Sophos Scan Engine

Integration and Configuration of the Sophos Virus Scanner in iQ.Suite Watchdog

Dokumentversion 3.1

iQ.Suite für IBM Domino, Version 17
iQ.Suite für Microsoft Exchange/SMTP, Version 13

Content

1 Introduction

For virus scanning in iQ.Suite Watchdog the virus scanner from our business partner Sophos can be used.

The scanner is integrated in the iQ.Suite as anti-virus Engine called SAVI (**S**ophos **A**nti **V**irus **I**nterface). The scanner provides effective protection against system damaging programs, such as viruses, trojans, spyware and malware. As a Scan Engine of the module iQ.Suite Watchdog, the Sophos virus scanner is seamlessly integrated in the existing range of services of the iQ.Suite.

At email scanning, the email bodies and file attachments are checked for typical patterns of harming programs. Emails that match this patterns are not delivered to the recipients but stored in the iQ.Suite Quarantine.

Service offer for the Sophos virus scanner:

- High rate of virus detection
- High speed on virus scanning
- Frequent, automatic updates for virus patterns and monthly updates for the Scan Engine
- Analysis on functionality of new virus patterns before usage in the scanner
- Archive scanning
- Return codes on password-protected files

You can use SAVI as **integrated Sophos Scan Engine** immediately after iQ.Suite installation. SAVI requires a separate license which can be requested from the GBS Sales Team.

Notes:

For further information on installation and configuration of the virus scanner, please refer to the iQ.Suite manuals. SAVI modifications are described in the Release Notes until the update of this document.

In multi-server environments, we recommend to use the **iQ.Suite Update Manager** as central update service. For further information, please refer to the separate document concerning the iQ.Suite Update Manager (TechDoc). Download on www.gbs.com.

2 iQ.Suite Configuration for IBM Domino

Perform the steps outlined below to use Sophos as an integrated virus scanner in the iQ.Suite:

1. Enable the configuration document of the Sophos Scan Engine and perform the desired settings, if required: WATCHDOG -> UTILITIES -> VIRUS SCANNER ENGINES -> SOPHOS SCAN ENGINE.
2. Optional: If you use a proxy server, make sure that a corresponding proxy server document is enabled (GLOBAL -> PROXY SERVER) and this document is selected for use in the Sophos Scan Engine.
3. Configure a corresponding virus scanner document under WATCHDOG -> UTILITIES -> VIRUS SCANNER. A preset job document is available. Select in the **Basics** tab the enabled 'Sophos Scan Engine'. If not already enabled, enable the Sophos virus scanner. The document is already enabled if the Sophos virus scanner has been selected in the iQ.Suite setup dialog.
4. Configure a Watchdog virus scanning job and enable the document.

   The current version of the Sophos Scan Engine and the latest virus patterns are downloaded initially. Depending on your system environment, the download may take a few minutes.
5. By default, the Sophos download area will be checked for the latest pattern versions each 60 minutes and new patterns are downloaded. You can modify the download time interval in the Engine configuration document.

Note: If an error occurs on future incremental pattern downloads, for troubleshooting set the log level in the global parameter `ToolKit_SubsysLogLevel` to the value '7'.

If required, virus patterns can be updated **manually**:

1. Ensure the iQ.Suite or the iQ.Suite Grabber has been deactivated.
2. If you use a proxy server, enter the connection data in the script *test_download.cmd* (Windows) or *test_download.sh* (Unix) under `sophos3/update`.
3. Execute the script.

Unix: The script has to be executed in the context of the Domino user. Otherwise errors may occur on further pattern updates, due to missing authorization.

3 iQ.Suite Configuration for Microsoft Exchange/SMTP

Perform the steps outlined below to use Sophos as an integrated virus scanner in the iQ.Suite:

1. Enable the Sophos Scan Engine: BASIC CONFIGURATION -> UTILITY SETTINGS -> SCAN ENGINES -> SOPHOS SCAN ENGINE.
2. Create a Virus Scanning Job and select in the **Scan Engines** tab the enabled 'Sophos Scan Engine'.
3. Optional: To use a proxy server for the updates, define the connection settings: BASIC CONFIGURATION -> GENERAL SETTINGS -> PROXY SERVERS.
4. If you have the Sophos Scan Engine already in use as an external Engine, disable it as well as the corresponding job.
5. Save the configuration.

   The Sophos download area will be checked for more recent virus patterns each 60 minutes. New pattern versions will be downloaded. To modify the download interval, enter the desired number of minutes under SOPHOS SCAN ENGINE -> UPDATE TAB.
6. Optional: If required, virus patterns can be updated **manually**: IQ.SUITE MONITOR -> SERVERS -> <SERVER NAME> -> SERVER STATUS -> TEST TAB -> **ENGINES UPDATE** -> START.

   The current version of the Sophos Scan Engine and the latest virus patterns are downloaded initially. Depending on your system environment, the download may take a few minutes.

   If the update process ends successfully, the message 'OK' is displayed; if an error occurred, 'Error' is shown instead. The update process is documented in the Event Log.
7. Click on IQ.SUITE MONITOR -> SERVERS -> <SERVER NAME> -> SERVER STATUS -> TEST TAB -> **ENGINES TEST**-> START.

   The Engine and pattern scanning is started. A test without errors is confirmed with 'OK', Errors are indicated with 'Error'.

Note: In case of errors, delete the *current.ini* file and click on **ENGINES UPDATE** to download the initial virus patterns again.

4 Technical Description

4.1 Functionality of the Sophos Scan Engine and of the Virus Pattern Update

To be able to download the virus patterns for virus scanning, the iQ.Suite has to be configured as described in the chapters above[1]. After the configured Watchdog virus scanning job has been enabled and saved, it is initialized. With the job initialization, the virus patterns are initially downloaded.

After the initial download, future pattern and Engine updates are initialized automatically according to the time interval defined in the iQ.Suite.

Current data for the Sophos scanner is provided on the GBS download area. The iQ.Suite periodically compares the used pattern and Engine versions with the versions of the GBS download area. If the data of the download area is more recent than the versions used in the iQ.Suite, the newer versions are downloaded automatically. The virus patterns are incrementally updated several times a day which reduces the downloaded data size to < 1 MB. This reduces network load and speeds up the download rate.

The data from the GBS download area is synchronized regularly with the data provided from Sophos. The frequent pattern and Engine updates ensure short term reaction on new published malware.

If you are using iQ.Suite Update Manager as central update service, please refer to the separate document concerning the iQ.Suite Update Manager (TechDoc) to obtain information on the functionality. Download on www.gbs.com.

[1] Refer to iQ.Suite Configuration for IBM Domino and iQ.Suite Configuration for Exchange/SMTP.

4.2 iQ.Suite for IBM Domino

4.2.1 Directory Structure

The configuration data of the integrated Sophos Scan Engine (*tk_sophos3.dll*) is stored in the `sophos3` directory. Path:

Under Windows: `<Program path>\iQSuite\sophos3`
Under Unix: `<Program path>/iqsuite/sophos3`

Under Unix, please note that the iQ.Suite must be installed individually on each server.

The structure of the Scan Engine's directory is described in the following chapter.

Note: Do not delete files or subdirectories from the `sophos3` directory. Otherwise unexpected and undesired effects may occur. The parameters required for automatic virus pattern updates are preset and don't need to be adjusted.

4.2.2 Description of the Components

Initially, the `sophos3` directory consists of the following files and subdirectories:

Nr	Files under Windows	Files under Unix, AIX, Solaris	Task
Files under `sophos3`:			
1	*soap.tk_sophos3.dll* *tk_sophos3.dll.exe* *soap.tk_sophos3.dll.defaults.ini* *soap.tk_sophos3.dll.ini*	*soap.tk_sophos3.dll* *tk_sophos3.dll.exe* *soap.tk_sophos3.dll.defaults.ini* *soap.tk_sophos3.dll.ini*	Components of the GROUP.Sandbox [2]
2	*tk_sophos3_ref_engine.cfg*	*tk_sophos3_ref_engine.cfg*	Configuration file for the Scan Engine which is analyzed from (**1**).
3	*tk_sophos3_ref_patterns.cfg*	*tk_sophos3_ref_patterns.cfg*	Configuration file for the virus patterns which is analyzed from (**1**).
4	*tk_sophos3.dll*	*tk_sophos3.dll*	GROUP-Interface-DLL which is used from (**1**).
5	*tk_sophos3_maint.cmd* *tk_sophos3_maint.lock*	*tk_sophos3_maint.sh* *tk_sophos3_maint.lock*	File that starts the incremental update.
6	*test_download.cmd*	*test_download.sh*	File to be executed manually. With this file, the current data set is downloaded.
7	*tk_sophos3_upd.bat* *tk_sophos3_update.bat*	*tk_sophos3_update.sh*	Files that perform the update. These files do not have to be executed manually.

[2] Functionality and configuration of the GROUP.Sandbox are described in a separate document. Download on www.gbs.com.

8	*tk_sophos3_upd_process.bat*	-	File that is executed automatically from (**7**).
Files under `sophos3/update`:			
9	*sophos_start_update.cmd*	*sophos_avupdate.sh*	File that starts execution of (**10**) and is called from (**6**).
10			File that starts the update.
	sophos_update.exe sophos_update2*.exe*	*tk_sophos_update* *tk_sophos_update2*	= Filename in iQ.Suite 17.0 = Filename as of iQ.Suite 17.1

The initial data set is first downloaded from the GBS download area to the temporary `tempDownload` directory. Then, the data is copied to `sophos3/update/extract/engine` (**12**) or to `sophos3/update/extract/patterns` (**13**). In case of successful download, this data is then copied to the directories `sophos3/engine` or `sophos3/patterns` from which it is used for virus scanning. The data in the temporary directory is automatically deleted.

Important information on the download is written to (**11**). Note that this file must exist to ensure automatic incremental updates in the future. Otherwise, the complete data set is downloaded.

After the first initial Engine and pattern update, the directories are extended as follows:

Nr	Files under Windows	Files under Unix	Task
Files under `sophos3/update`:			
11	*current.ini*	*current.ini*	This file contains essential information on the download. If this file does not exist, the complete initial data set is downloaded again. After this, the file is created and stored again.
Files under `sophos3/update/extract/engine` `sophos3/engine`:			
12	*<xy>.vdb* *<xy>.dat* *other*	*<xy>.vdb* *<xy>.dat* *other*	Engine files downloaded from the GBS download area. Also refer to description text above.
Files under `sophos3/update/extract/patterns` `sophos3/patterns`:			
13	*<xy>.ide*	*<xy>.ide*	Pattern files downloaded from the GBS download area. Also refer to description text above.

Note: To change the checking procedure of the virus scanner, modify the Engine parameters under WATCHDOG -> UTILITIES -> VIRUS SCANNER -> SOPHOS SCAN PARAMETERS -> SETTINGS TAB. For a detailed parameter description, please refer to the **Comments** tab of the Engine document.

4.3 iQ.Suite for Microsoft Exchange/SMTP

4.3.1 Directory Structure

The directory `<Program path>/GBS/iQ.Suite/Bin/SAVI` contains the configuration files of the integrated Sophos Scan Engine (*tk_sophos3.dll*).

The structure of the Scan Engine's directory is described in the following chapter.

Notes:

Do not delete any files or subdirectories from the `SAVI` directory. Otherwise, undesired and unexpected effects may occur. The parameters required for the update are preset and do not need to be changed.

Do not modify the batch files or configuration files, hence, these changes might be overwritten with an iQ.Suite update. Change the desired settings only in the iQ.Suite administration console.

4.3.2 Description of the Components

Initially, the `SAVI` directory consists of the following files and subdirectories:

Nr	Files under Windows	Task
Files under `SAVI`:		
1	*tk_sophos3_ref_engine.cfg*	Configuration file for the Scan Engine.
2	*tk_sophos3.dll*	GROUP-Interface-DLL.
3	*tk_sophos3_ref_patterns.cfg*	Configuration file for the virus patterns.
4	*tk_sophos3_upd.bat*	File that starts the update automatically. It does not need to be started manually.
5	*tk_sophos3_upd_process.bat*	File that is executed automatically by (**4**).
Files under `SAVI/Update`:		
6	*sophos_start_update.cmd*	Executable file that initializes execution of (**7**). It does not need to be started manually.
7		File that starts the update.
	sophos_update.*exe* sophos_update2.*exe*	= Filename in iQ.Suite 13.0 = Filename as of iQ.Suite 13.1
Files under `SAVI/Update/Extract`:		
	<empty>	

Given the large size of the virus pattern files required to perform a virus scan, they are not part of the initial iQ.Suite installation. After iQ.Suite installation and configuration, the virus patterns and the Engine files (approx. 94 MB) of Sophos are automatically downloaded from the GBS download area (approx. 94 MB).

The Engine and virus patterns are first downloaded to the directory `SAVI/Update/Extract/engine` (**11**) or `SAVI/Update/Extract/patterns` (**12**). Afterwards, the data is copied to `SAVI/engine` or `SAVI/patterns`. Hence, the data in these directories is used for email scanning, the virus scanner is temporarily disabled by the iQ.Suite.

The download procedure is logged in (**10**). If errors occur, please send these files to the GBS Support Team. (**13**) contains essential status information for the incremental update. Note that this file must exist to allow future incremental pattern updates.

After the first initial Engine and pattern download, the directories are extended as follows:

Nr	Files under Windows	Task
	Files under `SAVI`:	
8	*tk_sophos3_ref_engine.cfg.timestamp*	Internal Engine processing file.
9	*tk_sophos3_ref_patterns.cfg.timestamp*	Internal pattern processing file.
10	*tk_sophos3_UPD.<>.log* *e.g.* *tk_sophos3_UPD.success.log* *tk_sophos3_UPD.error.log* *tk_sophos3_UPD.history.log*	Log files of the update. Last successful update. Last faulty update. Updates of the past few months.
	Files under `SAVI/Update/Extract/engine` `SAVI/engine`:	
11	*<xy>.vdb* *<xy>.dat* *other*	Engine files downloaded from the GBS download area.
	Files under `SAVI/Update/Extract/patterns` `SAVI/patterns`:	
12	*<xy>.ide*	Virus pattern files downloaded from the GBS download area.
	Files under `SAVI/Update`:	
13	*current.ini*	File that contains essential information for the download. If this file does not exist, the complete data set is downloaded again and the file is created newly.

5 About GBS

GROUP Business Software is a leading supplier of solutions and services for the IBM and Microsoft collaboration platforms. With the Competence Centers Security, Modernization, Mobility and Portal & BPM, GBS enables its customers to manage the challenges of today and tomorrow faster, easier and more efficiently. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia. The European headquarters is located in Frankfurt/Germany, and the North American headquarters is based in Atlanta.

Further information at www.gbs.com.

European Headquarters
GROUP Business Software AG
MesseTurm
60308 Frankfurt / Germany
Phone: +49 69 789 8819-0
Fax: +49 69 789 8819-99

Email Main Office
GROUP Business Software
Ottostrasse 4
76227 Karlsruhe / Germany
Phone: +49 721 4901-0
Fax: +49 721 4901-199

North American Headquarters
GROUP Business Software (GBS)
585 Molly Lane
Woodstock, GA 30189 / USA
Phone: +1 404-891-1711
Fax: +1 770 720-1335

GROUP Business Software (GBS)
19 Allstate Parkway
Suite 120
Markham, Ontario / Canada - L3R 5A4
Phone: +1 905 475-4064
Fax: +1 905 475-4134

UK Office
GROUP Business Software (UK) Ltd.
Manchester Business Park
3000 Aviator Way
Manchester M22 5TG / UK
Phone: +44 161 266 1066
Fax: +44 700 604 1480

info@ gbs.com
http://www.gbs.com