SASI for iQ.Suite Wall

Integration and Configuration for Exchange/SMTP

Document version 2.0

GROUP TECHNOLOGIES

Content

1 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 Eisenach. It maintains a subsidiary in the USA, and distributes its products internationally, both directly and through partner companies.

www.group-technologies.com

2 Introduction

2.1 What is SASI?

SASI (**S**ophos **A**nti **S**pam **I**nterface) is an interface available as of iQ.Suite Version 6.0 for Exchange/SMTP that provides protection against spam and other forms of junk mail. As a spam analyzer of the iQ.Suite Wall module, SASI ideally complements the existing range of iQ.Suite features. By using SASI together with existing spam recognition modules (such as the content analysis using iQ.Suite CORE), your system environment is effectively complemented and optimized. The seamless integration of any existing components already installed, e.g. user quarantine, blacklists/whitelists or notifications, remains unaffected by SASI.

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 mail,

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. The patterns database is kept locally on the server running iQ.Suite. This database is automatically update at periodical intervals.

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

2.2 License Requirements

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

2.3 System Requirements

Using SASI requires a correct DNS environment as well as an open port 53. Without a properly configured DNS environment, timeouts will occur, which could strongly affect the processing of e-mails using SASI. To test DNS for correct configuration, proceed as described under Testing DNS on page **Fehler! Textmarke nicht definiert.**.

2.4 General Features

SASI for iQ.Suite Wall provides the following:

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

3 Basic Functions

3.1 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 other anti-spam modules such as content analysis using CORE.

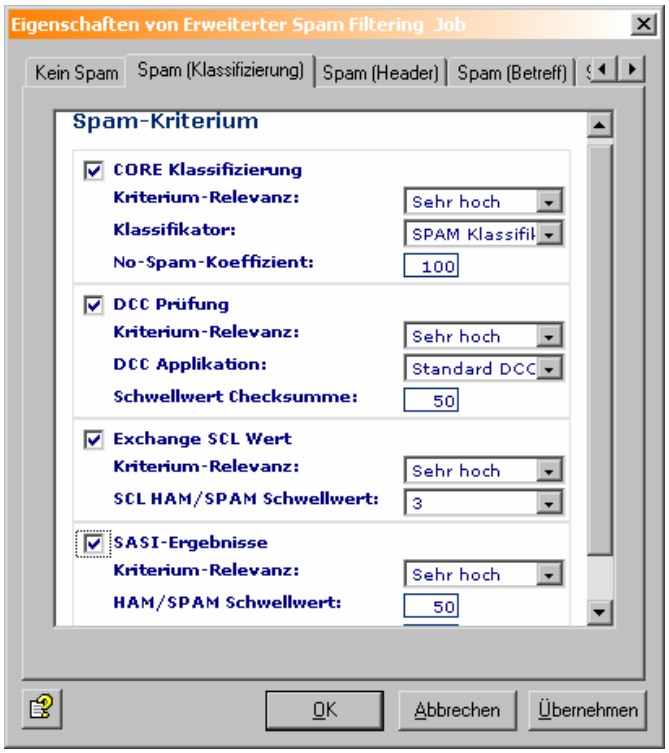


Fig. 1 SASI Criterion in Advanced Spam Filtering Job

3.2 Spam Detection

To identify spam mails, SASI analyzes the e-mail header, the message body and the attachment information. This also allows to identify spam mails with conspicuous PDF attachments. To analyze the e-mails, SASI checks them against known patterns of typical spam mails. The result of this analysis is a percentage that reflects the degree of concordance between the e-mail checked and these patterns. Whenever a preset threshold is exceeded, the e-mail is classified as spam. Spam mails are systematically intercepted and moved to the quarantine database.

3.3 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.

4 Detailed Description of the Update Procedure

Our SASI download area can be accessed via FTP or HTTP, using one of the following addresses:

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

NOTE: To ensure proper connection, use names rather than IP addresses.

NOTE: The update is performed by the **sasi_updateService.exe** program, every 60 minutes by default.

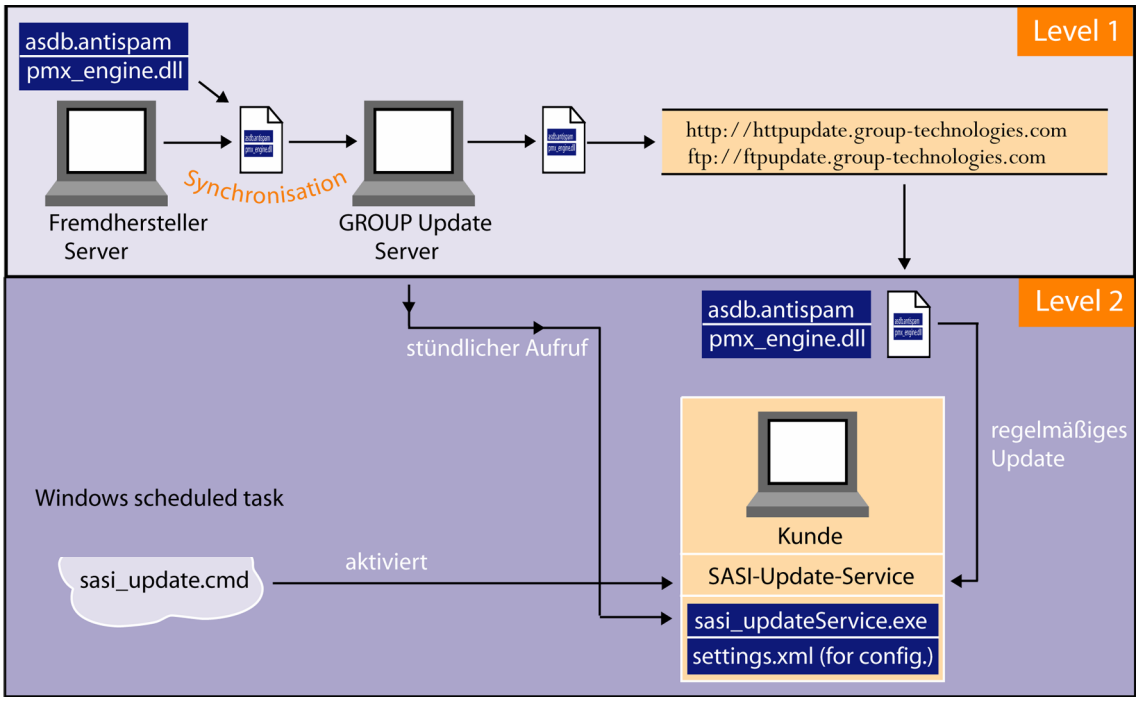


Fig. 2 SASI Update Procedure

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 11.

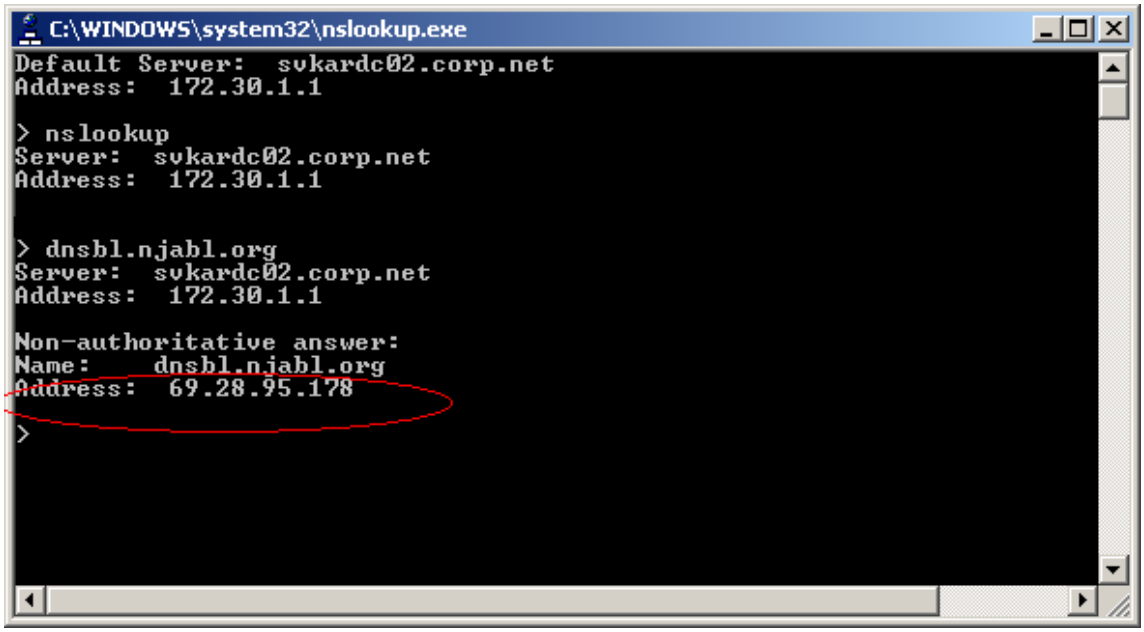
Once successfully extracted, the new SASI files are copied to the <iQSuite>\Bin\SASI\ directory, where they are immediately available for iQ.Suite.

5 Test Scenarios

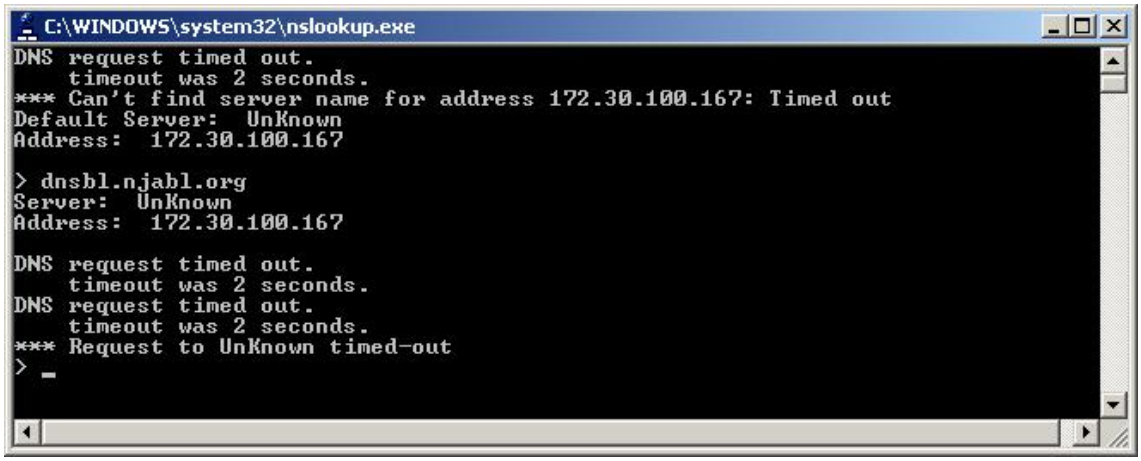
5.1 Testing DNS

To ensure that SASI provides satisfactory results, you need a properly configured DNS environment. To test this DNS environment, call the **nslookup.exe** 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:



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 e-mail is processed using SASI. In environment with high e-mail traffic, this can strongly affect the e-mail processing time and result in major interferences:



5.2 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 the 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:

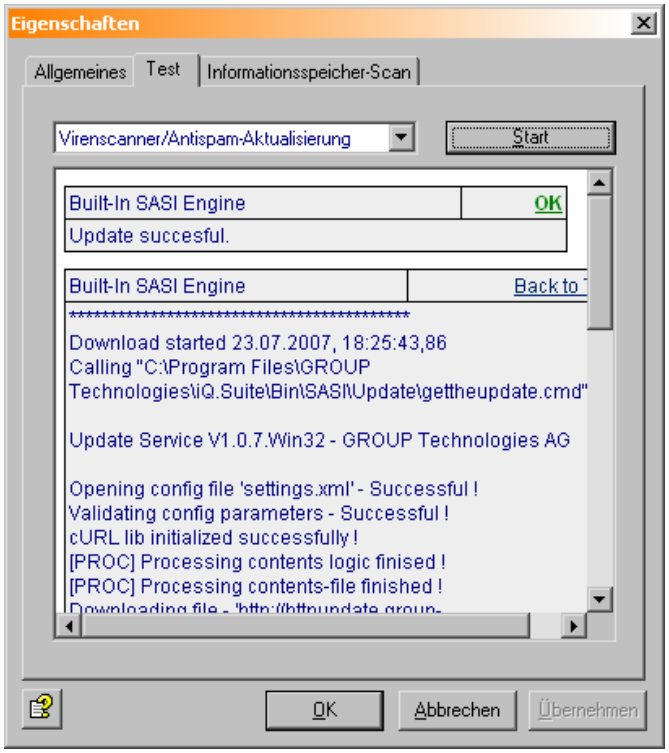


Fig. 3 Testing the SASI Update

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

5.3 Testing the SASI Recognition

To test the results returned by the SASI job proceed as follows:

- Import the test license (...iQ.Suite\License).
- Where required, adjust the settings.xml configuration file in the ...\iQ.Suite\Bin\SASI\Update directory (proxy, user, password).
- Test the pattern update using iQ.Suite Monitor.
- Create a new SASI quarantine for the SASI test.
- In the current spam filtering job under Combined Criteria -> Spam (classification), disable the “SASI” criterion.
- Duplicate the current spam filtering job.
- Place the new job after the current spam filtering job.
- In the new job, disable all of the criteria and enable “SASI”.
- Copy the 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.

6 Configuration Options for the 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 required settings are preconfigured and ready to use after iQ.Suite installation.

Normally, making changes to the **settings.xml** file is only required if, for instance, the HTTP connection uses a proxy server. In this case, the following parameters need to be adjusted:

Proxy enabled	**[true | false]** Default: false Configured during setup. Sets whether or not a proxy server is to be used.
Url	**proxy** Defines the address of the proxy server. Configured during setup.
Port	**8080** Sets the port of the proxy server to be used for communication. Setting made during Setup.
Username	**proxyuser** User name needed to access the proxy server. Configured during setup.
Password	**proxypassword** Password needed to access the proxy server. Configured during setup.
Authentication mode	**[Any | None | Basic | Digest | NTLM]** Default: Any Sets the method to be used for authentication.
Type mode	**[HTTP | SOCKS4 | SOCKS5]** Default: HTTP

All other parameters are described in the comments in the **settings.xml** file. Please contact our Support if you wish to make configuration changes to the file.

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 warrantee. 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 AG
European Headquarters

Hospitalstraße 6
99817 Eisenach
Germany

Head Office:
Fon +49(0)721-4901-0
Fax +49(0)721-4901-199

Hotline
Fon +49(0)721-4901-112
Fax +49(0)721-4901-1922

info@group-technologies.com
hotline@group-technologies.com
http://www.group-technologies.com

GT US, Inc.
North American Headquarters

221 East Main Street
Milford, MA 01757
USA

Fon: +1 508 473-3332
Fon: 877 476-8755 (US and Canada)
Fax: +1 508 473-9940

info@group-technologies.com
us.support@group-technologies.com
http://www.group-technologies.com