000, you choose SQL Enterprise Manager. With SQL Server 2005, you choose Microsoft SQL Server Management Studio.

- 2 Click the appropriate server.
- 3 From the Tools menu, click **SQL Server Configuration Properties**, and then click **Security**.
- 4 Under Authentication, click **SQL Server and Windows**.
- 5 Click **OK**, and then click **Close**.

Downloading database drivers

Some database collector installations require that you download and install a database driver on the target computer. The target computer can be the Information Manager appliance or a separate computer.

See [“Installing database drivers on a remote computer”](#) on page 15.

See [“Installing database drivers on an Information Manager appliance”](#) on page 15.

Note: Two versions of the Microsoft SQL Server JDBC database driver are available: a Windows version, and a UNIX version. If you run the collector on a computer that runs Microsoft Windows, you must download the Microsoft Windows version. If you run the collector on a computer that runs Linux or Solaris, you must download the UNIX version.

To download a database driver to the target computer

- 1 If you are installing the collector on the Information Manager appliance, log in to the SSIM client computer.

If you are installing the collector on a separate computer, log in to that separate computer.

- 2 Create a directory to store the contents of the database driver archive file.

An example directory is as follows: DBdrivers

- 3 Download the required database driver into the directory that you created in step 2, as follows:

- For the Microsoft SQL Server 2005 JDBC Driver 1.2, go to the following URL:

www.microsoft.com/downloads

The Microsoft SQL Server 2005 JDBC driver is compatible with both Microsoft SQL Server 2000 and Microsoft SQL Server 2005.

- For the Sybase JDBC driver, go to the following URL:
http://download.sybase.com/pub/jConnect/jConnect-6_05.zip
The Sybase driver is compatible with both UNIX and Windows operating systems.

Installing database drivers on a remote computer

You must install database drivers for all remote installations.

Before you install a database driver, you must download the driver to a remote computer.

See “[Downloading database drivers](#)” on page 14.

To install a database driver on a remote computer

- 1 On the remote computer, navigate to the directory to which you downloaded the database driver.

See “[Downloading database drivers](#)” on page 14.

- 2 Use the appropriate tool for the archive format to unpack the archive.

For a .zip file, use WinZIP or a similar utility.

For a UNIX tar.gz file, at the command prompt, type the following command:

```
tar zxvf file_name.tar.gz
```

When you download the Sybase JDBC driver, the driver is located in the jConnect-6_0\classes\ subdirectory. The driver file name is jconn3.jar.

Installing database drivers on an Information Manager appliance

If you install a collector that reads from a database on an Information Manager appliance, you may need to install a database driver on the Information Manager appliance.

To install a database driver on an Information Manager appliance

- 1 On the Information Manager appliance, log in as root.
- 2 To create a directory to store the contents of the JDBC driver archive file, at a command prompt, type the following command:

```
mkdir dbdrivers
```

- 3 To transfer the tar.gz file to the Information Manager appliance, use an SFTP client such as WinSCP to place the tar.gz in the directory that you created in step 2.

Before you install a database driver on an Information Manager appliance, you must download the driver to the SSIM Client computer.

See [“Downloading database drivers”](#) on page 14.

- 4 To extract the tar file, at the command prompt, type the following command:

```
tar -zxvf file_name.tar.gz
```

- 5 To change the owner of the driver files to the user sesuser and the group ses, at the command prompt, type the following command:

```
chown -R sesuser.ses /dbdrivers/*
```

Creating read-only database users

In order for the collector to query the point product, you must set up a read-only database user account with access to the point product's database. You can use an existing database account, or you can create an account specifically for the collector.

See [“Creating a read-only database user account for Microsoft SQL Server 2000”](#) on page 16.

See [“Creating a read-only database user account for Microsoft SQL Server 2005”](#) on page 17.

See [“Creating a read-only database user account for Microsoft SQL Server 2000 Desktop Engine \(MSDE\)”](#) on page 19.

See [“Creating a read-only database user account for Sybase”](#) on page 20.

Creating a read-only database user account for Microsoft SQL Server 2000

Collectors that use a database sensor require that you create a read-only database user account so that the collector can query for events.

See [“Creating a read-only database user account for Microsoft SQL Server 2005”](#) on page 17.

See [“Creating a read-only database user account for Microsoft SQL Server 2000 Desktop Engine \(MSDE\)”](#) on page 19.

To create a read-only database user account for Microsoft SQL Server 2000

- 1 In the SQL Server Enterprise Manager window, in the left pane, expand **Console Root > Microsoft SQL Servers > SQL Server Group**.
- 2 Click the appropriate server host name or click **local**, and then click **(Windows NT) > Security**.
- 3 Right-click **Logins**, and then click **New Login**.
- 4 In the SQL Server Login Properties - New Login dialog box, on the General tab, in the Name box, type the name of the read-only logon account.
- 5 Click **SQL Server Authentication**.
- 6 In the SQL Server Authentication Password box, type a password.
- 7 In the Database list, select the database name.
- 8 In the Language list, click **<Default>**.
- 9 On the Database Access tab, select the database name.
- 10 Under Permit in Database Role, click **db_datareader**.
This role gives the user read-only data access to the database.
The role of public is always selected and cannot be cleared.
- 11 Click **OK**.
- 12 Confirm the password for the user that you created, and then click **OK**.
- 13 Close the SQL Server Enterprise Manager window.

Creating a read-only database user account for Microsoft SQL Server 2005

Collectors that use a database sensor require that you create a read-only database user account so that the collector can query for events.

See [“Creating a read-only database user account for Microsoft SQL Server 2000”](#) on page 16.

See [“Creating a read-only database user account for Microsoft SQL Server 2000 Desktop Engine \(MSDE\)”](#) on page 19.

To create a read-only database user account for Microsoft SQL Server 2005

- 1 Start Microsoft SQL Management Studio.
- 2 In the Connect to Server window, in the Server name box, select the SQL Server 2005 computer on which the database is installed.
- 3 In the Authentication box, click **SQL Server Authentication**.
- 4 In the Login box, type a user name that has permissions to create new accounts.
- 5 In the Password box, type the password for the user name.
- 6 Click **Connect**.
- 7 On the SQL Server Management Studio window, in the Object Explorer pane, right-click **Security**, and then click **New > Login**.
- 8 In the Login-New dialog box, perform the following tasks in the order in which they appear:
 - In the Select a page pane, click **General**.
 - In the right pane, in the Login name box, type a logon name for the new user.
 - Check **SQL Server authentication**, type a password for the user, and then confirm the password.
 - Uncheck **User must change password at next login**.
 - In the Default database box, select the database to be read by this user.
- 9 In the Login-New dialog box, in the Select a page pane, click **Server Roles**.
- 10 In the right pane, click **public**.
- 11 In the Login-New dialog box, in the Select a page pane, click **User Mapping**.
- 12 In the right pane, under Users mapped to this login, make sure that you have selected the database to read.
- 13 Under Database role membership for the database, click **db_datareader**.

This role gives the user read-only data access to the database. The role of public is always selected and cannot be cleared.
- 14 Click **OK**.

Creating a read-only database user account for Microsoft SQL Server 2000 Desktop Engine (MSDE)

Collectors that use a database sensor require that you create a read-only database user account so that the collector can query for events.

To create a read-only database user account for Microsoft SQL Server 2000 Desktop Engine (MSDE)

- 1 From the Start menu, select **Programs > Accessories > Command Prompt**.
- 2 Navigate to the directory that contains the OSQLEXE file.

The default directory location for this file is C:\Program Files\Microsoft SQL Server\80\Tools\Binn.

- 3 To log in as the system administrator user, type the following command:

```
osql -U sa
```

- 4 At the Password prompt, type the system administrator password.
- 5 At the command prompt, type the following commands:

```
EXEC sp_addlogin 'account_name', 'password', 'database_name'
```

```
USE database_name
```

```
EXEC sp_grantdbaccess 'account_name'
```

```
EXEC sp_addrolemember 'db_datareader', 'account_name'
```

```
go
```

- 6 At the prompt, type the following command:

```
quit
```

The following is an example list of the commands that must be executed. The confirmation message shows that a new logon was created, granted access to the database, and assigned to the db_datareader role:

```
D:\>osql -U sa Password:
1> EXEC sp_addlogin 'readonly', 'x$256wr', 'BVInternetSecuritySQL'
2> USE BVInternetSecuritySQL
3> EXEC sp_grantdbaccess 'readonly'
4> EXEC sp_addrolemember 'db_datareader', 'readonly'
5> go
New login created.
Granted database access to 'readonly'.
'readonly' added to role 'db_datareader'.
1> quit
```

Creating a read-only database user account for Sybase

To create a read-only database user account for Sybase

- 1 Start the Interactive SQL program.
On Windows, this program is named dbisqlc.exe.
- 2 Select **Supply User ID and password**, specify a DBA user name and password, and then click **OK**.
- 3 In the SQL Statements window, type the following command:

```
GRANT CONNECT TO "read_only_user_name" IDENTIFIED BY "password"
```

- 4 Click **Execute**.
- 5 In the SQL Statements window, type the following command:

```
GRANT SELECT ON "DBA"."view_name" TO "read_only_user_name" FROM "DBA"
```
- 6 Click **Execute**.
- 7 Repeat steps 5 and 6 for the following views:

V_AGENT_BEHAVIOR_LOG	V_SERVER_ADMIN_LOG
V_AGENT_PACKET_LOG	V_SERVER_SYSTEM_LOG
V_AGENT_SECURITY_LOG	V_LAN_DEVICE_DETECTED
V_AGENT_TRAFFIC_LOG	V_SERVER_CLIENT_LOG
V_AGENT_SYSTEM_LOG	V_SERVER_ENFORCER_LOG
V_ENFORCER_CLIENT_LOG	V_SERVER_POLICY_LOG
V_ENFORCER_SYSTEM_LOG	V_ALERTS
V_ENFORCER_TRAFFIC_LOG	

- 8 In the SQL Statements window, type the following commands:

```
GRANT GROUP to DBA  
  
go  
  
GRANT MEMBERSHIP IN GROUP "DBA" TO "read_only_user_name"
```

- 9 Click **Execute**.

Collectors that use a database sensor require that you create a read-only database user account so that the collector can query for events.

Configuring the SQL Server instance to listen on a non-dynamic port

You must configure the SQL Server instance to listen to network requests. The SQL Server must listen on a non-dynamic port.

To configure the SQL Server instance to listen to network requests on a non-dynamic port

- 1 Start SQL Server Configuration Manager.
- 2 In the left pane, expand SQL Server 2005 Network Configuration.
- 3 Right-click **Protocols for *instance_name***.
- 4 Make sure that the following fields are set as follows:
 - In TCP/IP Properties, on the IP Address tab, make sure that Active and Enabled are both set to Yes.
 - Make sure that TCP Dynamic Ports is blank for the IP address that the collector connects to.
 - Make sure that TCP Port contains the value 1433 for the IP Address that the collector connects to.

Configuring an SSL connection for the Microsoft SQL Server 2005 JDBC driver 1.2

If you use Microsoft SQL Server 2005 database with the Microsoft SQL Server 2005 JDBC driver 1.2, you can configure an SSL connection.

Note: Microsoft SQL Server 2005 JDBC driver 1.1 or earlier does not support SSL.

In order to configure an SSL, you must complete the following procedures:

- Configure SSL for an SQL Server.
See [“To configure SSL for the SQL Server”](#) on page 21.
- Configure the sensor properties for an encrypted protocol.
See [“To configure the sensor properties for an encrypted protocol”](#) on page 22.

To configure SSL for the SQL Server

- 1 Start SQL Server Configuration Manager.
- 2 Expand SQL Server Network Configuration, right-click the protocols for the server that you want, and then click **Properties**.

- 3 On the Certificate tab, select the certificate that you want to use to protect your connection.
Self-signed certificates are supported but not recommended because they do not provide adequate security.
- 4 On the Flags tab, view or specify the protocol encryption option.
The logon packet is always encrypted.
- 5 Set the ForceEncryption option to Yes.
ForceEncryption encrypts all client/server communication and clients that cannot support encryption are denied access.
- 6 Restart the SQL Server.

To configure the sensor properties for an encrypted protocol

- 1 In the Information Manager console, in the left pane, click **System**.
- 2 Select the Product Configurations tab, and then expand the tree until you see the collector name.
- 3 In the left pane, select the appropriate configuration.
- 4 In the right pane, on the sensor tab, under the list of sensors, click the sensor.
- 5 In the Database URL field, add the following property string at the end of the URL:

```
;encrypt=true
```

For example,

```
jdbc:sqlserver://192.168.19.40:1433;DatabaseName=SOPHOS3;encrypt=true
```

- 6 If you are using a self-signed certificate, add the following property string at the end of the URL:

```
;trustServerCertificate=true
```

For example,

```
jdbc:sqlserver://192.168.19.40:1433;DatabaseName=SOPHOS3;encrypt=true;  
trustServerCertificate=true
```

- 7 Click **Save**.
- 8 In the left pane, right-click the appropriate configuration, and then click **Distribute**.

- 9 When you are prompted to distribute the configuration, click **Yes**.
- 10 In the Configuration Viewer window, click **Close**.

Importing sensor settings

Symantec Endpoint Protection 11.0 can use a Microsoft SQL Server database or a Sybase database. If you are using a Microsoft SQL database, the default sensor properties are compatible.

Remote connections are not allowed with a Sybase database. If you use Symantec Endpoint Protection 11.0 with a Sybase database, you must install the collector on the same computer that runs the Sybase database. On-appliance installations are supported only if you use a Microsoft SQL Server database.

If you are using a Sybase database, you must complete the following procedures to import sensor settings:

- Stop the Symantec Event Agent.
See [“To start and stop the Symantec Event Agent service on Windows”](#) on page 23.
See [“To start and stop the Symantec Event Agent daemon on UNIX”](#) on page 24.
- Replace the Microsoft SQL Server-compatible sensor configuration with a Sybase-compatible sensor configuration.
See [“To replace the Microsoft SQL Server-compatible sensor configuration with a Sybase-compatible sensor configuration”](#) on page 24.
- Import the sensor settings.
See [“To import sensor settings”](#) on page 24.
- Restart the Symantec Event Agent.
See [“To start and stop the Symantec Event Agent service on Windows”](#) on page 23.
See [“To start and stop the Symantec Event Agent daemon on UNIX”](#) on page 24.

To start and stop the Symantec Event Agent service on Windows

- 1 On the computer on which you installed the Symantec Event Agent, on the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, click **Administrative Tools**.
- 3 In the Administrative Tools window, click **Services**.
- 4 In the Services dialog box, right-click **SESA AgentStart Service**.
- 5 Select one of the following:
 - **Start**

- **Stop**

To start and stop the Symantec Event Agent daemon on UNIX

- 1 On the computer on which you installed the Symantec Event Agent, become superuser.
- 2 At the command prompt, do one of the following:
 - To start the Symantec Event Agent daemon, type the following command:
`service sesagentd start`
 - To stop the Symantec Event Agent daemon, type the following command:
`service sesagentd stop`

To replace the Microsoft SQL Server-compatible sensor configuration with a Sybase-compatible sensor configuration

- ◆ From the collector installation package, copy the config.xml file that is located in the utils\SybaseMode directory to the collector installation directory.

On Windows, the default collector directory is C:\Program Files\Symantec\Event Agent\collectors\symcep

On UNIX, the default collector directory is /Symantec/Agent/collectors/symcep

To import sensor settings

- 1 In the Information Manager console, in the left pane, click **System**.
- 2 Select the **Product Configurations** tab, and then expand the tree until you see the collector name.
- 3 In the middle pane, select the appropriate configuration.
- 4 In the right pane, on the sensor tab, click **Import configuration from XML file**.
- 5 In the Import Configuration From File window that appears, specify the XML file that you want to import into the collector.

The sensor settings file is located in the utils\SybaseMode subdirectory of your collector package.

The sensor settings file is named DBSensorConfigForSEPwithSybase.xml

About Symantec Endpoint Protection 11.0 logs

The collector collects only those Symantec Endpoint Protection 11.0 events that are written to one of the following tables or views:

Table 1-1 Symantec Endpoint Protection 11.0 logs

Log	View from which the log is captured
AgentBehavior Logs	V_AGENT_BEHAVIOR_LOG
AgentPacket Logs	V_AGENT_PACKET_LOG
AgentSecurity Logs	V_AGENT_SECURITY_LOG
AgentTraffic Logs	V_AGENT_TRAFFIC_LOG
AgentSystem Logs	V_AGENT_SYSTEM_LOG
EnforcerClient Logs	V_ENFORCER_CLIENT_LOG
EnforcerSystem Logs	V_ENFORCER_SYSTEM_LOG
EnforcerTraffic Logs	V_ENFORCER_TRAFFIC_LOG
ServerAdmin Logs	V_SERVER_ADMIN_LOG
ServerSystem Logs	V_SERVER_SYSTEM_LOG
LanDeviceDetected Logs	V_LAN_DEVICE_DETECTED
ServerClient Logs	V_SERVER_CLIENT_LOG
ServerEnforcer Logs	V_SERVER_ENFORCER_LOG
ServerPolicy Logs	V_SERVER_POLICY_LOG
Alerts Logs	V_ALERTS

All events captured by these tables and views are sent to Information Manager unless filters are enabled.

Installing Symantec Endpoint Protection 11.0 Event Collector queries on the Information Manager appliance

The collector package includes several queries. You can import these queries into the Information Manager appliance to provide detailed reporting on Symantec Endpoint Protection 11.0 events. These queries are provided as templates, and may be customized as needed.

Note: These queries are included on the Information Manager 4.6 appliance. You must complete this procedure only for Symantec Security Information Manager 4.5.

Most of the queries work off of a 24-hour time frame. To make these queries work, you can set up a scheduled timer that is set to run once every 24 hours. If you want to schedule your collector to run more than once every 24 hours, you must change the time parameters of these queries.

The queries are listed in the System Events query group, in the Events page.

The collector includes the following queries:

- Action Details Last 24 Hrs
- Action Summary Event Count Last 24 Hrs
- Action Summary Last 24 Hours
- Blocked Enforcer Traffic Details Last 24 Hrs
- Blocked Enforcer Traffic Summary Last 24 Hrs
- Top 25 Hosts With Host Integrity Failed Last 24 Hrs
- Top 25 Virus Types Details Last Hrs
- Top 25 Virus Types Summary Last 24 Hrs
- All Security Risk Details Last 24 Hrs
- All Virus Event Details Last 24 Hrs
- Top 10 Security Risks Cleaned Last 24 Hrs
- Top 10 Security Risks Last 24 Hrs
- Top 10 Security Risks Quarantined Last 24 Hrs
- Top 10 Security Risks Uncorrected Last 24 Hrs
- Top 10 Virus Last 24 Hrs
- Top 10 Virus Quarantined Last 24 Hrs
- Top 10 Virus Uncorrected Last 24 Hrs
- Denied Connections Last 24 Hrs
- Firewall Events Per Hour During the Day
- Top 10 Denied Inbound Traffic by Source Address Last 24 Hrs
- Top 10 Denied Inbound Traffic by Source Port Last 24 Hrs
- Top 10 Denied Outbound Traffic by Source Address Last 24 Hrs

- Top 10 Denied Outbound Traffic by Source Port Last 24 Hrs
- Top 5 Targets for Dropped or Denied Firewall Events over Week
- Network Intrusion Activity Last 24 Hrs
- Top 10 Destination IPs for NIDS events Last 24 Hrs
- Top 10 Destination Ports for NIDS events Last 24 Hrs
- Top 10 Symantec Event Codes for NIDS Events Over a Day
- Top 10 Vendor Codes for NIDS Events Over a Day

To install the queries on the Information Manager appliance

- 1 If you have an Information Manager client open, close it.
- 2 To upload the queries to the appliance, you must do the following tasks in the order shown:
 - In the collector installation directory, navigate to the query .tar file at the following location:
utils/QueryPackage/symcepqueries.tar.gz
 - Use a secure file transfer protocol such as SFTP or SCP to transfer the query .tar file to the Information Manager appliance.
- 3 Connect to the Information Manager appliance through an SSH client or log in to the appliance locally.

You must use an account with administrative privileges.

- 4 On the Information Manager appliance, at a Linux prompt, navigate to the .tar file that you uploaded in step 2.
- 5 To decompress and extract the tar file, type the following command:

```
tar zxvf symcepqueries.tar.gz
```

- 6 When the files are extracted, type the following command:

```
sh installqueries.sh
```

- 7 When you are prompted for the Directory Administrator name, enter the Information Manager administrator name.

The default Information Manager administrator name is administrator.

- 8 To restart the event service, type the following command:

```
service sesevents restart
```

- 9 To see the new queries, open the Information Manager client.

If the Information Manager client is already open, close it, and then reopen it.

The queries are listed under System Queries, Product Queries, Symantec Endpoint Protection.

Adding Symantec Endpoint Protection 11.0 domain or group information to events

You can add Symantec Endpoint Protection 11.0 domain or client group information to events by populating the `org_unit_list.txt` file. The collector populates the `org_unit` field with the contents of the `org_unit_list.txt` file. The `raw_event` value that is sent to Information Manager remains the unaltered, pre-plugin event.

An example of the the domain and client group information that will be added to the events is as follows:

```
|org_unit|ou=grp1| or |org_unit|ou=dom1|
```

An example of an `org_unit_list.txt` file is as follows:

```
dom1,ou=dom1  
grp1,ou=grp1  
corpdm,ou=Corporate  
salesgrp,ou=SalesOrg
```

Note: The Organizational Unit that you specify in the `org_unit_list.txt` file must exist for Symantec Security Information Manager. At least one Role with permissions to the Organization Unit must also exist.

See the *Symantec Security Information Manager Administrator's Guide* for instructions on how to add and configure Organizational Units and Roles.

If the `org_unit_list.txt` file is blank, the `org_unit` field is populated with the default value.

Domain and Group values are parsed from the `DOMAIN_ID` and `GROUP_ID` fields, respectively.

You must place the `org_unit_list.txt` file in the following directory:

...\`Symantec\Event Agent\collectors\`

You must enter Organizational Unit values with the format of "ou=", as shown above.

An example of an original raw event is as follows:

```
TIME_STAMP|1197642298000|DOMAIN_ID|dom1|SITE_ID|Site_CARRICKClay|
SERVER_ID|carrick\issedcarrick|EVENT_ID|9|HOST_NAME_SC|CARRICK|
USER_NAME|Administrator|DOMAIN_NAME|WORKGROUP
```

An example of the original raw event with appended domain or group information is as follows:

```
TIME_STAMP|1197642298000|DOMAIN_ID|dom1|SITE_ID|Site_CARRICKClay|
SERVER_ID|carrick\issedcarrick|EVENT_ID|9|HOST_NAME_SC|CARRICK|
USER_NAME|Administrator|DOMAIN_NAME|WORKGROUP|org_unit|ou=dom1|
```

To add domain or group information to events

- 1 Navigate to the `utils` directory of the installation package.
- 2 Copy the `sample_org_unit_list.txt` file to the following directory on the collector computer:

...\`Symantec\Event Agent\collectors\sample_org_unit_list.txt`

- 3 Rename

```
sample_org_unit_list.txt
```

to

```
org_unit_list.txt
```

- 4 Add domain or group information as shown in the following examples:

- If Client A has a domain dom1 and wants to have an Organizational Unit that corresponds to this same value, add the following to the org_unit_list.txt file:

```
dom1,ou=dom1
```

- If the Client has a group name grp1 and wants to have an Organizational Unit that corresponds to this same value, add the following to the org_unit_list.txt file:

```
grp1,ou=grp1
```

5 Save the org_unit_list.txt file.

Sensor properties for Symantec Endpoint Protection 11.0 Event Collector

Table 1-2 Database sensor properties

Sensor property	Description
JDBC Drivers Directory	<p>/opt/Symantec/simserver/collectors/drivers/mysql-connector-java-5.0.7</p> <ul style="list-style-type: none"> ■ If you use a Microsoft SQL Server database, specify the path where the Microsoft SQL Server JDBC driver is installed. If you install the collector on the Information Manager 4.6 appliance, this directory is as follows: /opt/Symantec/simserver/collectors/drivers/mssqljdbc_2005/enu If you install the collector on a Windows computer, the default directory is as follows: C:\Program Files\Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.2\enu ■ If you use a Sybase database, specify the path where the Sybase JDBC driver is installed. If you install the collector on the Information Manager 4.6 appliance, this directory is as follows: /opt/Symantec/simserver/collectors/drivers/jConnect-6_0 If you install the collector on a Windows computer, the default directory is as follows: C:\your_download_directory\sybase-jdbcdrivers\jConnect-6_05\jConnect-6_0\classes

Table 1-2 Database sensor properties (*continued*)

Sensor property	Description
Database URL	<p>The default database URL is as follows:</p> <ul style="list-style-type: none"> ■ If you use a Microsoft SQL Server database, the database URL is as follows: jdbc:sqlserver://*host_name*:1433;DatabaseName=sem5 ■ If you use a Sybase database, the database URL is as follows: jdbc:sybase:Tds:localhost:2638 <p>The database URL includes the following sections:</p> <ul style="list-style-type: none"> ■ JDBC driver information This section provides information on the type of JDBC driver that is used. ■ Host name If the collector database runs on a different computer than the collector, change localhost (or hostname) to the IP address or host name of the collector database computer. ■ TCP port If the TCP port on the collector database computer was changed, change this value to the new value. ■ Database name If you use a Microsoft SQL Server database, the default database is named sem5.
User Name	<p>Specify the read-only database user account name for the Symantec Endpoint Protection 11.0 database.</p> <p>This account must use SQL Server authentication, not Windows authentication.</p>
Password	<p>Specify the password for the database user account name for the Symantec Endpoint Protection 11.0 database.</p>
Start Reading From	<p>Specify from where to start reading the database upon restart of the collector as follows:</p> <ul style="list-style-type: none"> ■ BEGINNING Specifies that the database is read from the beginning. BEGINNING is the default position. ■ END Specifies that the database is read from the end. Only events that are written to the database after the collector starts are read.

Enabling Assets table population on Symantec Security Information Manager

The Assets table provides a centralized list of network assets that Information Manager can use for event correlation and rules processing. You can identify the Confidentiality, Integrity, and Availability (CIA) values for each asset; the

applicable policies; the ports that are potentially vulnerable; and the specific vulnerabilities of each asset. You can also associate the host name of an asset with the IP address, as well as with the operating system, the operating system version, and the distinguished name for each system.

If you use Information Manager 4.5, you must edit the `Asset_Detector.cfg` file to add or remove collectors.

If you use Information Manager 4.5, you must first apply Information Manager 4.5 with Maintenance Release 2.

See [“To enable Assets table population with Information Manager 4.5”](#) on page 32.

If you use Information Manager 4.6, you can use the Information Manager console to add or remove collectors.

See [“To enable Assets table population with Information Manager 4.6”](#) on page 33.

The Asset detector discovers assets through the `destination_ip` field. If the `destination_ip` is not available, the Asset detector uses the `machine_ip` field.

Information Manager creates new assets in the following ways:

- If an asset does not exist in the Assets table, Information Manager creates a new asset. The network to which the asset belongs must not be locked (the network may be updated).
- If an asset already exists in the Assets table (as defined by the IP address), it is automatically updated.

For more information on the Assets table, see the *Symantec Security Information Manager Administrator's User Guide*.

To enable Assets table population with Information Manager 4.5

- 1 Use a secure shell client, such as `putty`, to connect to the IP address of the Information Manager appliance, and then log in as `db2admin`.
- 2 At the command prompt, type the following command:

```
su -
```
- 3 Navigate to the following directory:
`/opt/Symantec/simserver/simcm/monitors/`
- 4 Use a text editor, such as `vi`, to open and edit the `Asset_Detector.cfg` file.

- 5 To enable Assets table population, add the following line to the Asset_Detector.cfg file:

```
<property name="product_id" value="3165" type="java.lang.Integer"
Description=""/>
```

The product_id of the collector is 3165. The Description is any descriptive name for the collector.

- 6 To disable Assets table population for the collector, delete the corresponding line in the Asset_Detector.cfg file.

Do not repeat configurations for the same collector. The .cfg file includes a predefined list of enabled default collectors. From the list, you can disable (remove the line) or enable (leave the line in), as necessary.

To enable Assets table population with Information Manager 4.6

- 1 In the Information Manager console, in the left pane, click **Rules**.
- 2 In the tree in the middle pane, expand **Monitors > System Monitors > Asset Detector**.
- 3 From the Properties tab, to the right of the product grid, click the ellipses (the three dots).
- 4 In the Property Editor dialog, add or remove collectors.

About Assets table population for Symantec Endpoint Protection 11.0 Event Collector

Assets are auto-populated based only on Symantec Endpoint Protection 11.0 events that fall into the following classes:

- POLICY_COMP_EVENT_CLASS_ID = 1931000;
- VULN_EVENT_CLASS_ID = 1081000

Most events are from the LAN_DEVICE_DETECTED table and AgentSecurity view.

Events with the following Event Type ID from Symantec Endpoint Protection 11.0 populate the Assets table:

- 1932000 - Compliance Check
- 1082000 Vulnerability Detected

The following table shows the Assets table fields that the collector sends to Information Manager to populate the Assets table. If an asset already exists in the Assets table (as defined by the IP address), Information Manager updates it with these fields.

Table 1-3 Assets table fields

Collector Information Manager field	Assets table field
IP Destination Address	IP Address
Destination Host Name	Host Name
Host OS (if available)	OS Name (maximum 32 characters)
Host OS version	OS Version (maximum 20 characters)
Host MAC	MAC Address
Organization unit	Org_unit

Running LiveUpdate for collectors

You can run LiveUpdate to receive collector updates such as support for new events and query updates.

Warning: The collector is compatible with both MS SQL Server databases and Sybase databases. By default, the collector is set up to use an MS SQL Server database. If you use the collector with a Sybase database, running LiveUpdate will revert the configuration back to the MS SQL Server drivers. You must repeat the procedure that imports the alternate sensor settings.

See [“Importing sensor settings”](#) on page 23.

If you install a collector on Information Manager 4.5, you must complete the following procedures in the order presented:

- Run LiveUpdate for collectors added to the Information Manager 4.5 appliance. See [“To run LiveUpdate for collectors added to the Information Manager 4.5 appliance”](#) on page 35.
- Verify that LiveUpdate ran successfully on Information Manager 4.5. See [“To verify that LiveUpdate ran successfully on Information Manager 4.5”](#) on page 36.

If you install a collector on Information Manager 4.6, or if you use a collector that is preinstalled on Information Manager 4.6, you must complete the following procedures in the order presented:

- Use the Administrator Web page to run LiveUpdate.
- Use the Administrator Web page to verify that LiveUpdate ran successfully.

See “[To run LiveUpdate from the Administrator Web page](#)” on page 35.

If you installed the collector on a separate computer, you must complete the following tasks in the order presented:

- Run LiveUpdate for a collector installed on a separate computer.
See “[To run LiveUpdate for a collector installed on a separate computer](#)” on page 36.
- Verify that LiveUpdate ran successfully for a collector installed on a separate computer.
See “[To verify that LiveUpdate ran successfully for a collector installed on a separate computer](#)” on page 37.

For information about running LiveUpdate on internal LiveUpdate servers, see the *Symantec LiveUpdate Administrator User's Guide*.

To run LiveUpdate from the Administrator Web page

- 1 From a Web browser, navigate to the Information Manager Administrator Web page, and then log in with administrator credentials.
- 2 From the list on the left, click **LiveUpdate**.
- 3 In the list of products, to select the items to update, in the corresponding check box, check **Update**.

At the bottom of the page, you can also click **Check All**.
- 4 At the bottom of the page, click **Update**.

If LiveUpdate runs successfully, the status column in the Summary page displays Success.
- 5 To troubleshoot a problem with LiveUpdate, under Session Log, click **View Log File**.

To run LiveUpdate for collectors added to the Information Manager 4.5 appliance

- 1 Connect to the Information Manager 4.5 appliance, and log in as root.
- 2 Navigate to the collectors directory.

The default directory is `/opt/Symantec/sesa/Agent/collectors/`
- 3 At the command prompt, type the following command:


```
sh ./runliveupdate.sh
```
- 4 To stop the Symantec Event Agent, type the following command:


```
service sesagentd stop
```

- 5 To change the ownership of the updated collector files, type the following command:

```
chown -R sesuser.ses *
```

- 6 Navigate to the Symantec Event Agent directory.
The default directory is /opt/Symantec/sesa/Agent/

- 7 To restart the Symantec Event Agent, type the following command:

```
service sesagentd start
```

To verify that LiveUpdate ran successfully on Information Manager 4.5

- 1 Connect to the Information Manager 4.5 appliance, and log in as root.
- 2 Navigate to the collectors subdirectory of the Symantec Event Agent directory.

The default directory is as follows:

```
/opt/Symantec/sesa/Agent/collectors/
```

- 3 Verify that a file named LiveUpdate-Collector.txt exists.

This text file shows the date of the last LiveUpdate and contains information about any defects that were addressed and any enhancements that were added.

- 4 Navigate to the LiveUpdate directory.

The default directory is as follows:

```
/opt/Symantec/LiveUpdate
```

- 5 To view the last 100 lines of the liveupdt.log file, type the following command:

```
tail -100 liveupdt.log | more
```

The first part of the log is in text format; the second part of the log repeats the information in XML format.

If LiveUpdate was unsuccessful, a status message that notes the failure appears at the end of the log file.

For example, Status = Failed (return code - 2001).

To run LiveUpdate for a collector installed on a separate computer

- 1 On the collector computer, navigate to the collector directory as follows:

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

`/opt/Symantec/sesa/Agent/collectors/`

2 At a command prompt, do one of following tasks:

- On Windows, type the following command:

`runliveupdate.bat`

- On UNIX, as the root user, type the following command:

`runliveupdate.sh`

To verify that LiveUpdate ran successfully for a collector installed on a separate computer

1 On the collector computer, navigate to the collector directory as follows:

- On Windows, the default directory is as follows:

`C:\Program Files\Symantec\sesa\Event Agent\collectors\`

- On UNIX, the default directory is as follows:

`/opt/Symantec/sesa/Agent/collectors/`

2 Verify that a file named LiveUpdate-Collector.txt exists.

This text file shows the date of the last LiveUpdate and contains information about any defects that were addressed and any enhancements that were added.

3 Navigate to the LiveUpdate directory as follows:

- On Windows, the default LiveUpdate directory is as follows:

`C:\Documents and Settings\All Users\Application Data\Symantec\Java
LiveUpdate`

- On UNIX, the default LiveUpdate directory is as follows:

`/opt/Symantec/LiveUpdate`

4 To view the liveupdt.log file, do one of the following tasks:

- On Windows, use a text editor such as Notepad to view the liveupdt.log file.

- On UNIX, to view the last 100 lines of the liveupdt.log file, type the following command:

`tail -100 liveupdt.log | more`

The first part of the log is in text format; the second part of the log repeats the information in XML format.

If LiveUpdate was unsuccessful, a status message that notes the failure appears at the end of the log file.

For example, Status = Failed (return code - 2001).

Implementation notes

This chapter includes the following topics:

- [Product ID for Symantec Endpoint Protection 11.0 Event Collector](#)
- [Event example](#)
- [Schema packages](#)
- [Event mapping for Information Manager](#)

Product ID for Symantec Endpoint Protection 11.0 Event Collector

The product ID of the collector is 3165.

Event example

The following are example events:

Agent Behavior Log

```
||EVENT_ID|501|EVENT_TIME|1164985804796|DOMAIN_ID|default|SITE_ID|
Site Ferd|SERVER_ID|carrick|GROUP_ID|global/clientpeeps|SEVERITY_AB|
15|HOST_NAME|charlton|ACTION_AB|3|TEST_MODE|1|DESCRIPTION|
OS Protection is ready|VAPI_NAME|System|RULE_ID|ff7589|RULE_NAME|
Built-in rule|CALLER_PROCESS_NAME_AB|SysPlant|PARAMETER|
c:\someapplication|ALERT_AB|221|USER_NAME|None|DOMAIN_NAME|None|
TIME_STAMP|1164967908625|
```

Agent Packet Log

```
TIME_STAMP|1164979988640|EVENT_ID|401|DOMAIN_ID|default|SITE_ID|
Site Ferd|SERVER_ID|carrick|GROUP_ID|global/clientpeeps|EVENT_TIME|
```

```
1164997174562|HOST_NAME|psv|LOCAL_HOST_IP|180502473|REMOTE_HOST_IP|  
180502335|REMOTE_HOST_NAME|everton|LOCAL_PORT|24567|REMOTE_PORT|  
44562|TRAFFIC_DIRECTION|1|BLOCKED|0|APP_NAME|C:\textpad.exe|  
ALERT_AP|0|
```

Agent Security Log

```
TIME_STAMP|1165229951234|EVENT_ID|209|DOMAIN_ID|default|SITE_ID|  
Site Ferd|SERVER_ID|carrick|GROUP_ID|global/clientpeeps|EVENT_TIME|  
1165247801796|SEVERITY|11|HOST_NAME|charlton|LOCAL_HOST_IP|  
180502334|REMOTE_HOST_IP|180502352|REMOTE_HOST_NAME|null|  
TRAFFIC_DIRECTION|1|NETWORK_PROTOCOL|2|HACK_TYPE|3|REPETITION_AS|  
23|APP_NAME|C:\textpad.exe|EVENT_DESC|Host Integrity check failed  
Requirement: "AntiVirus Auto-protect check" passed Requirement:  
"AntiVirus enforcement - Symantec" failed|LOCAL_HOST_MAC|  
000874EA7AD6|REMOTE_HOST_MAC|000874EB9020|LOCATION_NAME|  
SSIM Dev Env->Quarantine|USER_NAME|Administrator|DOMAIN_NAME|  
Workgroup|
```

Agent Traffic Log

```
TIME_STAMP|1186749351250|EVENT_ID|302|DOMAIN_ID|  
default|SITE_ID|Site Ferd|SERVER_ID|carrick|GROUP_ID|  
global/clientpeeps|EVENT_TIME|1186749161765|SEVERITY|10|HOST_NAME|  
FERDINAND|LOCAL_HOST_IP|3232281343|REMOTE_HOST_IP|3232281099|  
REMOTE_HOST_NAME|null|NETWORK_PROTOCOL|3|LOCAL_PORT|137|REMOTE_PORT|  
137|TRAFFIC_DIRECTION|1|REPETITION|6|APP_NAME|null|BLOCKED|0|  
RULE_ID|B49D5EC60AC23F610044F3AA98A1239A|RULE_NAME|Block Local File  
Sharing|ALERT_AT|0|LOCAL_HOST_MAC|FFFFFFFFFFFFFF|REMOTE_HOST_MAC|  
00112548CE1B|LOCATION_NAME|Office|USER_NAME|Administrator|  
DOMAIN_NAME|FERDINAND
```

AGENT System LOG

```
TIME_STAMP|1165229951234|EVENT_ID|302449166|DOMAIN_ID|default|  
SITE_ID|Site Ferd|SERVER_ID|carrick|GROUP_ID|global/clientpeeps|  
EVENT_TIME|1164985804796|SEVERITY_ASY|1|HOST_NAME|charlton|  
EVENT_SOURCE|Smc|EVENT_DESC|Location has been changed to Office|
```

ENFORCER CLIENT LOG

```
|TIME_STAMP|1166204122796|DOMAIN_ID|default|SITE_ID|Site Ferd|  
ENFORCER_ID_EC|carrick|EVENT_ID|0|EVENT_TIME|1166097209000|  
ENFORCER_TYPE|0|REMOTE_HOST|10.32.100.100|ACTION_EC|Authenticated|  
PERIOD|0|EVENT_DESC_EC|Query|Client has been authenticated by 3rd  
party server 10.32.6.232|REMOTE_HOST_MAC|00-06-5B-EE-25-4D|
```

ENFORCER SYSTEM LOG

```
|TIME_STAMP|1166204122796|SITE_ID|Site Ferd|ENFORCER_ID_ES|  
carrick|EVENT_ID|514|EVENT_TIME|1166097209000|ENFORCER_TYPE|0|  
SEVERITY_ES|2|EVENT_DESC_ESQuery|Service Stopped|
```

ENFORCER TRAFFIC LOG

```
|TIME_STAMP|1166204122796|DOMAIN_ID|default|SITE_ID|Site Ferd|  
ENFORCER_ID_ET|carrick|EVENT_ID|17|EVENT_TIME|1166097209000|  
ENFORCER_TYPE|0|LOCAL_HOST_IP|169871080|REMOTE_HOST_IP|169895012|  
NETWORK_PROTOCOL|4|LOCAL_PORT|138|REMOTE_PORT|122|  
TRAFFIC_DIRECTION_ETQuery|1|BLOCKED|0|TOTAL_BYTES|726|REPETITION|  
3|ALERT|0|
```

SERVER ADMIN LOG

```
|TIME_STAMP|1166204122796|DOMAIN_ID|Default|SITE_ID|Site Ferd|  
SERVER_ID|CARRICK|SEVERITY_SA|800|ADMIN_NAME_SAQUERY|  
administrator|EVENT_ID|4099|EVENT_DESC|null|
```

SERVER SYSTEM LOG

```
|TIME_STAMP|1166204122796|DOMAIN_ID|Default|SITE_ID|Site Ferd|  
SERVER_ID|CARRICK|SEVERITY_SS|800|EVENT_ID|267|EVENT_DESC|  
Agent Sweeping Started|
```

LAN DEVICE DETECTED LOG

```
|TIME_STAMP|1166204122796|MAC_ADDRESS|00-23-e4-d5-73-35|  
IP_ADDRESS_LDD|180502355|DEVICE_DETECTED_TIME|1167246894156|  
DELETED|0|
```

SERVER_CLIENT_LOG

```
|TIME_STAMP|1166204122796|DOMAIN_ID|Default|SITE_ID|Site Ferd|  
SERVER_ID|CARRICK|EVENT_ID|8|HOST_NAME_SC|ClientXP|USER_NAME|  
QaUser|DOMAIN_NAME|Locally|
```

SERVER_ENFORCER_LOG

```
|TIME_STAMP|1166002571000|SITE_ID|Site Ferd|SERVER_ID|CARRICK|  
ENFORCER_ID_SE|somename|EVENT_ID_SE|9|
```

SERVER_POLICY_LOG

```
|TIME_STAMP|1166204122796|DOMAIN_ID|Default|SITE_ID|Site Ferd|  
SERVER_ID|CARRICK|ADMIN_ID|admin|EVENT_ID|0|EVENT_DESC_SP|  
Add a Host Integrity Policy [NOTEPAD] at [Office]|
```

```
ALERT LOG
IDX|EB5F4C180AC23F6100FAE0D9D273AD56|ALERT_IDX|1|SOURCE|
Real Time Scan|VIRUSNAME_IDX|23F04D680AC23F610027441C55EFB3D1|
NOOFVIRUSES|1|FILEPATH|D:/DUMBVIRS/PAM/UNREF/DSCE2100.COM|
DESCRIPTION|""|ACTUALACTION_IDX|4|REQUESTEDACTION_IDX|5|
ALERTDATETIME|2007-08-07 18:26:28.0|USER_NAME|Administrator|
SOURCE_COMPUTER_NAME|null|SOURCE_COMPUTER_IP|0|TIME_STAMP|
1186515237609|SOURCE_COMPUTER_IP_TEXT|0.0.0.0|VIRUSNAME|
DSCE.2100|TYPE|0|VIRUSDEF|2007-08-07 rev. 003|SEQUENCE|71591|
DOMAIN_NAME|system|GROUP_NAME|Global\GroupContent|SERVER_NAME|
FERDINAND|SITE_NAME|Site FERDINAND|COMPUTER_DOMAIN_NAME|
WORKGROUP|COMPUTER_NAME|CARRICK|CURRENT_LOGIN_USER|
Administrator|CURRENT_LOGIN_DOMAIN|LocalComputer|IP_ADDR1_TEXT|
10.194.63.98|MAC_ADDR1|00-c0-9f-26-3d-ec|OS_LANG|9|DISK_TOTAL|
39991275520|MEMORY|2146942976|OPERATION_SYSTEM|
Windows Server 2003 family Standard Edition|SERVICE_PACK|null|
BIOS_VERSION|DELL - 1|AGENT_VERSION|11.0.723.926|AGENT_TYPE|
105|PROFILE_VERSION|5.0.0|STATUS|1|LAST_UPDATE_TIME|
1186593957484|INFECTED|1|WORSTINFECTION_IDX|0|LAST_VIRUS_TIME|
1186511212000|LAST_SCAN_TIME|1186532552000|LAST_DOWNLOAD_TIME|
0|CONTENT_UPDATE|1|PROFILE_SERIAL_NO|
86D9-08/07/2007 11:13:03 765|MAJOR_VERSION|11|LICENSE_STATUS|
0|LICENSE_EXPIRY|0
```

Schema packages

The collector uses the following schema packages:

- `symc_base_class`
- `symc_fw_conn_stats_class`
- `symc_firewall_network_class`
- `symc_network_class`
- `symc_host_intrusion_class`
- `symc_intrusion_class`
- `symc_network_intrusion_class`
- `symc_compliance_class`
- `symc_data_virus_incident_class`
- `symc_data_incident_class`

- symc_vuln_class

Event mapping for Information Manager

[Table 2-1](#) shows the Information Manager field name, the corresponding Symantec Endpoint Protection 11.0 field name, and how they are populated.

Table 2-1 Event mapping

Information Manager field name	Symantec Endpoint Protection 11.0 field name	Comment
Category ID	“Application” or “Security”	
Compliance Aspect ID	This field is populated for Host integrity Passed and Failed events	Possible values are as follows: <ul style="list-style-type: none"> ■ 1937124 – Process Active ■ 1937125 – Process Inactive ■ 1937126 – Generic Error
Compliance Found Value	Policy check Obtained from the EVENT_DESC field	
Compliance Status ID	Information on whether the compliance passed or failed Based on the EVENT_ID field	Possible values are as follows: <ul style="list-style-type: none"> ■ 1937200 - Pass ■ 1937201 - Fail
Data Status	Computer status that is related to the virus that was captured (ACTUALACTION_IDX)	Possible values are as follows: <ul style="list-style-type: none"> ■ 117230 - Corrected ■ 117231 - Partially Corrected ■ 117232 - UnCorrected ■ 117233 - Infected ■ 117234 - Blocked ■ 117236 - Delayed ■ 117237 - Deleted ■ 117238 - Quarantined ■ 117239 - Unknown
Description	Description of the captured event For Alert messages, this field stores information on whether the Agent is a SNAC ONLY or SEP Agent	The main descriptive part of the event message is retained here

Table 2-1 Event mapping (*continued*)

Information Manager field name	Symantec Endpoint Protection 11.0 field name	Comment
Destination Host Name	Destination host name if it exists; otherwise the destination IP address (REMOTE_HOST_NAME)	
Event Count	REPETITION	Sometimes preceded by the phrase "Infc:"
Event Date	Date and Time of the Event (TIMESTAMP)	The event is captured in database format
Event Type ID	Event ID that is associated with each event which indicates whether the event is a firewall or IDS event	
Host MAC	MAC address of the client computer, if necessary	
Intrusion Action	Intrusion action attempted (ACTION) For some events only	Possible values are as follows: <ul style="list-style-type: none"> ■ 1037201 - Other ■ 1037202 - Unknown ■ 1037205 - Modify ■ 1037210 - Start ■ 1037212 - Stop ■ 1037217 - Crash
IP Destination Address	Destination IP address of the event (REMOTE_HOST_IP)	
IP Destination Port	Destination port of the event, if available (REMOTE_PORT)	
IP Source Address	Source IP address of the event (LOCAL_HOST_IP)	
IP Source Port	Source port of the event, if available (LOCAL_PORT)	
Network Protocol	Protocol that is associated with the event (NETWORK_PROTOCOL)	
Option 1	Vendor Code	

Table 2-1 Event mapping (*continued*)

Information Manager field name	Symantec Endpoint Protection 11.0 field name	Comment
Option 2	Profile version and Profile serial number For Alert Messages	
Option 4	DOMAIN and LOCATION information For Agent Type messages	
OS Domain	Computer domain name Populated from the COMPUTER_DOMAIN_NAME field For Alert messages only	
Point Product Version	SEP Agent version number for Alert messages For Alert messages	
SCS Client Group	SEP Client Group Name Populated from the GROUP_NAME field For Alert messages	
SCS Parent	Parent Server's Machine Name Populated from the SERVER_NAME field For Alert messages	
SCS Server Group	SEP Domain group (sav domain) Populated from the DOMAIN_NAME field For Alert messages	
Source Host Name	Source host name if it exists; otherwise, the source IP address (LOCAL_HOST_NAME)	

Table 2-1 Event mapping (*continued*)

Information Manager field name	Symantec Endpoint Protection 11.0 field name	Comment
Start Time	Last Scan Time Derived from the LAST_SCAN_TIME field For Alert messages	
Target Resource	The target of the intended event, if available For example, a URL, a user name, or a file server's IP address	
User Name	User name exists after the key phrase User: or at the end of the event (USER_NAME)	
Vendor Signature	Signature to identify and distinguish various SEP events (EVENT_ID)	
Virus Definitions	Virus Definitions at the point-in-time that is associated with the client in question Populated from the VIRUSDEF field	
Windows Domain Name	Current login domain name Populated from the CURRENT_LOGIN_DOMAIN field For Alert messages only	

Event filtering and aggregation

This chapter includes the following topics:

- [Event filtering and aggregation for Symantec Endpoint Protection 11.0 Event Collector](#)

Event filtering and aggregation for Symantec Endpoint Protection 11.0 Event Collector

Because of the role that intrusion-detection point products such as Symantec Endpoint Protection 11.0 play in defense in depth scenarios, aggregating events is not recommended. However, it is possible that systems on a network play a specific role in ensuring the security of an organization. This type of role may result in false positives from the device. For example, computers within the network that are responsible for assessing vulnerability risks may use techniques that cause intrusion-detection point products to report that the network is under attack. If you have this type of scenario, you may consider aggregating the events from that computer.

Filtering is not recommended beyond the filters that are provided with the collector. Aggregation is also not recommended. However, if information is not used to assess and track outbreaks, you can aggregate events which have a status of quarantined. This status is found in the Data Incident Class. The event field is called Data Status ID. The value for quarantined is 117230.

The filter for all TEST MODE events is enabled by default. All other filters are disabled by default.

[Table 3-1](#) shows the default filters included with the collector.

Table 3-1 Default filters

Filter Name	Criteria
Filter for all AgentBehavior Logs	Removes events where LogType equal to AgentBehavior This filter is disabled by default
Filter for all AgentPacket Logs	Removes events where LogType equal to AgentPacket This filter is disabled by default
Filter for all AgentSecurity Logs	Removes events where LogType equal to AgentSecurity This filter is disabled by default
Filter for all AgentTraffic Logs	Removes events where LogType equal to AgentTraffic This filter is disabled by default
Filter for all AgentSystem Logs	Removes events where LogType equal to AgentSystem This filter is disabled by default
Filter for all EnforcerClient Logs	Removes events where LogType equal to EnforcerClient This filter is disabled by default
Filter for all EnforcerSystem Logs	Removes events where LogType equal to EnforcerSystem This filter is disabled by default
Filter for all EnforcerTraffic Logs	Removes events where LogType equal to EnforcerTraffic This filter is disabled by default
Filter for all LanDeviceDetected Logs	Removes events where LogType equal to LanDeviceDetected This filter is disabled by default
Filter for all ServerAdmin Logs	Removes events where LogType equal to ServerAdmin This filter is disabled by default

Table 3-1 Default filters (*continued*)

Filter Name	Criteria
Filter for all ServerSystem Logs	Removes events where LogType equal to ServerSystem This filter is disabled by default
Filter for all ServerClient Logs	Removes events where LogType equal to ServerClient This filter is disabled by default
Filter for all ServerEnforcer Logs	Removes events where LogType equal to ServerEnforcer This filter is disabled by default
Filter for all ServerPolicy Logs	Removes events where LogType equal to ServerPolicy This filter is disabled by default
Filter for all AlertsQuery Logs	Removes events where LogType equal to AlertsQuery This filter is disabled by default
Filter for all Don't log broadcast and multicast Traffic Logs	Removes events where rule_name equal to 2E3231383000138101E606A968CB7F91:Don't log broadcast and multicast traffic This filter is disabled by default You can enable this filter if you would like not to see the traffic that is generated by the rule "Don't log broadcast and multicast traffic" in Information Manager
Filter for all TEST MODE events	Removes events where option6 equal to TEST MODE This filter is enabled by default
Filter for Details Pending Events	Removes events where flagfilter equal to "yes" This filter is enabled by default

