SOPHOS

Security made simple.

Sophos Reporting Interface user guide

Product version: 5.2

Document date: January 2013

Contents

1 About this guide

This guide describes Sophos Reporting Interface that enables you to use third-party reporting 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 5.2.

Note: If you want to export data to third-party log-monitoring applications, for example Splunk, you can do so with Sophos Reporting Log Writer. For more information, see the *Sophos Reporting Log Writer user guide*.

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

2 What is Sophos Reporting Interface

Sophos Reporting Interface provides a means of generating detailed and custom-made reports about the endpoints that are managed by Sophos Enterprise Console.

Sophos Reporting Interface allows third-party applications, such as Crystal Reports and SQL Reporting Services to access data in the SQL server stored by Enterprise Console. The required database objects are installed as part of the Enterprise Console database installation.

3 About using Sophos Reporting Interface

Important: Sophos Reporting Interface makes Enterprise Console data available to third-party applications. The data may contain confidential information about your users and computers. By using Sophos Reporting Interface you assume the responsibility of the security of the data made available, which includes ensuring the data can only be accessed by authorized users.

Besides restricting access to the data retrieved by Reporting Interface, we also strongly recommend that you encrypt connections between any clients and the Enterprise Console database. For more information, see the SQL Server documentation:

- Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager), SQL Server 2012
- Encrypting Connections to SQL Server 2008 R2
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console, SQL Server 2005

Note:

- In some system environments, additional queries made to the Enterprise Console database whilst accessing the Reporting Interface could impact the performance of other database operations. There may be a noticeable decrease in performance of Enterprise Console during large transfers of data from the Reporting Interface.
- We recommend using numeric IDs instead of string values if you want to bind any external logic to the data retrieved by Reporting Interface. This will help to avoid potential compatibility issues should any string values change in a future release of Enterprise Console.

You can use Reporting Interface with third-party applications such as Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services, or Crystal Reports.

For an example on how to use Crystal Reports to access Reporting Interface, see Appendix: Configure Crystal Reports with Reporting Interface (page 15).

For shared information on using your own reporting tools, please refer to the Sophos Reporting Interface thread on SophosTalk.

4 What information can be accessed?

Sophos Enterprise Console records information on:

- Computers
- Packages
- Groups
- Events
- Threats

4.1 Computers

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

- **vComputerHostData** provides information on each computer monitored by Enterprise Console.
- **vPolicyComplianceData** lists which policies have been applied to each computer as well as the policy compliance status.

4.2 Groups

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

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

4.3 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 package information using the following database views:

- **vPackageData** lists the versions of Sophos Anti-Virus that are currently available or have been available in the past.
- **vComputerPackageMapping** lists which package each computer currently has installed.

4.4 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 Control using **vEventsWebData**
- Threat actions using **vThreatEventData**

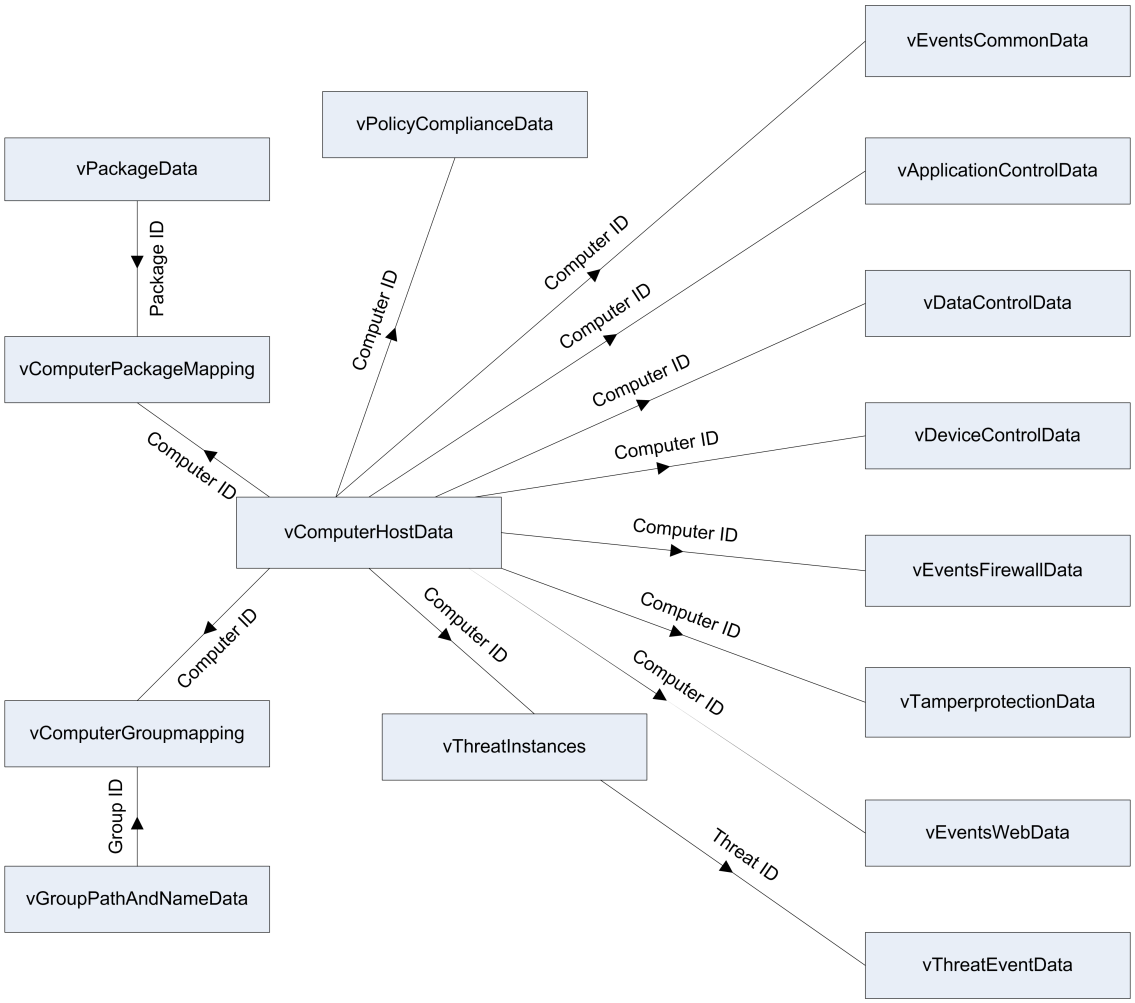
4.5 Threats

Threats are files or applications which have been identified as belonging to one of the alert item categories (Viruses/spyware, Suspicious behavior/files, Adware and PUA). They are uniquely identified by their *ThreatID*. You can access threat information using the following database views:

- **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.

4.6 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 to use for joining each of the available views.


vEventsCommonData
vPolicyComplianceData
vPackageData
vApplicationControlData
Package ID
Computer ID
Computer ID
vDataControlData
vComputerPackageMapping
Computer ID
Computer ID
vDeviceControlData
Computer ID
vComputerHostData
Computer ID
vEventsFirewallData
Computer ID
Computer ID
Computer ID
vTamperprotectionData
Computer ID
vComputerGroupmapping
vThreatInstances
Group ID
vEventsWebData
Threat ID
vGroupPathAndNameData
vThreatEventData

5 Reporting Interface data sources

The following data sources are available for Reporting Interface.

Note: Letter of the alphabet listed beside a data source is used to represent the data source in the matrix below.

A. vComputerHostData

B. vThreatInstances

C. vEventsCommonData

D. vEventsApplicationControlData

E. vEventsDataControlData

F. vEventsDeviceControlData

G. vEventsFirewallData

H. vEventsTamperProtectionData

I. vEventsWebData

J. vThreatEventData

K. vComputerGroupMapping

L. vGroupPathAndNameData

M. vComputerPackageMapping

N. vPackageData

O. vPolicyComplianceData

The following matrix shows which data fields are available in which data sources. All date-time columns are returned in UTC in the format "yyyy-mm-dd hh:mi:ss" (24 hours).

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	nvarchar	•														
DNSName	nvarchar	•														
OperatingSystemID	integer	•														
OperatingSystem Name	nvarchar	•														
ServicePack	nvarchar	•														
ThreatTypeID	integer		•													
ThreatTypeName	nvarchar		•													

Data field	Data type	Data source														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ThreatSubTypeID	integer		•													
ThreatSubTypeName	nvarchar		•													
Priority	integer		•													
ThreatName	nvarchar		•													
FullFilePath	nvarchar		•													
FileVersion	nvarchar		•													
CheckSum	nvarchar		•													
FirstDetectedAt	datetime		•													
RuleName	nvarchar					•										
TrueFileType	nvarchar					•										
DestinationPath	nvarchar					•										
DestinationTypeID	integer					•										
DestinationType Name	nvarchar					•										
SourcePath	nvarchar					•										
FileName	nvarchar					•										
DestinationValue	nvarchar					•										
FileSize	long					•										
DeviceTypeID	integer						•									
DeviceTypeName	nvarchar						•									
Model	nvarchar						•									
DeviceID	integer						•									

Data field	Data type	Data source													
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Role	nvarchar							•								
FileName	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							•								
TargetTypeID	integer								•							
TargetTypeText	nvarchar								•							
Target	nvarchar								•							
RuleID	integer									•						

Data field	Data type	Data source														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
BlockedSite	nvarchar									•						
ReferringURL	nvarchar									•						
ReasonID	integer									•						
ReasonName	nvarchar									•						
CategoryID	integer									•						
CategoryName	nvarchar									•						
ActionTakenID	integer										•					
ActionTakenName	nvarchar										•					
ScannerTypeID	integer										•					
ScannerTypeName	nvarchar										•					
StatusID	integer										•					
StatusName	nvarchar										•					
GroupID	integer											•	•			
PathAndName	nvarchar												•			
Depth	integer												•			
PackageID	integer													•	•	
Product	nvarchar														•	
SAVVersion	nvarchar														•	
EngineVersion	nvarchar														•	
VirusDataVersion	nvarchar														•	
ExpiryTime	datetime														•	

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

6 Appendix: Configure Crystal Reports with Reporting Interface

This example shows you how to use Crystal Reports version 2008 or later to access Reporting Interface.

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 7)

To create Reporting Interface connection with Crystal Reports:

1. Open Crystal Reports and create a new connection using **OLE DB (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 Reporting Interface, see Reporting Interface data sources (page 9).

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/en-us/support/knowledgebase/112873.aspx.

7 Technical support

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

- Visit the Sophos 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