SOPHOS

Security made simple.

Sophos Reporting Log Writer user guide

Sophos Enterprise Console 5.1 or later

Product version: 5.1
Document date: October 2015

Contents

1 About this guide

This guide describes Sophos Reporting Log Writer that enables you to use third-party 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 5.1 or later.

If you want to use third-party reporting applications, such as Crystal Reports or SQL Reporting Services, you can do so with Sophos Reporting Interface. For more information, see the *Sophos Reporting Interface user guide*.

Sophos documentation is published at http://www.sophos.com/en-us/support/documentation.aspx.

2 What is Sophos Reporting Log Writer

Sophos Reporting Log Writer is a specialized application which exports data for use by third-party log-monitoring applications, for example Splunk, which retrieve data from plain text files rather than directly from a database.

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.

Important: Sophos Reporting Log Writer makes Enterprise Console data available to third-party applications. By installing it 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 Install Sophos Reporting Log Writer

Note: The data retrieved by Log Writer may contain confidential information about the users and computers managed by SEC. You should manage 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.

3.1 Check the requirements

You should check that you have:

- .NET Framework 3.5 installed.
- Sufficient privileges to install a new service on the computer where Log Writer will be installed.

3.2 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. However, the account must have the Write permission to the log output folder (by default, C:\Program Files\Sophos\Reporting Interface\Log Files).

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.

3.3 Installation

3.3.1 Download the installer

This section assumes that you have a MySophos account and that you have associated your license credentials with it. If you need help, go to www.sophos.com/en-us/support/knowledgebase/111195.aspx

To download the installer:

1. Go to www.sophos.com/en-us/support/downloads.aspx.
2. Type your MySophos username and password.

   You see a web page that shows your licenses.

3. Under your license name, find the **Console** downloads. Download the Sophos Reporting Interface installer.

3.3.2 Install Log Writer

To install Log Writer:

1. Find the Sophos Reporting Interface installer that you downloaded earlier and double-click the installer.
2. Change the destination folder where the installation files are copied, if you want to, and click **Install**.

   The installation files are copied to the computer.

3. Find the installer **Sophos Reporting Log Writer.msi**. Do one of the following:
   - 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 "Sophos Reporting Log Writer.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, double-click the installer.

   The **Sophos Reporting Log Writer Setup** wizard starts and guides you through the installation.

4. When installation is complete, click **Finish**. If you have the **Show configuration file** check box selected, the default configuration file **SophosLogWriterConfig.xml** is displayed in Windows Explorer.
   - 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 7).
   - To edit the Log Writer configuration file, see Configure Log Writer (page 8).

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.

3.4 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.

4 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 11).

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 <fileSize> element limits the size of the current log file. The <noOfBackupFiles> element sets the number of back up log files that can be created before older files are deleted.

     Example: If you have set the <fileSize> element for 500KB and the <noOfBackupFiles> 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>
      <noOfBackupFiles>[NUMBER OF BACKUP FILES]</noOfBackupFiles>
      <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>
```

3. 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>
```

4. 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.

5 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 (added new data fields)

E. EventsFirewallData

F. EventsTamperProtectionData

G. EventsWebData (added new data fields)

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 that are available with SEC 5.0 or later versions 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	•	•	•	•	•	•	•	•	

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
ComputerName	nvarchar	•	•	•	•	•	•	•	•	•
ComputerDomain	nvarchar	•	•	•	•	•	•	•	•	•
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 (SEC 5.0 or later)	long			•						
DeviceTypeID	integer				•					
DeviceTypeName	nvarchar				•					
Model	nvarchar				•					

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
DeviceID	nvarchar				•					
Role	nvarchar					•				
FilePath	nvarchar					•				
FileVersion	nvarchar					•				•
FileChecksum	nvarchar					•				
CommandLine	nvarchar					•				
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							•		

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
BlockedSite	nvarchar							•		
ReferringURL	nvarchar							•		
ReasonID (SEC 5.0 or later)	integer							•		
ReasonName (SEC 5.0 or later)	nvarchar							•		
CategoryID (SEC 5.0 or later)	integer							•		
CategoryName (SEC 5.0 or later)	nvarchar							•		
ActionTakenID	integer								•	
ActionTakenName	nvarchar								•	
ScannerTypeID	integer								•	
ScannerTypeName	nvarchar								•	
StatusID	integer								•	
StatusName	nvarchar								•	
ThreatID	integer									•
ThreatName	nvarchar								•	•
ThreatTypeID	integer								•	•
ThreatTypeName	nvarchar								•	•
ThreatSubTypeID	integer									•
ThreatSubTypeName	nvarchar									•
FullFilePath	nvarchar								•	•
CheckSum	nvarchar									•

Data field	Data type	Data source								
		A	B	C	D	E	F	G	H	I
FirstDetectedAt	datetime									•
Priority	integer									•

6 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.

7 Technical support

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

- Visit the SophosTalk community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

8 Legal notices