

# SOPHOS

## Sophos Enterprise Console version 3.0 scheduled reporting guide

Document date: June 2007





# Contents

- About this guide.....4
- 1 Scheduled reporting tools.....5
- 2 Using RepStat.exe .....7
- 3 Using RepThrt.exe.....15
- 4 Using XMLTrans.exe .....19
- 5 Using RepMail.exe.....22
- 6 Report configuration using the report utilities .....25
- Technical support.....34

## **About this guide**

This guide tells you how to generate scheduled reports using specialized reporting tools provided by Sophos. You can create reports about items detected by Sophos security software and about the status of computers on your network.

# 1 Scheduled reporting tools

Enterprise Console enables you to generate scheduled reports about detected items and about the status of computers on your network.

Several specialized tools can configure and generate these reports:

- RepStat.exe

This report collects, stores, and exports snapshots of computer and outstanding item statistics from the Enterprise Console database.

- RepThrt.exe

This report exports snapshots of outstanding item details.

- XMLTrans.exe

This report converts XML data to a presentation format by applying pre-defined XSLT templates. The tool is not specific to Enterprise Console, but it has been configured to convert by default the output from RepStat.exe

- RepMail.exe

This report sends text files as attachments to email messages. This tool is not specific to Enterprise Console but its default input is synchronized with the default output of RepStat.exe and XMLTrans.exe.

You can use the Windows Scheduler to run individual tools. Alternatively, you can combine the use of a number of these tools in a batch file. This allows you to customize reporting to your requirements.

The tools do not provide hard-coded formatting of the reports. Instead, formatting is done with external XSLT templates. The following standard templates are provided:

- srep2htm.xsl

This is an XSLT template containing instructions for transforming the RepStat.exe report output into HTML format.

- `srep2csv.xsl`

This is an XSLT template containing instructions for transforming the RepStat.exe report output into CSV format.

- `trep2htm.xsl`

This is an XSLT template containing instructions for transforming the RepThrt.exe report output into HTML format.

- `trep2csv.xsl`

This is an XSLT template containing instructions for transforming the RepThrt.exe report output into CSV format.

- ❗ The templates `srep2csv.xml` and `srep2hrm.xml` are replaced during an upgrade from Enterprise Console version 2.0. The templates `srep1csv.xml` and `srep1hrm.xml` are generated for situations where it is necessary to preserve the default format of the reports from version 2.0. The templates `srep1csv.xml` and `srep1hrm.xml` may not be supported in future versions.

Several other files contain report customization details:

- `crepconf.xml`

This is the report configuration file. It contains information about which data fields to include, their order, whether to display headers, company name and differences from the previous snapshot.

- `crephdrs.xml`

This is the report resource file. It contains headers and other strings translated into all supported languages.

- `creplang.xsl`

This is the report language configuration file. It determines the language of the report.

You can customize your reports by changing parameter values in `crepconf.xml` and `creplang.xsl` files with a text editor (e.g. Notepad).

[Section 6](#) gives examples of using the above report tools.

## 2 Using RepStat.exe

RepStat.exe is a command-line reporting tool that performs two functions:

- It collects snapshots of computer and outstanding item statistics and saves them to the Enterprise Console database.
- It exports data from saved snapshots to a file in XML format.

By default, RepStat.exe executes both actions in sequence.

Command-line qualifiers can disable either action. If you disable both actions, an error code is returned.

Differences between sequential snapshots are not stored or reported by this tool. Such differences are implemented by the XSLT transformations which convert report data to the final presentation format.

The tool must be run with a user account that has sufficient rights to:

- access the database (member of group Sophos DB Users)
- write to the output file.

### Command-line qualifiers

Qualifier	Action
-noreport	Skip exporting a report.
-nocollect	Skip collecting a snapshot.
-output= <file_path>	Specifies the output XML file in which the report will be saved. If the file exists, its contents will be overwritten. If the qualifier is not specified, a file with the default name statrep.xml will be created in the folder from which RepStat.exe has been started. The account under which the tool is running must have sufficient rights to write to the output file.

Qualifier	Action
-numentries= <number>	Specifies how many snapshots to include in the report. If not specified, the report will contain data from the two most recent snapshots.
-uptodatelat= <minutes>	Specifies the update latency in minutes for calculating the up-to-date time threshold. The tool searches for the latency value settings in the following order: <ol style="list-style-type: none"> <li>1. command-line qualifier -uptodatelat</li> <li>2. value 'UpToDateLatencyMins' in registry entry [HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\EE\Management Tools]</li> <li>3. If none of these settings is available, a default value of 60 minutes is applied.</li> </ol>
-udl= <file_ path>	Specifies the path to a Universal Data Link (UDL) file containing the database connection configuration. The tool searches for a database connection string in the following order: <ol style="list-style-type: none"> <li>1. udl file path specified with the qualifier -udl</li> <li>2. value 'DatabaseConnectionGUI' in registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\EE\Management Tools]</li> <li>3. value 'DatabaseConnectionMS' in registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\EE\Management Tools]</li> </ol>
-debug	Enables sending log messages to the debug output.

## Return codes

Code	Message
0	Success.
1	Invalid command-line qualifier.
2	Unknown exception.

Code	Message
3	Failed to initialize COM.
4	Snapshot collection has failed.
5	Report generation has failed.
6	Failed to open the output file.
7	Failed to write to the output file.
8	All actions have been disabled.

## Installation dependencies

The tool depends on a number of DLLs:

- EmErr.dll
- EmTrace.dll
- msvcp71.dll
- msucr71.dll

All of these are deployed as part of the Sophos Enterprise Console server installation.

## Reported data fields

The following data fields are exported by the report:

Name	Description
Company	Company name as set from the console GUI.
ID	Unique identifier assigned to the snapshot.

<b>Name</b>	<b>Description</b>
CollectedAtGMT	UTC date and time of the snapshot: yyyy-mm-ddThh:mm:ss (e.g. "2005-10-05T09:49:53").
TotalNumber	Total number of computers.
Assigned	Number of computers assigned to groups.
Managed	Number of managed computers.
Connected	Number of managed computers that have been connected at the time of the snapshot.
WithAUInstalled	Number of managed computers with Sophos AutoUpdate installed.
WithSAVInstalled	Number of managed computers with Sophos Anti-Virus installed.
WithSAVOnAccess	Number of managed computers with enabled on-access scanner.
WithAppCtrlOnAccess	Number of managed computers with active on-access application control.
WithSCFInstalled	Number of managed computers with Sophos Client Firewall installed.
WithSCFStarted	Number of managed computers with active Sophos Client Firewall.
WithVirusAlerts	Number of managed computers having at least one outstanding virus/spyware item.
WithPUAAlerts	Number of managed computers having at least one outstanding adware/PUA item.
WithSCFAlerts	Number of managed computers having at least one outstanding firewall item.

Name	Description
WithSuspiciousAlerts	Number of managed computers having at least one outstanding suspicious item.
WithAppCtrlAlerts	Number of managed computers having at least one outstanding controlled application item.
WithDetectedItems	Number of managed computers having at least one outstanding detected item.
WithSAVErrors	Number of managed computers with outstanding Sophos Anti-Virus errors.
WithSCFErrors	Number of managed computers with outstanding Sophos Client Firewall errors.
WithUpdateErrors	Number of managed computers with update errors.
WithSophosProductErrors	Number of managed computers having outstanding update errors or Sophos managed product errors.
WithInstallErrors	Number of managed computers with installation errors.
OutOfDate	Number of connected managed computers running an out-of-date installation package. A computer is considered out-of-date if EM Library has deployed a more recent package to the central installation directories (CIDs), but the computer has not been updated after a pre-defined latency time (60 minutes by default).
WithDifferentSAVpolicy	Number of managed computers with Sophos Anti-Virus installed that violate their group's SAV policy. Deprecated.
WithDifferentAUpolicy	Number of managed computers with AutoUpdate installed that violate their group's Update policy. Deprecated.

<b>Name</b>	<b>Description</b>
WithDifferentSCFpolicy	Number of managed computers with Sophos Client Firewall installed that violate their group's firewall policy. Deprecated.
WithDifferentPolicy	Number of managed computers that violate their group's policy for at least one of the managed Sophos applications installed on them.
VirusCount	Total number of outstanding viruses and spyware programs on all computers.
PUACount	Total number of outstanding adware/PUA items on all computers.
SCFCount	Total number of outstanding firewall items on all computers.
SuspiciousCount	Total number of outstanding suspicious items on all computers.
AppCtrlCount	Total number of outstanding controlled application items on all computers.
HoursSinceLastEMLibUpdate	Number of hours elapsed since the last EMLibrary update. Value of 999999 indicates that the last EMLibrary update time was not available.

## History length

The history of accumulated statistics snapshots is stored in the database. The maximum number of stored snapshot entries is restricted by a pre-defined history length. The history length value is set in days, and is stored in the column "StatisticsLengthInDays" of the database table "ReporterParameters".

The default history length limit is 90 days. If the parameter value has been changed to less than one day, it will be ignored and a history length of 1 day will be applied by the purge algorithm.

## Example of XML data output

```
<?xml version="1.0" encoding="utf-16" ?>
<StatisticsReport>
  <Company>Sophos plc</Company>
  <Computers>
    <Entry ID="3" CollectedAtGMT="2007-
03-21T08:48:33" TotalNumber="1500"
Assigned="1500" Managed="1500"
Connected="750" WithAUIinstalled="1490"
WithSAVInstalled="1490"
WithSAVOnAccess="1189"
WithAppCtrlOnAccess="1189"
WithSCFInstalled="1490"
WithSCFStarted="1490" WithVirusAlerts="206"
WithPUAAlerts="227" WithSCFAlerts="484"
WithSuspiciousAlerts="991"
WithAppCtrlAlerts="1038"
WithDetectedItems="1432" WithSAVErrors="372"
WithSCFErrors="541" WithUpdateErrors="0"
WithSophosProductErrors="772"
WithInstallErrors="0" OutOfDate="301"
HoursSinceLastEMLibUpdate="2"
WithDifferentSAVpolicy="380"
WithDifferentAUpolicy="379"
WithDifferentSCFpolicy="422"
WithDifferentPolicy="1044" VirusCount="319"
PUACount="297" SCFCount="495"
SuspiciousCount="1759" AppCtrlCount="1100" />
    <Entry ID="2" CollectedAtGMT="2007-
03-21T08:44:20" TotalNumber="1500"
Assigned="1500" Managed="1500"
Connected="750" WithAUIinstalled="1490"
WithSAVInstalled="1490"
WithSAVOnAccess="1195"
WithAppCtrlOnAccess="1195"
```

```
WithSCFInstalled="1490"  
WithSCFStarted="1490" WithVirusAlerts="197"  
WithPUAAlerts="216" WithSCFAlerts="450"  
WithSuspiciousAlerts="965"  
WithAppCtrlAlerts="1000"  
WithDetectedItems="1423" WithSAVErrors="350"  
WithSCFErrors="500" WithUpdateErrors="0"  
WithSophosProductErrors="724"  
WithInstallErrors="0" OutOfDate="255"  
HoursSinceLastEMLibUpdate="999999"  
WithDifferentSAVpolicy="384"  
WithDifferentAUpolicy="395"  
WithDifferentSCFpolicy="390"  
WithDifferentPolicy="1037" VirusCount="309"  
PUACount="284" SCFCount="450"  
SuspiciousCount="1681" AppCtrlCount="1000" />  
</Computers>  
</StatisticsReport>
```

## 3 Using RepThrt.exe

RepThrt.exe is a command-line reporting tool that exports a snapshot of outstanding detected item details from the Enterprise Console database.

By default, RepThrt.exe exports details about all outstanding detected items. You can use a command-line qualifier to customize the export action to only those threats that have been detected for first time since the last successful export.

The tool must be run with an account that has sufficient rights to:

- access the database (member of group Sophos DB Users)
- write to the output file
- read and write to the file storing the latest execution time.

### Command-line qualifiers

Qualifier	Action
-latest	Includes only outstanding detected items registered since the last export performed by RepThrt.exe.
-output= <file_path>	Specifies the output XML file to which the report will be saved. If the file exists, its contents will be overwritten. If the qualifier is not specified, a file with the default name thrtrep.xml will be created in the folder from which RepThrt.exe has been started. The account under which the tool is running must have sufficient rights to write to the output file.
-lasttimeto= <file_path>	Specifies the file path to which the time of the last successful export performed by RepThrt is stored. If the file exists, its contents will be overwritten. If the qualifier is not specified, a file with the default name RepThrt.ltt will be created in the folder from which RepThrt has been started. The account under which the tool is running must have sufficient rights to read from and write to the file.

Qualifier	Action
-udl= <file_path>	Specifies the path to a Universal Data Link (UDL) file containing the database connection configuration. The tool searches for a database connection string in the following order: <ol style="list-style-type: none"> <li>1. udl file path specified with the qualifier -udl</li> <li>2. value 'DatabaseConnectionGUI' in registry entry [HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\EE\Management Tools]</li> <li>3. value 'DatabaseConnectionMS' in registry entry [HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\EE\Management Tools]</li> </ol>
-debug	Enables sending log messages to the debug output.

## Return codes

Code	Message
0	Success.
1	Invalid command-line qualifier.
2	Unknown exception.
3	Failed to initialize COM.
4	Invalid latest execution time value.
5	Report generation has failed.
6	Failed to open the output file.
7	Failed to write to the output file.
8	Failed to read the last execution time.
9	Failed to save the last execution time.

## Installation dependencies

The tool depends on a number of DLLs:

- EmErr.dll
- EmTrace.dll
- msvcp71.dll
- msvcr71.dll

These are all deployed as part of Sophos Enterprise Console server installation.

## Reported data fields

The following data fields are exported by the report:

Name	Description
Company	Company name as set from the console GUI.
TimeGMT	UTC time when the report has been produced.
FirstDetectedSinceGMT	Minimum UTC time value used for the filter activated by the qualifier -latest. This attribute is not present if -latest has not been used.
Type	Item type code: 1 - Virus/spyware 2 - Adware/PUA 3 - Firewall 4 - Suspicious behavior 5 - Suspicious file 6 - Controlled application
Name	Item name.

Name	Description
FilePath	Path to the affected file. The field is left blank if an item is not associated with a particular file.
FirstDetectedAt	UTC date and time when the item was first detected.
ComputerID	Unique computer ID number.
ComputerName	Computer name prefixed by the domain name: "domain\name".
ID	Unique ID number assigned to the item instance.

### Example of XML data output

```
<?xml version="1.0" encoding="utf-16" ?>
<StatisticsReport TimeGMT="2006-06-16T09:37:13" >
  <Company>MyCompany</Company>
  <ThreatsAndPotentialThreats >
    <Entry Type="1" Name="EICAR-AV-Test" FilePath="C:\eicar.com"
      FirstDetectedAt="2006-06-14T16:52:34"
      ComputerID="1" ComputerName="Domain\Machine1" ID="1"/>
  </ThreatsAndPotentialThreats>
</StatisticsReport>
```

## 4 Using XMLTrans.exe

XMLTrans.exe is a command-line tool for transforming XML files by using XSLT template files. The tool does not have any functionality specific to Enterprise Console, except that the default name of the input XML file is chosen to match the default output file name from tool RepStat.exe. The tool must be run with an account that has sufficient rights to read the input file and the template file, and write to the output file.

### Command-line qualifiers

Qualifier	Action
-xml= <file_path>	Specifies the path to an XML file generated by the tool RepStat.exe. The default is: statrep.xml.
-output= <file_path>	Specifies an output file path where the report will be saved. The default is: statrep.htm.
-xslt= <file_path>	Name of the XSLT template file to use for the transformation. The default is: srep2htm.xsl.
-htm	Indicates that the report is in HTML format. The output file path will be formed from the input (XML) path by changing the file extension to .htm. The qualifier will be ignored if the qualifier -output is specified.
-csv	Indicates that the report is in CSV format. The output file path will be formed from the input (XML) file path by changing the file extension to .csv. The qualifier will be ignored if the qualifier -output is specified.
-debug	Enables sending log messages to the debug output.

## Return codes

Code	Message
0	Success.
1	Invalid command-line qualifier.
2	Unknown exception.
3	Failed to initialize COM.
4	Failed to load the XML file.
5	Failed to load the XSLT file.
6	Failed to transform the XML contents.
7	Failed to open the output file.
8	Failed to write to the output file.
9	Failed to instantiate XML document.
10	Unexpected MSXML error.

## Installation dependencies

The tool uses MSXML4 objects. MSXML4 is a free Microsoft re-distributable installed as part of Sophos Enterprise Console.

## Additional distribution files

- crepconf.xml - A report configuration file.
- crephdrs.xml - A file containing the report headers translated to all languages.
- creplang.xsl - A file containing the report language settings.
- srep2csv.xsl - A pre-defined transformation of the RepStat.exe output to CSV format.

- `srep2htm.xsl` - A pre-defined transformation of the `RepStat.exe` output to HTML format.
- `trep2csv.xsl` - A pre-defined transformation of the `RepThrt.exe` output to CSV format.
- `trep2htm.xsl` - A pre-defined transformation of the `RepThrt.exe` output to HTML format.

The files `srep2csv.xml` and `srep2hrm.xml` are replaced during an upgrade from Enterprise Console version 2.0. The files `srep1csv.xml` and `srep1hrm.xml` are generated for situations where it is necessary to preserve the default format of the reports from the earlier version.

## 5 Using RepMail.exe

RepMail.exe is a command-line tool for sending a report file as an email message attachment. RepMail.exe does not have any functionality specific to Enterprise Console, except that the default file name is set to match the default output file name of the tool XMLTrans.exe.

### Command-line qualifiers

Qualifier	Action
-server= <SMTP_server>	SMTP server address. (mandatory)
-to= <recipient>	Well-formed email address of the recipient. (mandatory)
-attach= <file_path>	Path to the report file to send. The file will be attached to the email message. Optionally its contents can be embedded in the body of the message (see option -body). (default: statrep.htm)
-body= <body_string>	If the body string specified from the command line is blank, it will be replaced with the contents of the file specified with the qualifier -attach. (default: <blank>)
-from= <from_string>	Well-formed email address string used to set message field "From". (default: ComputerState@Report)
-subject= <subject_string>	Message subject string. (default: Computer state report)
-user= <user_name>	(default: <blank>)
-passw= <password>	(default: <blank>)

Qualifier	Action
-port= <port_ number>	(default: 25)
-debug	Enables sending log messages to debug output.

## Return codes

Code	Message
0	Success.
1	Invalid command-line qualifier.
2	Unknown exception.
3	Unexpected COM error.
4	Invalid "Server" value.
5	Invalid "To" value.
6	Invalid "From" value.
7	Failed to open file.
8	Failed to read file.
9	The specified file is empty.
10	Failed to update the message configuration.
11	Failed to attach file.
12	Failed to send the message.

## **Installation dependencies**

RepMail.exe is implemented by using Microsoft CDO objects. CDO is a standard part of the Windows 2000 and Windows XP installation.

## 6 Report configuration using the report utilities

This section describes the use of `creplang.xml` and `crepconf.xml`, and gives examples of how to use the scheduled reporting utilities.

### 6.1 Language (`creplang.xml`)

Language configuration settings are stored in the file `creplang.xml`. This is an XSLT file that is imported directly to the main report template files:

```
<?xml version="1.0" encoding="utf-8" ?>
<xsl:stylesheet version="1.0" xmlns:
xsl="http://www.w3.org/1999/XSL/Transform" >
<xsl:variable name="language">en</xsl:
variable>
<xsl:variable name="sublanguage"></xsl:
variable>
<xsl:variable name="timezone">0</xsl:
variable>
</xsl:stylesheet>
```

The configuration data determines what language will be used for producing the report headers and the format for representing date and time.

- ❗ The displayed time is always UTC.

The file contains the definitions of three XSLT variables:

- language
- sublanguage
- timezone.

The variable “language” is mandatory. It must take one of the following values:

- “en” English
- “de” - German
- “es” - Spanish
- “fr” - French
- “it” - Italian
- “ja” - Japanese
- “zh-cn” - Simplified Chinese
- “zh-tw” - Traditional Chinese

The variable ‘sublanguage’ is optional. It can currently take only one value:

- “us” - English (USA)

The variable ‘timezone’ is not used, and is reserved for future implementations.

## 6.2 Report contents and layout (crepconf.xml)

The file crepconf.xml contains the parameters and options that control what data will be included, and in what order it will appear in the report. All attributes take values of either “1” for enabling the option, or “0” for disabling it:

```
<?xml version="1.0" encoding="utf-8" ?>
<StatisticsReportConfiguration>
  <Computers DisplayCompany="1"
    DisplayTitle="1" DisplayDifferences="1"
    DisplayHeader="1">
    <column link="ID" enabled="1" iscount="0" />
    <column link="CollectedAtGMT" enabled="1"
      iscount="0" />
```

```
<column link="TotalNumber" enabled="1"
iscount="1" />
<column link="Assigned" enabled="1"
iscount="1" />
<column link="Managed" enabled="1"
iscount="1" />
<column link="Connected" enabled="1"
iscount="1" />
<column link="WithDetectedItems" enabled="1"
iscount="1" />
<column link="OutOfDate" enabled="1"
iscount="1" />
<column link="HoursSinceLastEMLibUpdate"
enabled="1" iscount="1" />
<column link="WithDifferentPolicy"
enabled="1" iscount="1" />
<column link="WithSophosProductErrors"
enabled="1" iscount="1" />
<column link="WithVirusAlerts" enabled="1"
iscount="1" />
<column link="WithPUAAlerts" enabled="1"
iscount="1" />
<column link="WithSCFAlerts" enabled="1"
iscount="1" />
<column link="WithSuspiciousAlerts"
enabled="1" iscount="1" />
<column link="WithAppCtrlAlerts" enabled="1"
iscount="1" />
<column link="VirusCount" enabled="1"
iscount="1" />
```

```
<column link="PUACount" enabled="1"
iscount="1" />
<column link="SCFCount" enabled="1"
iscount="1" />
<column link="SuspiciousCount" enabled="1"
iscount="1" />
<column link="AppCtrlCount" enabled="1"
iscount="1" />
<column link="WithAUIInstalled" enabled="1"
iscount="1" />
<column link="WithSAVInstalled" enabled="1"
iscount="1" />
<column link="WithSAVOnAccess" enabled="1"
iscount="1" />
<column link="WithSCFInstalled" enabled="1"
iscount="1" />
<column link="WithSCFStarted" enabled="1"
iscount="1" />
<column link="WithAppCtrlOnAccess"
enabled="1" iscount="1" />
</Computers>
<ThreatsAndPotentialThreats
DisplayCompany="1" DisplayTitle="1"
DisplayHeader="1">
<column link="Type" enabled="1" />
<column link="FirstDetectedAt"
enabled="1" />
<column link="Name" enabled="1" />
<column link="ComputerName" enabled="1" />
<column link="FilePath" enabled="1" />
```

```
<column link="ComputerID" enabled="0" />
<column link="ID" enabled="0" />
</ThreatsAndPotentialThreats>
</StatisticsReportConfiguration>
```

## Computer report options

- **DisplayCompany** controls if the company name will appear in the report.
- **DisplayTitle** controls if the title will appear in the report.
- **DisplayDifferences** controls if differences between the values of sequential snapshots will be displayed for countable data values.
- **DisplayHeader** controls if table column headers will be displayed.

## Computer report column options

- **enabled** controls if the data field will appear in the report.
- **iscount** determines if the data value is countable (if difference between sequential snapshots can be calculated).

## Threat report options

- **DisplayCompany** controls if the company name will appear in the report.
- **DisplayTitle** controls if the title will appear in the report.
- **DisplayHeader** controls if table column headers will be displayed.

## Threat report column options

- **enabled** controls if the data field will appear in the report.

## 6.3 Examples of using the report tools

### Default

- Create snapshot and export the two most recent snapshots to file statrep.xml.
- Generate report in HTML format and save to file statrep.htm.
- Email the generated report.

```
@RepStat.exe
@if ERRORLEVEL 1 GOTO RepStatErr
@XMLTrans.exe
@if ERRORLEVEL 1 GOTO XMLTransErr
@RepMail.exe -server="ServerName"
-to="UserName"
@if ERRORLEVEL 1 GOTO RepMailErr
@goto end
:RepStatErr
@echo RepStat execution failed
@goto end
:XMLTransErr
@echo XMLTrans execution failed
@goto end
:RepMailErr
@echo RepMail execution failed
:end
```

## Generate and store statistics daily, produce report weekly

Execute daily:

- Create and save snapshot
  - Do not export data for report
- ```
@RepStat.exe -noreport
@IF ERRORLEVEL 1 GOTO RepStatErr
@GOTO end
:RepStatErr
@echo RepStat execution failed
@GOTO end
:end
```

Execute weekly:

- Do not create new snapshot
  - Export the 7 most recent snapshots to file weekly.xml
  - Generate report in CSV format in file weekly.csv
  - Email the generated report.
- ```
@RepStat.exe -nocollect -numentries=7
-output="c:\temp\weekly.xml"
@IF ERRORLEVEL 1 GOTO RepStatErr
@XMLTrans.exe -xml="c:\temp\weekly.xml"
-xslt="srep2csv.xsl" -output="c:\temp\
weekly.csv"
@IF ERRORLEVEL 1 GOTO XMLTransErr
@RepMail.exe -server="ServerName"
-to="UserName" -attach="c:\temp\weekly.csv"
@IF ERRORLEVEL 1 GOTO RepMailErr
```

```
@GOTO end

:RepStatErr

@echo RepStat execution failed

@GOTO end

:XMLTransErr

@echo XMLTrans execution failed

@GOTO end

:RepMailErr

@echo RepMail execution failed

:end
```

## **Threat report**

- Export data for the threats detected since the last report generation.
- Generate report in HTML format.
- Email the generated report.

```
@RepThrt.exe -latest

@if ERRORLEVEL 1 GOTO RepThrtErr

@XMLTrans.exe -xml="thrtrep.xml"
-xslt="trep2htm.xsl" -htm

@if ERRORLEVEL 1 GOTO XMLTransErr

@RepMail.exe -server="ServerName"
-to="UserName" -attach="thrtrep.htm"

@if ERRORLEVEL 1 GOTO RepMailErr

@GOTO end

:RepThrtErr

@echo RepThrtErr execution failed
```

```

@GOTO end

:XMLTransErr

@echo XMLTransErr execution failed

@GOTO end

:RepMailErr

@echo RepMailErr execution failed

:end

```

## Create default reports compatible with version 2.0

The default format of both HTML and CSV reports generated by XMLTrans has changed in Enterprise Console 3.0. Small changes to the calling commands to use alternative transformations (srep1htm.xsl for HTML reports and srep1csv.xsl for CSV reports) will ensure that the default number of fields and their sequence are preserved.

Command in version 2.0 producing a report	Command in version 3.0 producing a report compatible with version 2.0
<i>Default HTML report</i>	
<pre>@XMLTrans.exe or @XMLTrans.exe -xslt=srep2htm.xsl</pre>	<pre>@XMLTrans.exe -xslt=srep1htm.xsl</pre>
<i>Default CSV report</i>	
<pre>@XMLTrans.exe -csv or @XMLTrans.exe -xslt=srep2csv.xsl -output=statrep.csv</pre>	<pre>@XMLTrans.exe -xslt=srep1csv.xsl -csv or @XMLTrans.exe -xslt=srep1csv.xsl -output=statrep.csv</pre>

## Technical support

For technical support, visit [www.sophos.com/support](http://www.sophos.com/support).

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

Copyright © 2007 Sophos Group. 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 licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.