Avira Scan Engine

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

Document Version 4.0

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

Content

1 Introduction 3

2 iQ.Suite Configuration for IBM Domino 4

3 iQ.Suite Configuration for Microsoft Exchange/SMTP 5

4 Technical Description 6

4.1 Functionality of the Avira Scan Engine and of the Virus Pattern Update 6
4.2 iQ.Suite for IBM Domino 7
4.2.1 Directory Structure 7
4.2.2 Description of the Components 7
4.2.3 Central Update 9
4.3 iQ.Suite for Microsoft Exchange/SMTP 10
4.3.1 Directory Structure 10
4.3.2 Description of the Components 10
4.3.3 Central Update 12

5 Testing the Update Process 13

5.1 Procedure in iQ.Suite for IBM Domino 13
5.2 Procedure in iQ.Suite for Microsoft Exchange/SMTP 13

6 About GBS 14

1 Introduction

For virus scanning in iQ.Suite Watchdog, the Scan Engine from our business partner Avira (formerly Avira AntiVir Engine) can be used.

The scanner is integrated in the iQ.Suite as anti-virus Engine called SAVAPI (**S**ecure **A**nti**V**irus **A**pplication **P**rogramming **I**nterface). The scanner provides effective protection against system damaging programs, such as viruses, trojans and malware. As a Scan Engine of the module iQ.Suite Watchdog, the Avira 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 Avira virus scanner:

- High rate of virus detection
- High speed on virus scanning
- Frequent, automatic updates for virus patterns and SAVAPI Engine[1] files

You can use the Avira virus scanner as **integrated Avira Scan Engine** immediately after iQ.Suite installation. The required Avira license is part of the iQ.Suite licencing.

Since the structural features of harming programs change permanently, the components for virus detection must be modified continuously. For an effective virus-protection, Avira regularly provides us with new engine and virus pattern files that contain improved verification algorithms. These updated files are used for virus scanning in the iQ.Suite to grant a consistent high rate of virus detection and continuous improvement of the analysis results.

A validation procedure is implemented in the iQ.Suite. Before the downloaded Engine and pattern files are used, the data is checked on functionality. This ensures that the virus scanner is still operational after the update.

Notes:

For further information on installation and configuration of the virus scanner, please refer to the iQ.Suite manuals. SAVAPI 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.

[1] SAVAPI 3.4.0.11 (SDK 3.4) is used.

2 iQ.Suite Configuration for IBM Domino

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

1. Enable the configuration document of the Avira Scan Engine and perform the desired settings, if required: WATCHDOG -> UTILITIES -> VIRUS SCANNER ENGINES -> AVIRA 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 Avira 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 activated 'Avira Scan Engine'. If not already enabled, enable the Avira virus scanner. The document is already enabled if the Avira 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 Avira 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 Avira download area will be checked for the latest pattern versions each 60 minutes and new patterns are downloaded. You can modify the time interval in the *soap.tk_savapi.dll.ini* file (refer to Description of the Components).

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'.

3 iQ.Suite Configuration for Microsoft Exchange/SMTP

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

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

    The Avira 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 AVIRA SCAN ENGINE -> UPDATE TAB.
11. 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 Avira 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.
12. 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'.

4 Technical Description

4.1 Functionality of the Avira 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[2]. 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 Avira scanner is provided on a download area. The iQ.Suite periodically compares the used pattern and Engine versions with the versions of the Avira 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 significantly reduces the downloaded data size. This reduces network load and speeds up the download rate.

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.

[2] 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 Avira Scan Engine (*tk_savapi.dll*) is stored in the `savapi` directory. Path:

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

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 `savapi` 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

The `savapi` directory consists of the following files and subdirectories:

Nr	Files under Windows	Files under Unix	Task
Files under `savapi`:			
1	*tk_savapi.dll.exe* *soap.tk_savapi.dll.defaults.ini* *soap.tk_savapi.dll.ini*	*soap.tk_savapi.dll.srv* *soap.tk_savapi.dll.defaults.ini* *soap.tk_savapi.dll.ini*	GROUP.Sandbox components
2	*test_avupdate.cmd*	-	File that initializes the download for the current engine and pattern files. The file can be executed manually if required.
	<xy>.vdf		Pattern files used by the scanner.
	<xy>.dat *other*		Engine files used by the scanner.
3	*avupdate.exe* *avupdate_msg.avr*	*avupdate.bin* *avupdate_msg.avr*	Executable files used by Avira

Files under `savapi/update`:			
4	*tk_savapi_update_call.cmd*	*tk_savapi_update.sh*	Executable file that initializes execution of (**5**).
5	*tk_savapi_upd_process.bat*	*grp_avupdate.sh*	Executable file that initializes execution of (**3**).
6	*avupdate_savapi_mirror.conf*	*avupdate-scanner.conf*	Configuration file used by (**3**).
7	*avupdate_savapi_update.conf*	- -	Configuration file used by (**3**).
8	*avupdate.log*		Internal temporary file
Files under `savapi/update/extract`: (Mirror of the Avira update server)			
	other		Subdirectories that contain compressed download files.
	master.idx		Index file (<iQSuite>\`bin\Savapi\Update`); This file contains information on the current update data. The original file on the Avira server is downloaded on changes and compared with the local copy. If the files are not the same, an update is initialized.
	<xy>.info		Information files (<iQSuite>\`bin\Savapi\Update`); These files contain the logic for file comparison and update.
Files under `savapi/update/rc`:			
12	*savapi_check.exe*		Check file that validates the data set on functionality.
	other		Extracted engine and virus pattern files.

For updating the Engine and virus pattern files, the iQ.Suite regularly calls the Avira update file (**3**) with (**1**) and (**4**).

(**3**) contains commands for initializing the download, for comparison of the versions and for the update.

a) With (**6**) a so-called mirror of the Avira download area is created. The mirrored update files are stored compressed under `<iQSuite>\bin\savapi\update\extract`.

b) With (**7**) the files from the `extract` directory are compared with the current data set used by the virus scanner (directory: `<iqsuite>\bin\savapi`).

If the files in the `extract` directory are more recent, the iQ.Suite initializes a validation process that checks the downloaded data on functionality. The mirrored data from the `extract` directory is extracted to the `Update\RC` directory. With (**5**) the check file (**9**) that executes validation is called. On functional data, return code '10' is returned. Afterwards (**5**) performs a virus pattern update by extracting data from the `extract` directory to `<iqsuite>\bin\savapi\`. With this, the updated

data is used from the virus scanner. On faulty data, return code ‘70’ is returned. The files are not copied, hence, for virus scanning the data set used so far is used further.

The update process is logged in (**8**).

The download time interval can be modified in the *soap.tk_savapi.dll.ini* file (**1**).

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

4.2.3 Central Update

To control the updates over a central server, you can use the *Avira Internet Update Manager*. A central server loads the updates from the Internet and provides them as a web server to the individual clients. The clients load the updates from the central server, e.g. over a shared directory and not directly from the Internet. To configure such a central update, the GROUP.Sandbox of the SAVAPI must be modified[3]. In the *tk_savapi.dll.ini*, enter the parameter `DownloadFrom`=<*target address of the Avira Internet Update Manager*>.

Note: In multi-server environments, we recommend to use the **iQ.Suite Update Manager** as central update service.

[3] For further information on configuration of the *GROUP.Sandbox* please refer to the separate document on the iQ.Suite Sandbox. Download on www.gbs.com.

4.3 iQ.Suite for Microsoft Exchange/SMTP

4.3.1 Directory Structure

The directory `<Program path>/GBS/iQ.Suite/Bin/Savapi` contains the configuration files of the integrated Avira Scan Engine (*tk_savapi.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 `Savapi` 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

The `Savapi` directory consists of the following files and subdirectories:

Nr	Files under Windows	Task
	Files under `SAVAPI`:	
1	*tk_savapi_upd.bat*	This file initializes execution of (**2**) and does not need to be started manually.
2	*tk_savapi_upd_process.bat*	Initializes execution of (**3**)
	<xy>.vdf	Pattern files used by the scanner.
	<xy>.dat *other*	Engine files used by the scanner.
3	*tk_savapi_UPD.<>.log* *e.g.:* *tk_savapi_UPD.success.log* *tk_savapi_UPD.error.log* *tk_savapi_UPD.history.log*	iQ.Suite log files that log the update procedure.
	Files under `SAVAPI/Update`:	
4	*avupdate.exe* *avupdate_msg.avr*	Executable file from Avira
5	*avupdate_savapi_mirror.conf*	Configuration file used by (**3**).
6	*avupdate_savapi_update.conf*	Configuration file used by (**3**).
7	*avupdate.log*	Internal temporary file.

Files under `SAVAPI/Update/Extract`: (Mirror of the Avira update servers)

	other	Subdirectories with compressed download files.
	master.idx	Index file (<iQSuite>`\bin\Savapi\Update`); This file contains information on the latest update data. The original file on the Avira server is downloaded at data changes and compared with the local copy. If both files are not the same, the update is started.
	<xy>.info	Information files (<iQSuite>`\bin\Savapi\Update`); These files contain the logic for data comparison and the update procedure.

Files under `SAVAPI/Update/RC`:

8	*savapi_check.exe*	Check file that validates the data set on functionality.
	other	Extracted engine and pattern files.

For updating the engine and virus pattern files, the iQ.Suite regularly calls the Avira update file (**4**) with (**1**) and (**2**). (**4**) in combination with (**5**) creates a so-called mirror of the Avira download area and stores the mirrored update files in the `<iQSuite>\Bin\Savapi\Update\Extract` directory.

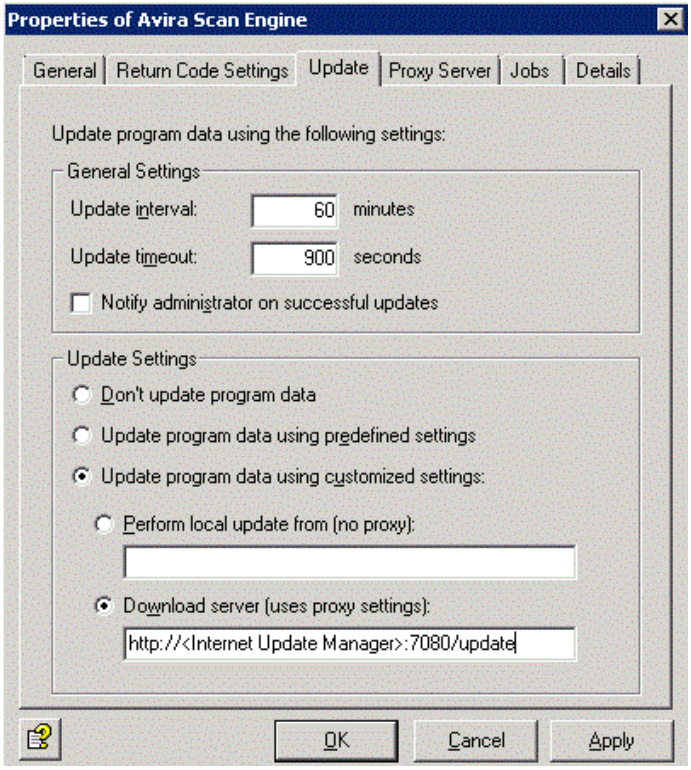
In combination with (**5**) and (**6**), the data in the `Extract` directory is compared with the current data set under `<iQSuite>\Bin\Savapi` used by the virus scanner. If the files in the `extract` directory are more recent, the iQ.Suite initializes a validation process that checks the downloaded data on functionality. The mirrored data from the `extract` directory is extracted to the `Update\RC` directory. With (**2**), the check file (**8**) that executes validation is called. On functional data, return code ‘10’ is returned. Afterwards, (**4**) performs a virus pattern update by extracting the data from the `Extract` directory to `<iQSuite>\Bin\Savapi\`. With this, the updated data is used from the virus scanner. If required, the operating virus scanner is stopped temporarily. On faulty data, return code ‘70’ is returned. The files are not copied, hence, for virus scanning the data set used so far is used further.

The update procedure is logged in (**3**).

4.3.3 Central Update

To control the updates over a central server, you can use the *Avira Internet Update Manager*. A central server loads the updates from the Internet and provides them as a web server to the individual clients. The clients load the updates from the central server, e.g. over a shared directory and not directly from the Internet.

In the iQ.Suite administration console, enter the address of the web server: SCAN ENGINES -> AVIRA SCAN ENGINE -> UPDATE TAB -> UPDATE PROGRAM DATA USING CUSTOMIZED SETTINGS -> DOWNLOAD SERVER (USES PROXY SETTINGS):



For the placeholder <Internet Update Manager> enter the IP address of the central web server on which the Avira Internet Update Manager is installed. The port number corresponds to the standard port of the Update Manager. The settings for the proxy server defined in the **Proxy Server** tab are used.

As an alternative to the Avira download server, you can use a shared directory to exchange the pattern files. For this, specify the shared directory under 'Perform local update from (no proxy)'. The settings for the proxy server defined in the **Proxy Server** tab are ignored.

Note: As an alternative to the *Avira Internet Update Manager*, we recommend to use the **iQ.Suite Update Manager** as central update service.

5 Testing the Update Process

5.1 Procedure in iQ.Suite for IBM Domino

If you want to be notified on successful or faulty updates, set the following parameters in the *avupdate_savapi_update.conf* file.

Parameter	Meaning
smtp-server	SMTP server
smtp-port	SMTP port
smtp-user	SMTP user
smtp-password	SMTP password
notify-when	0= never, 1= at each update, 2= at faulty updates only
auth-method	Authentification method: user/password
email-to	Recipient of the notifications
email-footer	Content of the email footer

The iQ.Suite starts the update. According to your configuration, you receive a notification email in case of a successful or faulty update.

To start the download for the most current Engine and virus pattern files, execute the *test_avupdate.cmd* file.

5.2 Procedure in iQ.Suite for Microsoft Exchange/SMTP

To test the connection to the SAVAPI download area, click on IQ.SUITE MONITOR -> SERVERS -> <SERVER NAME> -> SERVER STATUS -> TEST TAB -> **ENGINES UPDATE** -> START.

The iQ.Suite starts the update. The procedure is logged in the Event log.

A test without errors is confirmed with ‘OK’, errors are indicated with ‘Error’. To analyze the cause of error, use the report of the failed update (detailed view in the result window) or the history log. If necessary, set the log level to a higher value. When update problems persist, the administrator receives a notification email.

6 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