



SAVAPI3 Engine for iQ.Suite Watchdog

**Integration and Configuration in
iQ.Suite for Lotus Domino and
iQ.Suite for Microsoft Exchange**

Document Version 1.0

Think Lotus Think GROUP

 **GROUP**
TECHNOLOGIES
Email simplified

Table of Contents

1	Introduction	2
1.1	Definitions for SAVAPI3	2
1.2	Notes on Updating iQ.Suite	3
1.2.1	iQ.Suite for Lotus Domino	3
1.2.2	iQ.Suite for Microsoft Exchange	4
2	SAVAPI3 Antivirus Engine and Virus Pattern Updates	5
2.1	General	5
2.2	Technical Procedure	5
2.2.1	iQ.Suite for Lotus Domino	5
2.2.2	iQ.Suite for Microsoft Exchange	8
3	Test Scenarios	11
3.1	Testing the DNS Configuration	11
3.2	Testing the Update Process	12
3.2.1	Procedure under iQ.Suite for Microsoft Exchange	12
3.2.2	Procedure under iQ.Suite for Lotus Domino	12

1 Introduction

1.1 Definitions for SAVAPI3

SAVAPI3 (**S**ecure **A**nti**V**irus **A**pplication **P**rogramming **I**nterface) is an antivirus engine developed by Avira and designed to protect systems against malicious software.

As of *iQ.Suite for Lotus Domino Version 12.2* and *iQ.Suite for Microsoft Exchange Version 8.0*, SAVAPI3 is used as engine implemented in the *AntiVir Engine 3 powered by Avira* virus scanner. Replacing the preceding SAVAPI2 product used in the *AntiVir Engine 2 powered by Avira* virus scanner, it provides optimal protection for your system environment through the latest virus recognition mechanisms.

SAVAPI3 for iQ.Suite Watchdog offers:

- High virus recognition rate
- High scanning speed
- Automatic updates of the SAVAPI3 antivirus engine and virus patterns

As the typical features of malware are permanently changing, the virus recognition components need to be constantly adjusted. For effective system protection we recommend to run periodical iQ.Suite updates and integrate the latest patterns searched for in emails. This will ensure a high recognition rate and continuously improving analysis results.

1.2 Notes on Updating iQ.Suite

1.2.1 iQ.Suite for Lotus Domino

Update Installation under Windows

Following an update to an iQ.Suite version ≥ 12.2 , the SAVAPI2 antivirus engine used until now will be replaced with the SAVAPI3 antivirus engine. Once installed, the virus scanner is ready to be used. Please note that any customized SAVAPI2 settings may not be imported by the SAVAPI3 antivirus engine.

In addition, please note the following:

- SAVAPI2 is uninstalled.
- The existing configuration file *savapi.ini* is overwritten. For reference purposes, a copy is saved in the *Savapi* folder and renamed to *savapi2.ini*.
- The existing virus scanner configuration document (SAVAPI2) is preserved for reference purposes. In addition, a new configuration document is created and enabled for SAVAPI3.
- The updates of the SAVAPI3 antivirus engine and the virus patterns are started automatically.
- The update takes into account any proxy server configurations.

Update Installation under Unix

The SAVAPI3 antivirus engine can be installed in the course of an update to an iQ.Suite version ≥ 12.2 (optional).

In addition, please note the following:

- SAVAPI2 is uninstalled.
- The existing virus scanner configuration document (SAVAPI2) is preserved for reference purposes. In addition, a new configuration document is created and enabled for SAVAPI3.
- The updates of the SAVAPI3 antivirus engine and the virus patterns are started automatically.
- Proxy server configurations can be specified in the course of the update.
- The iQ.Suite installation is not performed centrally, but for each server separately.

1.2.2 iQ.Suite for Microsoft Exchange

Following an update to an iQ.Suite version ≥ 8.0 , the SAVAPI2 antivirus engine used until now will be replaced with the SAVAPI3 antivirus engine. Once installed, the virus scanner is ready to be used. Please note that any customized SAVAPI2 settings are not imported by the SAVAPI3 antivirus engine.

In addition, please note the following:

- SAVAPI2 is uninstalled.
- The *savapi.ini* configuration file is no longer used.
- The updates of the SAVAPI3 antivirus engine and the virus patterns are started automatically.
- The update takes into account any proxy server configurations.

Note: Check that, following the update to an iQ.Suite version ≥ 8.0 , the SAVAPI2 services have been removed.

2 SAVAPI3 Antivirus Engine and Virus Pattern Updates

2.1 General

The update of the SAVAPI3 antivirus engine and the virus patterns is performed from a download area where the latest versions are provided for download. iQ.Suite automatically downloads these versions during operation, with no further adjustments required.

In case you are using a proxy server for the update, you can either specify the connection data during the iQ.Suite installation or subsequently configure the connection in the iQ.Suite administration console.

2.2 Technical Procedure

The following describes how the components involved in the update process work. The parameters required for the automatic virus pattern update are preset and need not be changed.

2.2.1 iQ.Suite for Lotus Domino

The update of the SAVAPI3 antivirus engine and the virus patterns is started automatically. The following files are used for the update (directory: <program path>\<iQ.Suite>\Savapi):

#	Files under Windows	Files under Unix	Task
1	<i>soap.ntk_savapi.dll</i> <i>ntk_savapi.dll.exe</i> <i>soap.ntk_savapi.dll.defaults.ini</i> <i>soap.ntk_savapi.dll.ini</i>	<i>soap.tk_savapi.dll</i> <i>soap.tk_savapi.dll.srv</i> <i>soap.tk_savapi.dll.defaults.ini</i> <i>soap.tk_savapi.dll.ini</i>	GROUP.Sandbox components ¹
2	<i>soap.ntk_savapi.dll.proxy.cmd</i>	<i>soap.tk_savapi.dll.proxy.sh</i>	(optional) proxy component
3	<i>tk_savapi_update_call.cmd</i>	<i>tk_savapi_update.sh</i>	Executable file; initiates the execution of (4)
4	<i>tk_savapi_upd_process.bat</i>	<i>grp_avupdate.sh</i>	Executable file; initiates the execution of (5)
5	<i>avupdate.exe</i> <i>avupdate_msg.avr</i>	<i>avupdate.bin</i> <i>avupdate_msg.avr</i>	Executable file(Avira)
6	<i>avupdate_savapi_mirror.conf</i>	<i>avupdate-scanner.conf</i>	Configuration file used by (5)
7	<i>avupdate_savapi_update.conf</i>	--	Configuration file used by (5)
8	--	<i>tk_avfile_update</i>	Executable file(<iQSuite>\bin\)
9	--	<i>tk_savapi_ref.cfg</i>	Configuration file

¹ The GROUP.Sandbox configuration is described in a separate document. Please contact our Support for assistance.

<i>savapi3.conf</i>	<i>savapi3.conf</i>	Configuration file for manually setting specific parameters
<i>master.idx</i>	<i>master.idx</i>	Index file (<iQSuite>\bin\Savapi\Update). Contains information on the latest update data. Whenever data is modified, the original is downloaded from the Avira server and checked against the local copy. If the versions are different, an update is initiated.
<i><xy>.info</i>	<i><xy>.info</i>	Info files (<iQSuite>\bin\Savapi\Update). Contain control information for matching data and the update process.
<i><xy>.vdf</i>	<i><xy>.vdf</i>	Pattern files

1. The GROUP.Sandbox components (1) take care of calling an executable SAVAPI file (3).
2. If proxy server settings have been set in the configuration, a proxy file is created (2) in which these configuration settings are stored.
3. Once the internal executable files have been started, the Avira executable is started (5). This file contains commands that take care of downloading, version control and updating using the configuration files (6) and (7).
 - a) Using the configuration file (6), a mirror of the download area is created. Once downloaded, the mirrored update files are temporarily stored in the <iQSuite>\Bin\Savapi\Update directory and extracted to the <iQSuite>\Bin\Savapi\Update\Extract directory.
 - b) Using the configuration file (7), the mirrored update files are checked against the currently existing files. If the update files are more recent, the new patterns are installed.
4. The installed data is used by the SAVAPI3 antivirus engine for virus detection. Under Unix, a further executable file (8) and a special configuration file (9) take care of updating the GROUP.Sandbox.

Note: The update requires an accessible server environment. You may have to set up a DNS server. A DNS test scenario is described under [Testing the DNS Configuration](#) on page 11.

Configuration options

Central Update

If you wish to control the update from a central server, you can use the *Avira Internet Update Manager*. A central server downloads the updates from the Internet and makes them available to each of the client computers as web server. The client computers download the updates from the central server rather than directly from the Internet, e.g. using a shared directory. To configure such a central update, the Savapi3 *GROUP.Sandbox*² needs to be modified. In the SOAP.Defaults.INI (*soap.(n)tk_savapi.dll.defaults.ini*) set the DownloadFrom parameter as follows: DownloadFrom=<Target address of the Avira Internet Update Manager>

Proxy Server

To use a proxy server for downloading the scan files, enter the proxy server connection data in the iQ.Suite administration console under *GLOBAL -> PROXY SERVER* and then select this option in the virus scanner configuration document.

² The GROUP.Sandbox configuration is described in a separate document. Please contact our Support for assistance.

2.2.2 iQ.Suite for Microsoft Exchange

All configuration settings for the update process are performed in the iQ.Suite administration console.

Note: Do not modify any batch or configuration files as these modifications may be overwritten following an iQ.Suite update.

The update of the SAVAPI3 antivirus engine and the virus patterns is started automatically. The following files are used for the update

(directory: <Program path>\<iQ.Suite>\Bin\Savapi):

#	Files under Windows	Files under Unix	Task
1	<i>tk_savapi_upd.bat</i>		Initiates the execution of (2)
2	<i>tk_savapi_upd_process.bat</i>		Initiates the execution of (3)
3	<i>avupdate.exe</i> <i>avupdate_msg.avr</i>	<i>avupdate.bin</i> <i>avupdate_msg.avr</i>	Executable file (Avira)
4	<i>avupdate_savapi_mirror.conf</i>	<i>avupdate-scanner.conf</i>	Configuration file used by (3)
5	<i>avupdate_savapi_update.conf</i>	<i>avupdate-scanner.conf</i>	Configuration file used by (3)
	<i>master.idx</i>	<i>master.idx</i>	Index file (<iQSuite>\bin\Savapi\Update); Contains information on the latest update data. Whenever data is modified, the original is downloaded from the Avira server and checked against the local copy. If the versions are different, an update is initiated.
	<i><xy>.info</i>	<i><xy>.info</i>	Info files (<iQSuite>\bin\Savapi\Update); Contain the logic for matching data and the update process.
	<i><xy>.vdf</i>	<i><xy>.vdf</i>	Pattern files

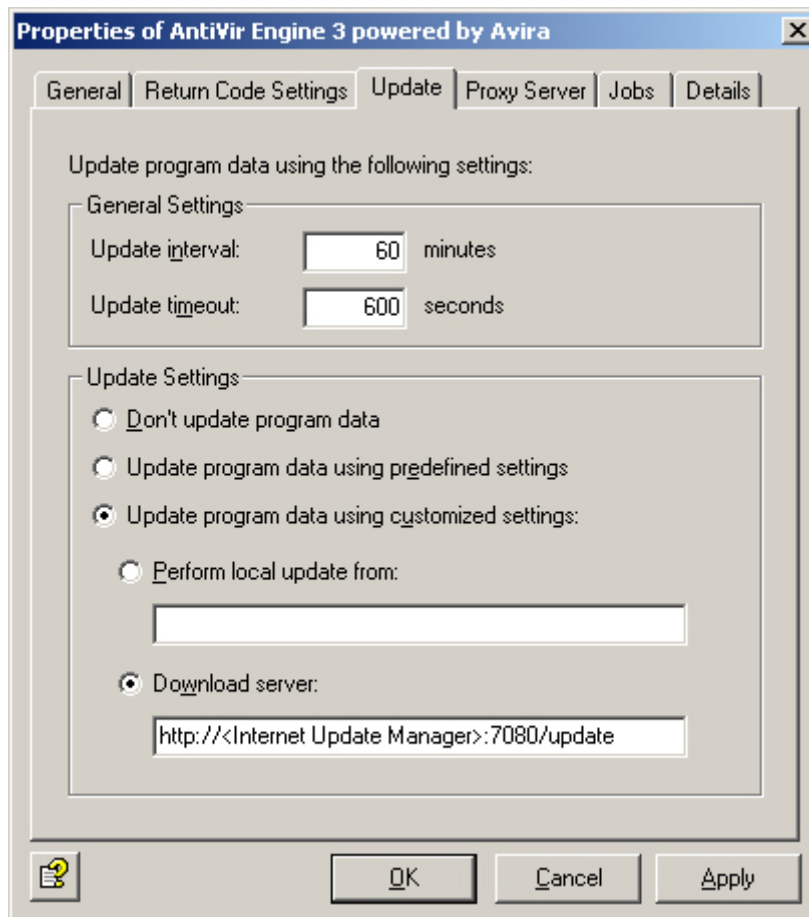
1. The executable file (1) is called by iQ.Suite and then, using the file (2), initiates the execution of the Avira update file (3).
2. This file then uses the configuration files (4) and (5) for downloading, version control and updating
3. Using the configuration file (4), a mirror of the download area is created. Once downloaded, the mirrored update files are temporarily stored in the <iQSuite>\Bin\Savapi\Update directory and extracted to the <iQSuite>\Bin\Savapi\Update\Extract directory.
4. Using the configuration file (5), the mirrored update files are checked against the currently existing files. If the update files are more recent, the new patterns are installed.

Note: The update requires an accessible server environment. You may have to set up a DNS server. A DNS test scenario is described under: [Testing the DNS Configuration](#) on page 11.

Central Update

If you wish to control the updates from a central server, you can set this in the iQ.Suite administration console. A central server downloads the updates from the Internet using the *Avira Internet Update Manager* and makes them available to each of the client computers as web server. The client computers download the updates from the central server rather than directly from the Internet.

Enter the address of the web server in the iQ.Suite administration console: Scan Engines -> *ANTI VIR ENGINE 3 POWERED BY AVIRA* -> *UPDATE TAB* -> *UPDATE PROGRAM DATA USING CUSTOMIZED SETTINGS* -> *DOWNLOAD SERVER*.



Under <Internet Update Manager> enter the IP address of the central web server where the Avira Internet Update Manager is installed. The port number specified here is the Update Manager default port. The proxy server settings are used as set under the **Proxy Server** tab.

Note: Make sure that the *Avira AntiVir Savapi Library v3 (Windows)* product is installed in the Avira Internet Update Manager console.

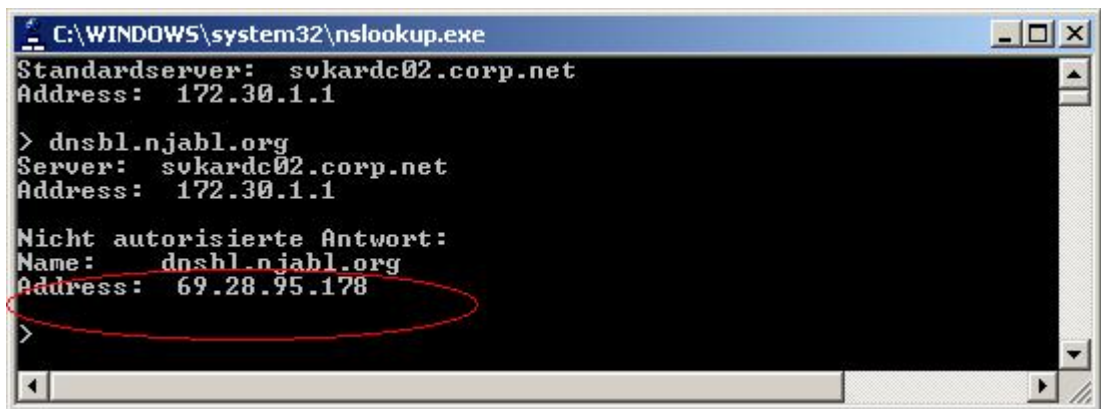
As an alternative to the Avira download server, you can also use a shared directory to exchange the pattern files. Specify this share under *PERFORM LOCAL UPDATE FROM*. The proxy server settings under the **Proxy Server** tab are ignored.

3 Test Scenarios

3.1 Testing the DNS Configuration

To test a DNS environment call the **nslookup.exe** program and proceed as follows:

1. At the console (command prompt) enter “nslookup” and press the ENTER key.
2. Send a DNS request to the domain `dnsbl.njabl.org` (press ENTER).
If an IP address is returned as response, the DNS configuration is correct.
In the example below, the IP address 172.30.1.1 corresponds to a locally configured DNS server:



```
C:\WINDOWS\system32\nslookup.exe
Standardserver: sukardc02.corp.net
Address: 172.30.1.1

> dnsbl.njabl.org
Server: sukardc02.corp.net
Address: 172.30.1.1

Nicht autorisierte Antwort:
Name: dnsbl.njabl.org
Address: 69.28.95.178
>
```

3. If no response is returned, e.g. because no DNS server can be found and addressed, the DNS configuration is wrong. This results in a timeout when the email is processed using SAVAPI3. In environment with high email traffic, this can strongly affect the email processing time and result in major interferences:



```
C:\WINDOWS\system32\nslookup.exe
DNS request timed out.
timeout was 2 seconds.
*** Der Servername für die Adresse 172.30.100.167 konnte nicht gefunden werden:
Timed out
*** Die Standardserver sind nicht verfügbar.
Standardserver: UnKnown
Address: 172.30.100.167

> dnsbl.njabl.org
Server: UnKnown
Address: 172.30.100.167

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Zeitüberschreitung bei Anforderung an UnKnown
>
```

3.2 Testing the Update Process

3.2.1 Procedure under iQ.Suite for Microsoft Exchange

To test the connection to the SAVAPI3 download area, you can use the iQ.Suite Monitor feature in the administration console. Proceed as follows:

- Select *iQ.SUITE MONITOR -> SERVERS -> <SERVER NAME> -> SERVER STATUS*.
- Open the **Test** tab and select the option *Scan Engines/Antispam Update* from the dropdown menu.
- Click “Start”.

iQ.Suite now starts the update process. When completed successfully, an “OK” message is returned. If unsuccessful, the message displays “Error”. The update process is logged in the Event Log. In case of an error, you may have to set the log level higher for troubleshooting purposes.

3.2.2 Procedure under iQ.Suite for Lotus Domino

To send a notification following a successful or unsuccessful update, 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= Each update, 2= Failed updates only
auth-method	Authentication method: User/Password
email-to	Recipient of the notification emails
email-footer	Content of the email footer

iQ.Suite starts the update process. Depending on the configuration, you will be notified of successful or failed updates.

About GROUP Technologies - A Division of GROUP Business Software AG*GROUP's Email, Archiving and Administration Department*

Organizational operations depend on highly-efficient modes of communication. Communication affects – more or less – all business processes. Email is heavily used for communication, in collaboration efforts and as a workflow engine. Email is a process which affects all aspects of internal and external information exchange. Following these facts, email is the number one business critical application and is burdened with internal and external risks, regulations, policies and standards.

GROUP Technologies focuses on delivering a process-controlled, centralized and easy-to-maintain email management solution for the Lotus Domino and the Microsoft Exchange markets.

GROUP Technologies Value Proposition

Expertise: The company is a trusted advisor to its customers in the areas of email security, compliance or IT optimization and is capable of solving any business challenge in these areas through its centralized and rules-based email process management approach.

Unified console/single point of administration: Multi-level anti-virus and anti-spam, automated de-/encryption, rule-enforcement, regulatory enforcement and real time archiving through a single point of administration within the entire organization.

Simplicity: The company's email solution features easy-to-use interfaces and is efficient in solving email challenges. As a server-based solution, client/user interaction is limited and reduced to the absolute necessary minimum input by the email user. The organization-wide implementation for all users is done on the server and is easy to administer through our unified console.

Email as a business process: Company defined processes control email usage ensuring compliance with internal policies as well as regulatory requirements. Simple configuration tools allow the system to easily be adapted to satisfy the demands of growing companies and new regulations that have yet to be envisioned.

GROUP Facts

Customers: GROUP's clients include many well-known companies such as Deutsche Bank, Ernst & Young, Honda, Heineken, Allianz and Miele. More than three million users and 3,000 companies worldwide protect and organize their systems with GROUP Technologies products.

© 2010 GROUP Business Software AG

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments.

The information contained in this document presents the topics from the viewpoint of GROUP Business Software AG at the time of publishing. Since GROUP Business Software AG needs to be able to react to changing market requirements, this is not an obligation for GROUP Business Software AG and GROUP cannot guarantee that the information presented in it is accurate after the publication date.

This document is intended for information purposes only. GROUP Business Software AG does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose.

All the product and company names that appear in this document may be trademarks of their respective owners.

European Headquarters

GROUP Business Software AG

MesseTurm
60308 Frankfurt / Germany
Phone: +49 69 789 8819-0
Fax: +49 69 789 8819-99

North American Headquarters

GROUP Business Software Corporation

40 Wall Street, 33rd Floor
New York, NY 10005 / USA
Phone: +1 212 995-2900
Fax: +1 212 995-2206

Email Main Office

GROUP Technologies

Ottostrasse 4
76227 Karlsruhe / Germany
Phone: +49 721 4901-0
Fax: +49 721 4901-199

UK Office

GROUP Business Software (UK) Ltd.

97 Buttermarket Street
Warrington WA1 2NL / UK
Phone: +44 1925 624950
Fax: +44 1925 240211

info@group-technologies.com
<http://www.group-technologies.com>

