



SASI for iQ.Suite Wall

- iQ.Suite for Exchange/SMTP -

Contents

1 Introduction	2
1.1 Terminology Used With SASI.....	2
1.2 License Requirements	2
1.3 General Features	3
2 Basic Functions	3
2.1 SASI Integration	3
2.2 Spam Recognition.....	4
2.3 Performing Updates	4
3 Update Procedure Details	5
4 Testing Possibilities	6
4.1 Testing the Update Process	6
4.2 Testing the SASI Recognition	7
5 Configuration Options	8
5.1 Configuration: SASI Update Service	8
5.1.1 Connection Settings.....	8
5.1.2 Proxy Settings.....	8
5.1.3 Update Settings	9
5.1.4 Notification Settings	10
6 About GROUP Technologies AG	12

1 Introduction

1.1 Terminology Used With SASI

SASI (**S**ophos **A**nti **S**пам **I**nterface) is an interface available as of iQ.Suite Version 6.0 for Exchange/SMTP that can be used to protect against spam and other junk mail. SASI is used as additional spam criterion in the advanced iQ.Suite spam filtering job.

By simultaneously using

- an anti-spam engine and
- a patterns database used to identify spam mails,

your Exchange/SMTP environment can be comprehensively and effectively protected.

To analyze the e-mails, SASI for iQ.Suite Wall checks them against known patterns of typical spam mails. Located on the server running iQ.Suite, the patterns database is automatically updated at periodic intervals.

The result of this analysis is a value that the advanced spam filtering job uses, among others, to determine the overall spam probability.

1.2 License Requirements

SASI for iQ.Suite Wall for spam protection is an iQ.Suite add-on feature and requires a valid license. This optional license is available for the iQ.Suite Wall module. For details please consult your sales partner.

1.3 General Features

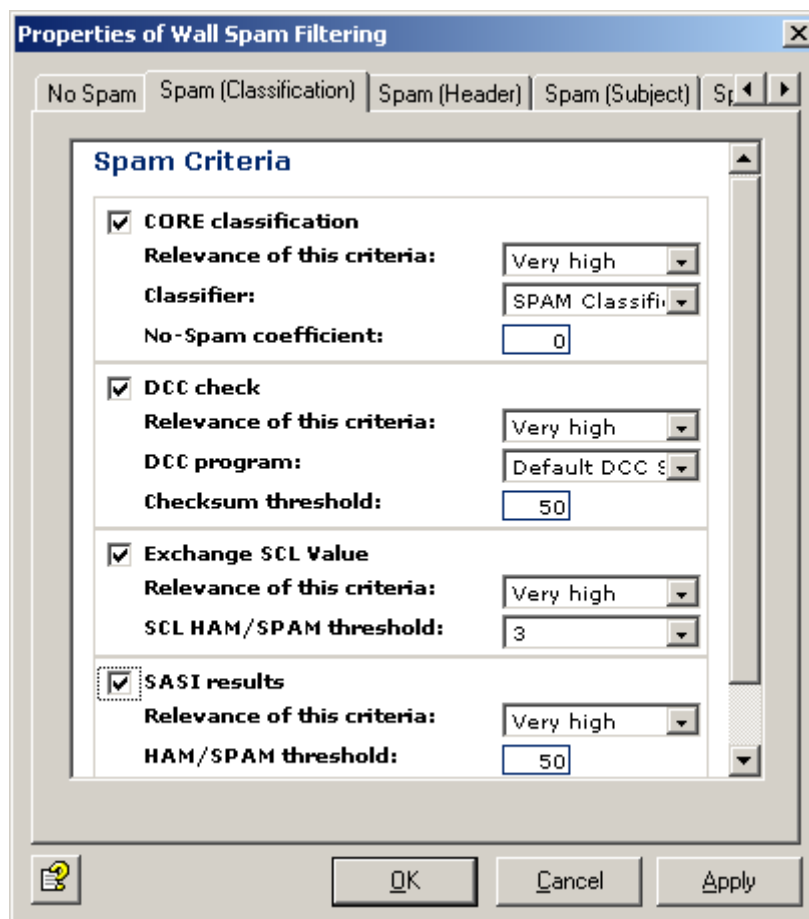
SASI for iQ.Suite Wall provides the following benefits:

- High spam recognition rate
- A near-to-zero rate of “false positives”, i.e. mails wrongly identified as spam
- Fully automatic update of both the anti-spam engine and the patterns, based on standard protocols (HTTP or FTP).

2 Basic Functions

2.1 SASI Integration

SASI for iQ.Suite Wall is integrated into the advanced spam filtering job as a combined criterion and can be enabled in addition to DCC and CORE.



SASI criterion in the advanced spam filtering job

2.2 Spam Recognition

SASI for iQ.Suite Wall analyzes the e-mail header, the body text and any file attachment information. This allows to identify, for instance, spam mails that only contain suspicious PDF attachments. To do so, SASI checks the e-mails against known patterns.

2.3 Performing Updates

As the structural characteristics of spam mails change at a rapid rate, the patterns need to be updated at periodic intervals. This ensures a consistently high recognition rate as well as continuously improved analysis results.

Updates are automatically performed every 60 minutes.

The following components are updated:

- SASI engine (pmx_engine.dll)
- SASI patterns (asdb.antispam and db.summary).

A dedicated download area was set up to this end. From there, both the SASI engine and the patterns are automatically downloaded at runtime.

By default, the HTTP protocol is used for updating (port 80).

As the iQ.Suite installation includes a complete SASI engine, the SASI function can be immediately enabled in the advanced spam filtering job.

During iQ.Suite setup, it is possible to specify proxy server information. These settings are used for the SASI updates via the Internet.

For details on how to change these settings after the installation as well as further configuration options please refer to [Configuration Options](#) on page 8.

3 Update Procedure Details

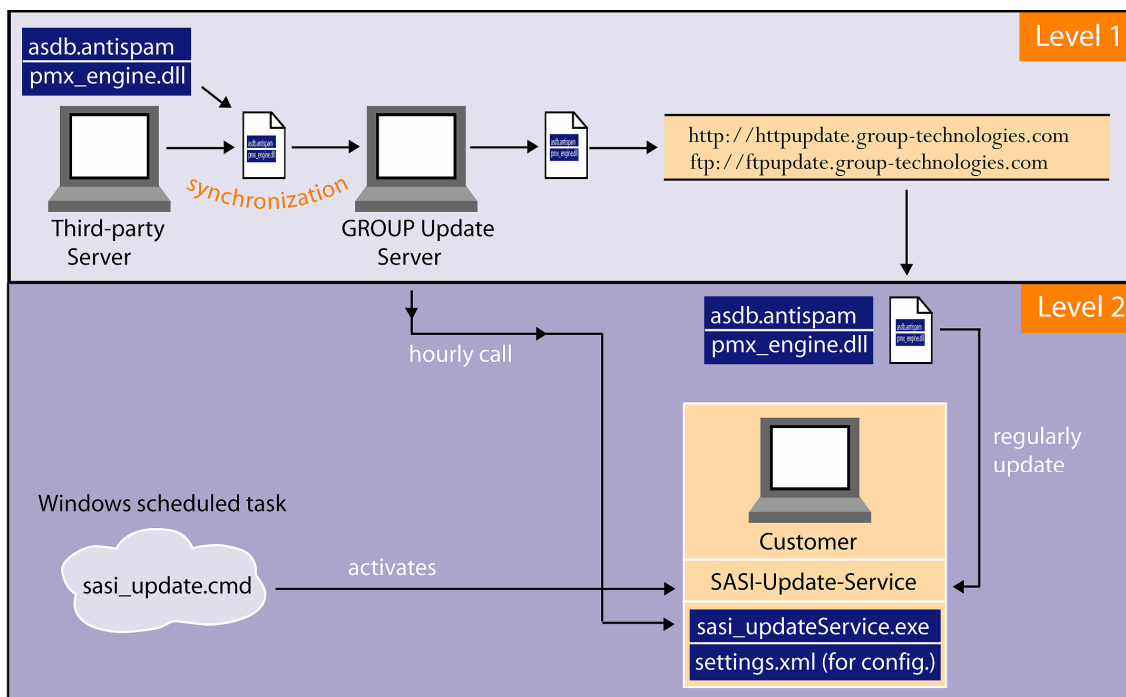
Our download area can be accessed through FTP or HTTP. the following addresses are available to this end:

- <ftp://ftpupdate.group-technologies.com>
- <http://httpupdate.group-technologies.com>

NOTE: To ensure a correct connection, it is recommended to use names rather than IP addresses.

The update is performed by the **sasi_updateService.exe** program.

NOTE: By default, the update is performed every 60 minutes.



During the update, the SASI Update Service stores the temporary files in the <iQSuite>\Bin\SASI\Update\Temp directory. After having downloaded all of the files required, they are unpacked to the <iQSuite>\Bin\SASI\Update\Extract directory.

The SASI Update Service uses the configuration information stored in the **settings.xml** file. For details on how to configure this file, please refer to [Configuration: SASI Update Service](#) on page 8.

Once successfully extracted, the new SASI files are copied to the <iQSuite>\Bin\SASI\ directory, where they are immediately available for iQ.Suite.

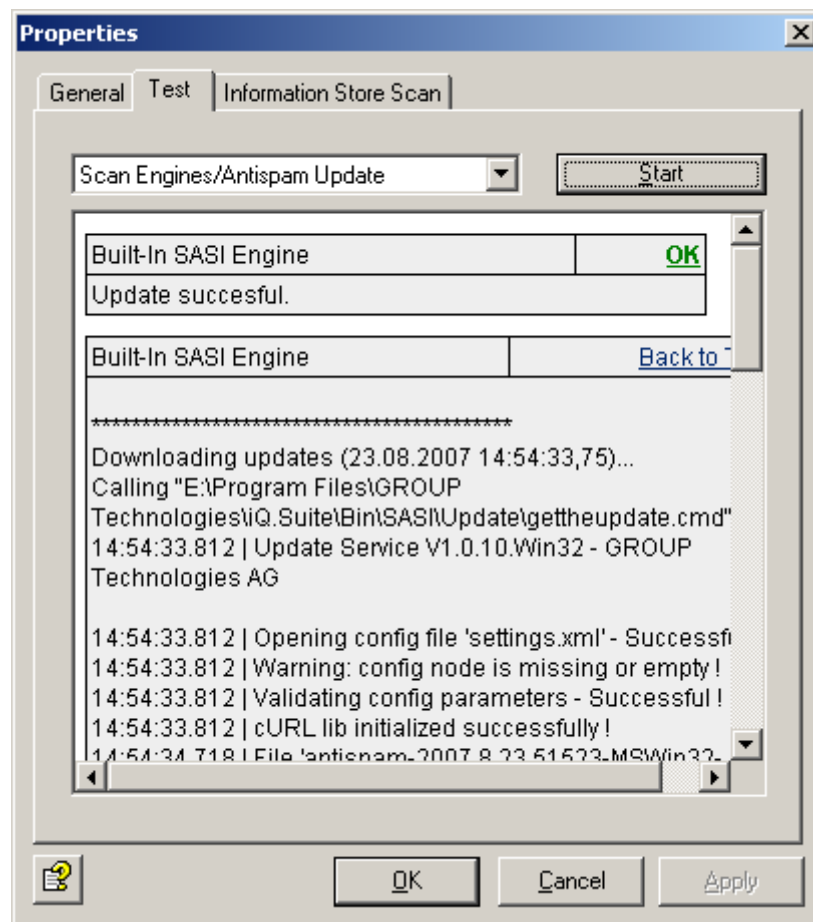
4 Testing Possibilities

4.1 Testing the Update Process

To test the connection to our SASI download area, you can use iQ.Suite Monitor. To do so, proceed as follows:

- Start iQ.Suite Management Console
- Select iQ.Suite Monitor -> Server -> *server name*
- Open the server properties and select the “Test” tab
- From the dropdown menu select “Update virus scanner / anti-spam”.
- Click “Start”.

iQ.Suite now starts the SASI update process with the settings from the settings.xml file. When completed successfully, an “OK” message is returned.



Testing the SASI update

If the test fails, an appropriate error message is displayed.

4.2 Testing the SASI Recognition

- Import test license (...iQ.Suite\License)
- Where required, adjust Settings.xml in the ...iQ.Suite\Bin\SASI\Update directory (proxy, user, password)
- Test pattern update using iQ.Suite Monitor
- Create new quarantine for SASI test
- In the current spam filtering job under Combined Criteria -> Spam (classification), disable the criterion "SASI"
- Duplicate the current spam filtering job
- Place the new job after the current spam filtering job
- In the new job, disable all criteria and enable "SASI"
- Copy e-mails with a medium or high spam probability level to the new SASI test quarantine
- Do NOT enable "Delete e-mails" during the test stage
- Check which e-mails are quarantined by SASI

5 Configuration Options

5.1 Configuration: SASI Update Service

SASI for iQ.Suite Wall uses configuration information from the **settings.xml** file, which is located in the <iQSuite>\Bin\SASI\Update directory.

The necessary settings are pre-configured and can be used immediately after having installed iQ.Suite.

Normally, adjusting the settings.xml file will only be necessary if, for instance, the HTTP connection uses a proxy server.

5.1.1 Connection Settings

The following lines describe the configuration options in the settings.xml file:

Url	<u>http://httpupdate.group-technologies.com</u> (default) <u>ftp://ftpupdate.group-technologies.com</u> <u>\\server\uncpath</u> Address from where the update files are transmitted to the GROUP-Website.
Username	sasi User name for accessing the GROUP download area.
Password	groupsasi Password for accessing the GROUP download area.
Port	80 (default) HTTP port for the connection.
ftp passivePort	[true false] Default: true For FTP mode only. Using the ftp command PORT or. ERPT. The EPRT command allows to specify an extended address for the data connection - EPRT<blank><d><net-prt><d><net-addr><d><tcp-port><d>

5.1.2 Proxy Settings

Proxy enabled	[true false] Default: false Setting made during Setup. Sets whether or not a proxy server is to be used.
----------------------	--

Url	proxy Sets the address of the proxy server. Setting made during Setup.
Port	8080 Sets the port of the proxy server to be used for communication. Setting made during Setup.
Username	proxyuser User name for accessing the proxy server. Setting made during Setup.
Password	proxypassword Password for accessing the proxy server. Setting made during Setup.

5.1.3 Update Settings

Triggerfile	updaterequest.tmp The update only runs if this trigger file exists.
Contentfile	content.txt This file contains all of the SASI files that are available for download on the GROUP website.
SourceDirectory	sasi/win32 Directory checked by the SASI Update Service for new files in the GROUP download area.
FilePattern	antispam-*-MSWin32-x86.zip In the GROUP download area, the SASI Update Service looks for new files with that name.
SourceFileMode	[all newest] Default: newest [all] Download all SASI files from the GROUP download area. [newest] Download the newest files only from the GROUP download area.
WorkingDirectory	Temp Directory where the SASI Update Service stores temporary files.
Cleanup	[true false] Default: true

	[true]	The SASI Update Service deletes old files before running an update.
	[false]	The SASI Update Service does not delete any files before running an update.
TargetFileMode	[copy extract]	
	Default: extract	
	[copy]	Copies the downloaded files to the target directory.
	[extract]	Extracts the downloaded files to the target directory.
TargetDirectory	Extract	
		Directory where the new files are to be copied or extracted to.

5.1.4 Notification Settings

As a general rule, iQ.Suite for Exchange/SMTP informs the Administrator of any errors that occur during the update process. Successful updates are documented in the Windows Event Viewer. Also, the settings.xml file can be used to configure additional notification settings.

Email mode	[off error info all]	
	Default: all	
	[off]	The system does not send any notifications
	[error]	The system sends error notifications only
	[info]	The system sends info notifications only
	[all]	The system sends error and info notifications
		Setting made during Setup.
Host	localhost	
		Address of the SMTP server.
		Setting made during Setup.
Recipient	admin@myserver.de	
		Recipient of the notifications.
		Setting made during Setup.
Sender	SASI-UPDATE	
		Name of the sender of the notifications.
		Setting made during Setup.
Authentication enabled	[true false]	
	Default: false	

	Sets whether or not the SMTP server requires an authentication.
Encoded	[true false] Default: false [true] User name and password contain Base64-coded character strings. [false] User name and password do not contain Base64 Base64-coded character strings.
Username	user@host User name for accessing the SMTP server.
Password	password Password for accessing the SMTP server.
Format mode	[info error] Specifies the beginning of an area in which an error or info notification is defined.
Subject	Sets the content of the Subject line. Using placeholders such as __DATE__, __DOWNLOADS__, __LOG_VIEW__ is possible.
Body	Sets the content of the message. Using placeholders such as __DATE__, __DOWNLOADS__, __LOG_VIEW__ is possible.

6 About GROUP Technologies AG

GROUP Technologies AG is a world leader in E-mail Lifecycle Management. The company's fully integrated iQ.Suite products ensure efficient security and effective organization of e-mail, from encryption, virus protection, and spam filters to e-mail classification and secure archiving.

The iQ.Suite is modular, fully scalable, and offers a high degree of investment security. The modules are completely server-based, can be centrally administered at a low cost, and are available for Lotus Domino, Microsoft Exchange and SMTP platforms.

With the iQ.Suite, companies can reduce costs, optimize the performance of their e-mail environment, and increase productivity. GROUP's clients include many well-known companies such as Deutsche Bank, Ernst & Young, Honda, Heineken, and Miele. More than six million users and 2,000 companies worldwide protect and organize their systems with GROUP Technologies products.

GROUP Technologies AG is headquartered in Karlsruhe. It maintains a subsidiary in the USA, and distributes its products internationally, both directly and through partner companies.

www.group-technologies.com

© 2006 GROUP Technologies

The product descriptions are general and descriptive in nature. They can be interpreted neither as a promise of specific properties nor as a declaration of guarantee or warranty. The specifications and design of our products can be changed at any times without prior notice, especially to keep pace with technical developments.

The information contained in this documentation deals with issues as assessed by GROUP Technologies AG at the time of publication. As GROUP Technologies AG is bound to react to changing market requirements, this document by no means represents an obligation by GROUP Technologies AG and GROUP cannot guarantee the correctness of the information presented in this document after its publication.

This documentation is intended for information purposes only. GROUP Technologies AG hereby excludes any warranty, express or implied, for this document. GROUP Technologies AG is unable to guarantee, either explicitly or tacitly, the quality, execution, standardization or suitability for a specific purpose.

All product or company names in this document may be protected brand names of their respective owners.

GROUP Technologies

Ottostrasse 4

76227 Karlsruhe / Germany

Phone +49(0)721-4901-0

Fax +49(0)721-4901-199

info.de@group-technologies.com

www.group-technologies.com



North American Headquarters

GROUP Technologies

120 Quarry Drive, Suite B214

Milford, MA 01754/USA

Phone +1 508-473-3332

Phone 877-476-8755 (US and Canada)

Fax +1 508-473-9940

info.us@group-technologies.com

www.group-technologies.com