

Sophos Reporting Interface user guide

This guide provides information on how to install and use:

Sophos Reporting Interface

Sophos Reporting Log Writer

Product version: 5.0

Document date: December 2011



Contents

1 About this guide.....	3
2 What do I install?.....	4
3 What are the key steps?.....	5
4 Check the requirements.....	6
5 Install Sophos Reporting Interface	7
6 Configure Reporting Interface with Crystal Reports.....	8
7 Install Sophos Reporting Log Writer.....	9
8 Configure Log Writer.....	11
9 What information can be accessed?.....	14
10 Reporting Interface data sources.....	17
11 Log Writer data sources.....	22
12 Uninstall Sophos Reporting Log Writer.....	26
13 Uninstall Sophos Reporting Interface.....	27
14 Technical support.....	28
15 Legal notices.....	29

1 About this guide

This guide describes Sophos tools that enable you to use third-party reporting and log-monitoring software to generate reports from threat and event data in Sophos Enterprise Console. It is intended for use by system administrators and database administrators.

It is assumed that you are familiar with and already using Sophos Enterprise Console (SEC) version 5.0.

Sophos documentation is published at <http://www.sophos.com/support/docs/>.

2 What do I install?

You install Sophos Reporting Interface and (optionally) Sophos Reporting Log writer.

- **Sophos Reporting Interface** enables direct access to the Enterprise Console database and allows the use of third-party applications such as Crystal Reports and SQL Reporting Services to communicate with the SQL server directly. The Sophos Reporting Interface must be installed as an extension to the Enterprise Console database.
- **Sophos Reporting Log Writer** allows the use of third-party log-monitoring applications, for example Splunk, which retrieve data from plain text files rather than directly from a database. The Sophos Reporting Log Writer can be installed on a computer with a standalone installation of SEC, or on any computer that has access to the Enterprise Console database.

Note: You must install Sophos Reporting Interface before you install Sophos Reporting Log Writer.

Important: The Sophos Reporting Interface and the Sophos Reporting Log Writer make SEC data available to third-party applications. By installing either of these you assume the responsibility of the security of the data made available, which includes ensuring the data can only be accessed by authorized users.

3 What are the key steps?

You carry out these key steps:

1. Check the requirements.
2. Install Sophos Reporting Interface.
3. (Optional) Configure Reporting Interface with Crystal Reports.
4. Install Sophos Reporting Log Writer, if you want to use third-party log-monitoring applications such as Splunk.
5. (Optional) Configure Log Writer.

4 Check the requirements

You should check that you have:

- SEC 5.0 installed.
- A valid, complete backup of your database and Enterprise Console installation.
- The necessary administrator privileges to make changes to the Enterprise Console database during the Reporting Interface installation.
- .NET Framework 3.5 installed.
- Sufficient privileges to install a new service on the computer where Log Writer will be installed.

5 Install Sophos Reporting Interface

Note:

- The data retrieved by Reporting Interface may contain confidential information about your computers. You should restrict access to this information. We recommend that you enable encryption in SQL Server when you are using remote databases. For information about encryption for Microsoft SQL Server, see <http://technet.microsoft.com/en-us/library/bb510663.aspx>.
- In some system environments, additional queries made to the SEC database whilst accessing the Reporting Interface could impact the performance of other database operations such as Sophos Enterprise Console. There may be a noticeable decrease in performance of Enterprise Console during large transfers of data from the Reporting Interface.

Sophos Reporting Interface must be installed on the computer that has the Enterprise Console database installed.

To install Reporting Interface:

1. Ensure you have a valid, complete backup of your database and Enterprise Console installation.
2. Double-click on the Sophos Reporting Interface installer to extract the files to a folder.
3. Browse to the folder where you have extracted the files and locate the DB folder that has the batch file *InstallSophosReportingInterface*.

- If you are installing Reporting Interface on a server that uses the default SOPHOS instance selected during the SEC database installation, double-click the batch file. It requires no additional parameters.
- If you are installing Reporting Interface with a custom database configuration, you must run the batch file with additional parameters as follows:

```
InstallReportingInterface.bat [SERVER\INSTANCE] [DOMAIN] [LOGFILE]
```

This will update the relevant database.

The installation script will generate a log file *InstallSophosReportingInterface.log* in its working folder. This log file will show if the installation was successful or detail any errors that have occurred during the installation.

6 Configure Reporting Interface with Crystal Reports

You can configure Reporting Interface with Crystal Reports. We recommend using Crystal Reports version 2008 or later.

Note: The Crystal Reports Wizard will automatically link columns with identical names between views that have been included in a report. However, some of the connections must be removed as similarly named columns do not necessarily have identical values for a single log event.

For example, the **InsertedAt** column is present in every view which denotes when each entry was added to the database. However, a single event may have different **InsertedAt** times for its corresponding entries in each view. If the Crystal Reports Wizard automatically links these columns, the links must be removed to prevent missing data. For information on which data sources are linked, see [Which datasources are linked?](#) (page 15)

To create Reporting Interface connection with Crystal Reports:

1. Open Crystal Reports and create a new connection using **OLEDB (ADO)** and choose **Microsoft OLE DB Provider for SQL Server**.
2. Enter the connection information and complete the wizard.

Sophos Reporting Interface will now be listed in the available data sources. For information on how to generate custom reports, see the Crystal Reports documentation.

For a list of data sources that are available for Log Writer, see [Reporting Interface data sources](#) (page 17).

For more information and examples on using Crystal Reports to access data provided by the Sophos Reporting Interface, see the Sophos knowledge base article 112873 <http://www.sophos.com/support/knowledgebase/article/112873.html>.

7 Install Sophos Reporting Log Writer

You can install the Sophos Reporting Log Writer, after installing Sophos Reporting Interface.

Note: The data retrieved by Log Writer may contain confidential information about the computers managed by SEC. You should restrict access to this information. We recommend that the access permissions of the installation folder, data formatting files and log files are all restricted to an appropriate account. Also, since the data transferred from the Sophos Reporting Interface to the log files is unencrypted the log files should only be written to the local machine rather than transferring the data over an unencrypted network transport such as SAMBA/CIFS shares.

7.1 Recommendations

We recommend that the Log Writer is installed on the computer that has the management server installed. However, it can be installed on any server that has access to the Sophos Enterprise Console database.

By default, the Log Writer service will be installed under the LocalSystem account, which has full access privileges to the local server. We strongly recommend that you reassign the service to an account with lower access privileges after installation. If the service is installed to a computer other than the management server it will need to be run under a user account with the appropriate permissions to access the SEC database remotely. For this reason, the account should be mapped to a SQL login which has the SELECT and EXECUTE permissions granted within the Sophos LogWriter schema.

Note: Make sure the Log Writer computer and the database computer have their computer's location, time zone, and clock set correctly based on their location.

7.2 Installation

To install Log Writer:

1. Find the Log Writer installer (InstallLogWriter.msi) file that has been extracted.

If you want to generate a verbose log file during the installation of Log Writer use the following command: `msiexec /l*v logfile.txt /i "SophosReportingLogWriter.msi"`

The log file will be created in the folder in which the command was executed. If you do not want to generate a log file continue to next step.

2. Double-click on the InstallLogWriter.msi file.
3. In the **Sophos Reporting Log Writer Setup** dialog box, click **Next**.

A wizard guides you through installation.

4. When installation is complete, click **Finish**. If you have the **Show configuration file** check box selected, a window appears with the default configuration file, SophosLogWriterConfig.xml, highlighted.
 - If you want to use the default configuration that is provided with Log Writer, continue to the next step and start the Log Writer service. For information on default configuration, see [Default Log Writer configuration](#) (page 10).
 - To edit the Log Writer configuration file, see [Configure Log Writer](#) (page 11).
5. To start the Log Writer service:
 - a) Open **Control Panel** and double-click **Administrative Tools**.
 - b) In **Administrative Tools** window, double-click on **Services**.

The list of available services is displayed.
 - c) Select **Sophos Reporting Log Writer** and click **Start** to start the service.

Log Writer reads the configuration file when it is first started and requires a restart of the service for any configuration changes.

7.3 Default Log Writer configuration

The default configuration file contains two datafeeds. The first datafeed will write to a log file DefaultCommonEvents.log. It extracts common event data using the EventsCommonData data source. The second datafeed will write to a log file DefaultThreats.log. It extracts the threat event data using the ThreatEventData data source.

The default log file will be in the 'Log Files' folder using the default data formatting files in the 'Configuration Files' folder located in the Log Writer installation folder. Data for the last 7 days will be extracted when the service is started for the first time with the default configuration.

8 Configure Log Writer

The Configuration Files folder is located in the Log Writer's installation folder. The folder contains an example configuration file for each of the available data sources. You can customize them based on your requirements.

The configuration file is available at the following location by default:
C:\Program Files\Sophos\Reporting Interface\SophosLogWriterConfig.xml.

For a list of data sources that are available for Log Writer, see [Log Writer data sources](#) (page 22).

To edit the Log Writer configuration file:

1. Modify the connection settings <connectionString> element which determines how Log Writer contacts the Enterprise Console database:

In the default configuration file the <connectionString> element is commented out (surrounded by "<!--" and "-->" tags). If this element is commented out or not present in the configuration file then the service will attempt to find the appropriate settings by scanning the registry for a SEC management service connection string. However, if the Log Writer is installed on a different machine to the management service then a connection string must be specified.

For typical installations, only the database server name and instance must be modified. If you have a non- standard database setup, a description of how to edit connection parameters is available from the Microsoft website at the following location:

<http://msdn.microsoft.com/en-us/library/system.data.sqlclient.sqlconnection.connectionstring.aspx>

Note:

- If the <connectionString> element is present but specifies an incorrect or empty connection string (such as DataSource="") the service will fail to start and will not look for the registry value.
- If a connection to the database has been specified, a <noOfDays> element must be defined which determines how many days of historical data to retrieve.
- The <commandTimeout> element specifies the time SQL server must wait before a command execution times out. It is optional and if it is not specified the server will wait indefinitely.

```
<?xml version="1.0" encoding="utf-8" ?>
<SophosDatafeed xmlns=
"http://www.sophos.com/msys/LogWriterConfig.xsd">
  <connection>
    <connectionString>
      Integrated Security = SSPI;
      Persist Security Info = False;
      Initial Catalog = Sophos[SECVersion];
      Data Source = [SERVER]\[INSTANCE]
    </connectionString>
    <commandTimeout>[TIMEOUT IN SECONDS] </commandTimeout>
```

```

</connection>
<noOfDays> [AGE OF HISTORICAL DATA]</noOfDays>

```

2. Define custom datafeeds to extract information from the database. We recommend adding only one feed at a time as this helps in troubleshooting and reduces the load on the database. The datafeed definition is as follows:

Note:

- Each datafeed must specify a single <tick> and <logFile> element. They specify the frequency to check the database for new data and the location to save data.
- The <applyLogFormat> element takes a value of either true or false and specifies whether to prefix each line with the date and time the line was written to the log file. This can be useful if a third-party tool such as Splunk is used which automatically picks up the first date on each line of the log file. If it is not set then the log file date is not prefixed.
- The <file size> element limits the size of the current log file. The <no_of_files> element sets the number of backup log files that can be created before older files are deleted.

Example: If you have set the <file_size> element for 500KB and the <no_of_files> element to 2, the first time the log file reaches 500KB it is renamed to add a suffix ".1" and a new log file is created without a suffix to capture new logs. Once the new log file reaches 500KB, the previously suffixed ".1" file is renamed to ".2" and the file that now reached 500KB is suffixed with ".1". A new log file is created again without a suffix to capture new logs. The next time this happens, the file with ".2" suffixed is deleted and the file with ".1" suffixed is renamed so that it has a ".2" suffix.

- Each datafeed contains one or more <call> elements which are labelled with a unique callID attribute. The Log Writer keeps track of each call made by storing a timestamp for each call in a "[CallID].last" file. The callID must be unique.

```

<datafeeds>
<datafeed>
  <tick> [POLL TIME IN SECONDS] </tick>
  <applyLogFormat> TRUE </applyLogFormat>
  <logFile>
    <noOfFiles> [NUMBER OF BACKUP FILES] </noOfFiles>
    <fileSize> [MAX FILE SIZE KB/MB/GB] </fileSize>
    <outputLocataion> [LOG FILE LOCATION] </outputLocation>
    <outputFilename> [LOG FILE NAME] </outputFilename>
  </logFile>

  <call callID = "[UNIQUE CALL NAME]">
    <dataSource> [DATA SOURCE TO USE] </dataSource>
    <dataConfigurationLocation>[CALL DATA CONFIGFILE
LOCATION]</dataConfigurationLocation>
    <dataConfigurationFile>[CALL DATA CONFIG
FILENAME]</dataConfigurationFile>
  </call>

```

```

    ...
  </datafeed>
  ...
</datafeeds>
</SophosDatafeed>

```

- If you want to edit the data sources, you can edit the `<call>` element. It specifies the data source to extract data and associates it with a data formatting file that determines the columns of the available data which should be saved. The data formatting file can be constructed as an ordered list of required fields as follows:

Note:

- The *field name* attribute can use any name.
- The *link* attribute must use a valid Reporting Interface field for the data source.
- For *enabled* attribute, 0 indicates data will not be extracted and 1 indicates data will be extracted.

```

<?xml version="1.0" encoding="utf-8" ?>
<LogFile>
  <Events>
    <field name="[FIELDNAME]" link="[FIELDNAME]" enabled="1" />
    ...
  </Events>
</LogFile>

```

- Start the **Sophos Reporting Log Writer** service.

Note:

- You must restart the Log Writer service for any configuration changes.
- Before you start the Log Writer service with a new configuration, we recommend you stop the Sophos Management Service whilst the Log Writer initializes new datafeeds and downloads historical data from the database.

9 What information can be accessed?

Sophos Enterprise Console records logging information on:

- Computers
- Packages
- Groups
- Events
- Threats

9.1 Computers

Computers are the individual endpoints currently being monitored by Enterprise Console and are uniquely identified by their *ComputerID*. You can access computer's logging information using the following database views:

- **vComputerHostData** provides information on each computer monitored by SEC.
- **vPolicyComplianceData** lists which policies have been applied to each computer.

9.2 Groups

Groups are a logical grouping of computers made from within Enterprise Console and are uniquely identified by their *GroupID*. You can access groups logging information using the following database views:

- **vGroupPathAndNameData** provides a list of group paths.
- **vComputerGroupMapping** lists which computers belong in which groups.

9.3 Packages

Packages are particular versions of Sophos Anti-Virus that may be present on the network and are uniquely identified by their *PackageID*. You can access packages logging information using the following database views:

- **vPackageData** lists the versions of Sophos Anti-Virus currently running on the network.
- **vComputerPackageMapping** lists which package each computer currently has installed.

9.4 Events

Events are notifications of events that have occurred on endpoints and are uniquely identified jointly by their *EventID* and *EventTypeID*.

Events are classified by their type into different categories. **vEventsCommonData** provides basic information on all events that have occurred and includes an **EventTypeName** to denote which of the following views will contain additional category-specific information on the event:

- Application Control using **vEventsApplicationControlData**
- Data Control using **vEventsDataControlData**
- Device Control using **vEventsDeviceControlData**
- Firewall using **vEventsFirewallData**
- Tamper Protection using **vEventsTamperProtectionData**
- Web using **vEventsWebData**
- Threat actions using **vThreatEventData**

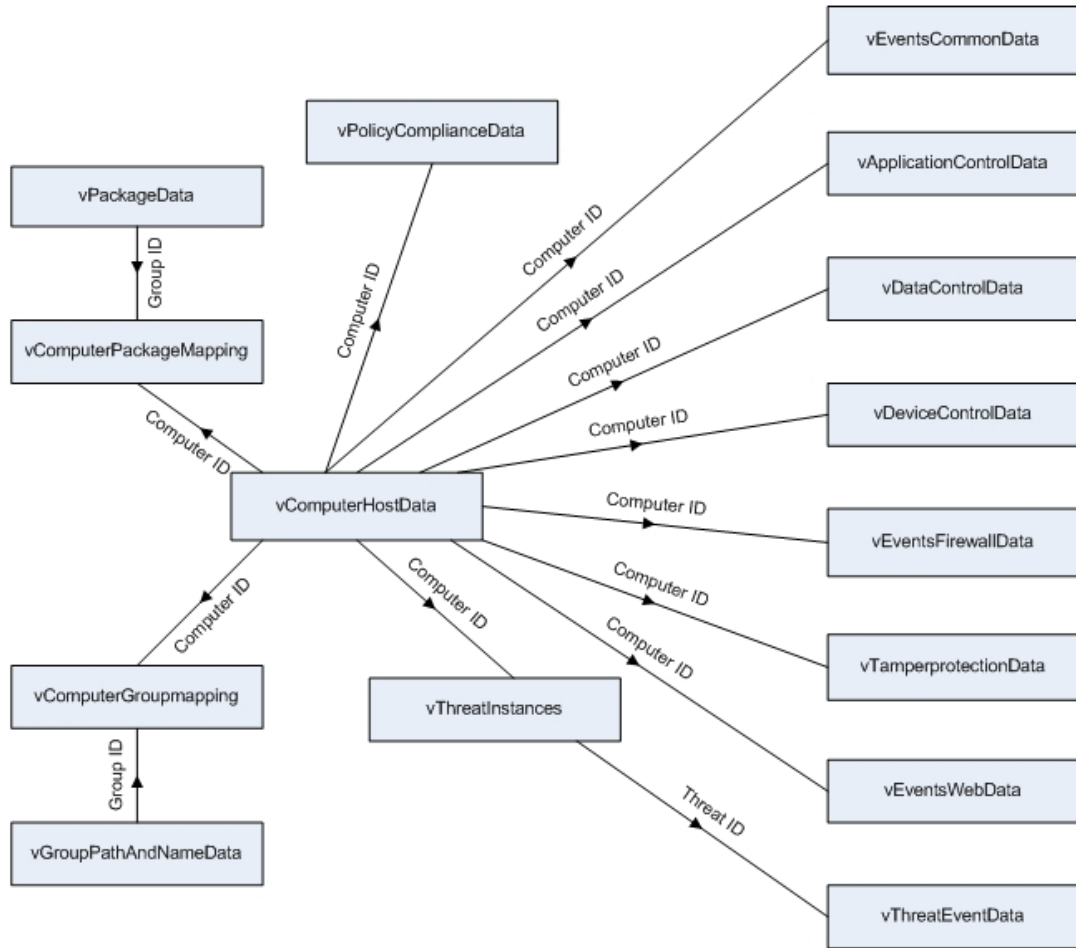
9.5 Threats

Threats are instances of malware that have been detected on endpoints and are uniquely identified by their *ThreatID*.

- **vThreatInstances** lists the threats that have been detected on each computer.
- **vThreatEventData** provides a list of actions that have been performed in response to threats detected on the network.

9.6 Which datasources are linked?

When merging data from multiple views, rows from each view that reference the same entity will need to be joined. This can be achieved by joining the rows that reference the same entity ID numbers. The following diagram shows which fields are responsible for joining each of the available views.



10 Reporting Interface data sources

The following data sources are available for Reporting Interface.

Note: Letter of the alphabet listed besides the data source is used in the table below to represent its availability for the data field.

- A. vComputerHostData
- B. vThreatInstances
- C. vEventsCommonData
- D. vEventsApplicationControlData
- E. vEventsDataControlData (extended in SEC 5.0)
- F. vEventsDeviceControlData
- G. vEventsFirewallData
- H. vEventsTamperProtectionData
- I. vEventsWebData (extended in SEC 5.0)
- J. vThreatEventData
- K. vComputerGroupMapping
- L. vGroupPathAndNameData
- M. vComputerPackageMapping
- N. vPackageData
- O. vPolicyComplianceData

The data fields available for each of these data sources are listed in the table below. All date-time columns are returned in UTC in the format "yyyy-mm-dd hh:mi:ss" (24 hours).

New Data fields included in version 5.0 are highlighted in bold.

Data field	Data type	Data source														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
EventID	integer			•	•	•	•	•	•	•	•					
ThreatID	integer		•								•					
ComputerID	integer	•	•	•	•	•	•	•	•	•		•		•		•
Name	nvarchar	•		•	•	•	•	•	•	•						
EventTime	datetime			•	•	•	•	•	•	•	•					

Data field	Data type	Data source														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
EventTypeID	integer			•	•	•	•	•	•	•						
EventTypeName	nvarchar			•	•	•	•	•	•	•						
ReportingName	nvarchar			•	•	•	•	•	•	•						
UserName	nvarchar			•	•	•	•	•	•	•	•					
ActionID	integer			•	•	•	•	•	•	•						
ActionName	nvarchar			•	•	•	•	•	•	•						
ScanTypeID	integer			•	•											
ScanTypeName	nvarchar			•	•											
SubTypeID	integer			•	•		•	•	•	•						
SubTypeName	nvarchar			•	•		•	•	•	•						
InsertedAt	datetime		•	•	•	•	•	•	•	•	•					
Domain	nvarchar	•														
IPAddress	nvarchar	•														
Description	nvarchar	•														
LastMessageReceived Time	datetime	•														
ThreatTypeID	integer		•													
ThreatTypeName	nvarchar		•													
ThreatSubTypeID	integer		•													
ThreatSubTypeName	nvarchar		•													
Priority	integer		•													
ThreatName	nvarchar		•													
FullFilePath	nvarchar		•													
FileVersion	nvarchar		•													
Checksum	nvarchar		•													
FirstDetectedAt	datetime		•													

Data field	Data type	Data source														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
RuleName	nvarchar					•										
TrueFileType	nvarchar					•										
DestinationPath	nvarchar					•										
DestinationTypeID	integer					•										
DestinationTypeName	nvarchar					•										
SourcePath	nvarchar					•										
FileName	nvarchar					•										
DestinationValue	nvarchar					•										
FileSize (New in version 5.0)	long					•										
DeviceTypeID	integer						•									
DeviceTypeName	nvarchar						•									
Model	nvarchar						•									
DeviceID	integer						•									
Role	nvarchar							•								
FileName	nvarchar							•								
FilePath	nvarchar							•								
FileVersion	nvarchar							•								
FileChecksum	nvarchar							•								
CommandLine	nvarchar							•								
Session	nvarchar							•								
Desktop	nvarchar							•								
Location	nvarchar							•								
ProtocolID	integer							•								
ProtocolText	nvarchar							•								
DirectionID	integer							•								

Data field	Data type	Data source														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
DirectionText	nvarchar							.								
LocalAddress	nvarchar							.								
RemoteAddress	nvarchar							.								
LocalPort	integer							.								
RemotePort	integer							.								
TargetTypeID	integer								.							
TargetTypeText	nvarchar								.							
Target	nvarchar								.							
RuleID	integer									.						
BlockedSite	nvarchar									.						
ReferringURL	nvarchar									.						
ReasonID (New in version 5.0)	integer									.						
ReasonName (New in version 5.0)	nvarchar									.						
CategoryID (New in version 5.0)	integer									.						
CategoryName (New in version 5.0)	nvarchar									.						
ActionTakenID	integer										.					
ActionTakenName	nvarchar										.					
ScannerTypeID	integer										.					
ScannerTypeName	nvarchar										.					
StatusID	integer										.					
StatusName	nvarchar										.					
GroupID	integer											.	.			
PathAndName	nvarchar												.			
Depth	integer												.			

Data field	Data type	Data source															
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
PackageID	integer														•	•	
Product	nvarchar															•	
SAVVersion	nvarchar															•	
EngineVersion	nvarchar															•	
VirusDataVersion	nvarchar															•	
ExpiryTime	datetime															•	
NotificationTime	datetime															•	
Expired	bit															•	
PolicyTypeID	integer																•
PolicyTypeName	nvarchar																•
ComplianceID	integer																•
ComplianceName	nvarchar																•

11 Log Writer data sources

The following data sources are available for Log Writer.

Note: Letter of the alphabet listed beside each data source is used in the table below to represent its availability for the data field.

A. EventsApplicationControlData

B. EventsCommonData

C. EventsDataControlData

D. EventsDeviceControlData (extended in SEC 5.0)

E. EventsFirewallData

F. EventsTamperProtectionData

G. EventsWebData (extended in SEC 5.0)

H. ThreatEventData

I. ThreatInstances

The data fields available for each of these data sources are listed in the table below. All date-time columns are returned in UTC in the format "yyyy-mm-dd hh:mi:ss" (24 hours).

New Data fields included in version 5.0 are highlighted in bold.

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
EventID	integer	•	•	•	•	•	•	•	•	
EventTime	datetime	•	•	•	•	•	•	•	•	
EventTypeID	integer	•	•	•	•	•	•	•		
EventTypeName	nvarchar	•	•	•	•	•	•	•		
SubTypeID	integer	•	•		•		•	•		
SubTypeName	nvarchar	•	•		•		•	•		
InsertedAt	datetime	•	•	•	•	•	•	•	•	•
UserName	nvarchar	•	•	•	•	•	•	•	•	
ComputerName	nvarchar	•	•	•	•	•	•	•	•	•
ComputerDomain	nvarchar	•	•	•	•	•	•	•	•	•

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
ComputerIPAddress	nvarchar	•	•	•	•	•	•	•	•	•
Name	nvarchar	•	•	•	•	•	•	•		
ReportingName	nvarchar	•	•	•	•	•	•	•		
ActionID	integer	•	•	•	•	•	•	•		
ActionName	nvarchar	•	•	•	•	•	•	•		
ScanTypeID	integer	•	•							
ScanTypeName	nvarchar	•	•							
RuleName	nvarchar			•						
TrueFileType	nvarchar			•						
DestinationPath	nvarchar			•						
DestinationTypeID	integer			•						
DestinationTypeName	nvarchar			•						
SourcePath	nvarchar			•						
FileName	nvarchar			•		•				
DestinationValue	nvarchar			•						
FileSize (New in version 5.0)	long			•						
DeviceTypeID	integer				•					
DeviceTypeName	nvarchar				•					
Model	nvarchar				•					
DeviceID	nvarchar				•					
Role	nvarchar					•				
FilePath	nvarchar					•				
FileVersion	nvarchar					•				•
FileChecksum	nvarchar					•				
CommandLine	nvarchar					•				

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
Session	nvarchar					•				
Desktop	nvarchar					•				
Location	nvarchar					•				
ProtocolID	integer					•				
ProtocolText	nvarchar					•				
DirectionID	integer					•				
DirectionText	nvarchar					•				
LocalAddress	nvarchar					•				
RemoteAddress	nvarchar					•				
LocalPort	integer					•				
RemotePort	integer					•				
Target	nvarchar						•			
TargetTypeID	integer						•			
TargetTypeText	nvarchar						•			
RuleID	nvarchar							•		
BlockedSite	nvarchar							•		
ReferringURL	nvarchar							•		
ReasonID (New in version 5.0)	integer							•		
ReasonName (New in version 5.0)	nvarchar							•		
CategoryID (New in version 5.0)	integer							•		
CategoryName (New in version 5.0)	nvarchar							•		
ActionTakenID	integer								•	
ActionTakenName	nvarchar								•	
ScannerTypeID	integer								•	

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
ScannerTypeName	nvarchar								•	
StatusID	integer								•	
StatusName	nvarchar								•	
ThreatID	integer									•
ThreatName	nvarchar								•	•
ThreatTypeID	integer								•	•
ThreatTypeName	nvarchar								•	•
ThreatSubTypeID	integer									•
ThreatSubTypeName	nvarchar									•
FullFilePath	nvarchar								•	•
Checksum	nvarchar									•
FirstDetectedAt	datetime									•
Priority	integer									•

12 Uninstall Sophos Reporting Log Writer

Note: During the uninstallation of Log Writer, the configuration file will also be deleted. We recommend you to take a backup of the configuration file if you plan to install Log Writer again.

To uninstall Log Writer:

1. Open **Control Panel > Add/Remove Programs**.
2. In the **Add/Remove Programs** dialog box, select **Sophos Reporting Log Writer** and click **Remove**.
3. In the **Confirm Uninstall** message box, click **Yes**.

A progress bar is displayed. Wait for uninstallation to complete.

13 Uninstall Sophos Reporting Interface

Note: We recommended you to take a full backup of the SEC database before and after the uninstallation process. Also, the SQL scripts must be verified by the database administrator to ensure the default values are appropriate for your setup.

To uninstall Reporting Interface:

- In the DB folder that has been extracted during installation, locate the batch file *UninstallSophosReportingInterface*.
 - If you are uninstalling Reporting Interface from a server that has the default SOPHOS instance selected during the SEC database installation, double-click the batch file. It requires no additional parameters.
 - If you are uninstalling Reporting Interface that has a custom database configuration, you must run the batch file with additional parameters as follows:

UninstallReportingInterface.bat [SERVER\INSTANCE] [DOMAIN] [LOGFILE]

14 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

15 Legal notices

Copyright © 2012 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.