SASI for iQ.Suite Wall

Integration and Configuration for Lotus Domino

Document version 2.1

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 10 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.

By simultaneously using

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

your Lotus Domino 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 the analysis is a value used to calculate the spam probability value.

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 consult 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 11.

Under Linux the following packages are required for an automatic update service (regardless of the Domino version used):

- gcc-4.1.1
- glibc-2.3.6

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 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.

To be analyzed, the mails must be available as EML file. To this end, all incoming e-mails are converted to EML format by an iQ.Suite Wall job.

The EML is an e-mail format used to display (multipart) MIME mails. It contains the MIME header including information about:

- the sender
- the recipients
- the servers involved in delivery
- the text and any attachments
- etc.

SASI analyzes the patterns of the EML file and evaluates the degree of concordance. Depending on the spam probability calculated, the following results are returned:

1. [0%, 20%] No spam; the e-mail does not include spam features and is delivered to the recipients.
2. [20%, 50%] In most cases no spam, the e-mail may contain spam features. Wall Jobs can be configured to move these e-mails to quarantine. In the default configuration, these e-mails are delivered.
3. [50%, 80%] Spam mail (quarantine, no delivery); the e-mail does contain spam features and is blocked. The e-mail should be placed in quarantine and might not be delivered to the recipients.
4. [80%, 100%] Spam mail (quarantine or deletion, no delivery); the e-mail does contain spam features and is blocked. The e-mail should be placed in quarantine and might not be delivered to the recipients.

3.2 Technical Overview

3.2.1 Performing Updates

As the structure and design of spam mails change rapidly, the patterns must be updated regularly to ensure high level spam protection and continuously improved analysis results..

Updates need to be run periodically for both

- the SASI engine and
- the SASI data (patterns).

For this purpose, GROUP has set up a synchronized download site, where you can find the current file versions for Windows and Linux environments.

The update of the current file versions is performed in three steps/levels, as described 3-Level Update Scheme on page 8.

NOTE: GROUP customers are only involved with the levels 2 and 3 as they have access to the GROUP server. This server is responsible for file synchronization with an appropriate third-party website. The GROUP download site always provides the most recent file versions.
Also refer to Level 1: Updating the GROUP Download Area on page 8.

The following files are affected by the necessary update from the GROUP website:

a) **asdb.antispam** and **db.summary** (patterns) as well as
b) **pmx_engine.dll** (spam engine).

Normally, the update of the asdb.antispam and db.summary files occurs automatically during operation and the new files can be used immediately after download.

The iQ.Suite setup packages include a preconfigured SASI version, which can be used immediately at the customer site.

NOTE: If you decide to install the iQ.Suite package in a directory other than "iQSuite" bzw. "grptools", you need to adjust the paths in the following file

<iQSuite>\SASI\Update\ntk_sasi_update.cmd (Windows).

<grptools>\SASI\Update\ntk_sasi_update.sh (Linux).

During setup the customer is prompted to set configuration parameters concerning the use of a proxy server and on how to receive update notifications. To configure the SASI standard version, refer to Configuration Options on page 11.

3.2.2 Required Directories

During the update, the engine searches, by default, for preconfigured files under the Domino program directory. The following directories are checked and analyzed:

Under Windows:

a) <iQSuite>\SASI\
b) <iQSuite>\SASI\Update
c) <iQSuite>\SASI\Update\Extract
d) <iQSuite>\SASI\Update\Temp (SASI Update Service)

Under Linux:

a) <grptools>\SASI\
b) <grptools>\SASI\Update
c) <grptools>\SASI\Update\Extract
d) <grptools>\SASI\Update\Temp (SASI Update Service)

NOTE: Please make sure these directories and files are available. Otherwise NO update will occur!

The following files are affected by the necessary update from the GROUP website:

e) **asdb.antispam** and **db.summary** (patterns) as well
f) **pmx_engine.dll** (spam engine).

4 3-Level Update Scheme

4.1 Level 1: Updating the GROUP Download Area

Synchronization with corresponding third-party website

GROUP customers only access the GROUP server. The server is responsible for file synchronization with a corresponding third-party website. The GROUP download site always provides the most recent file versions.

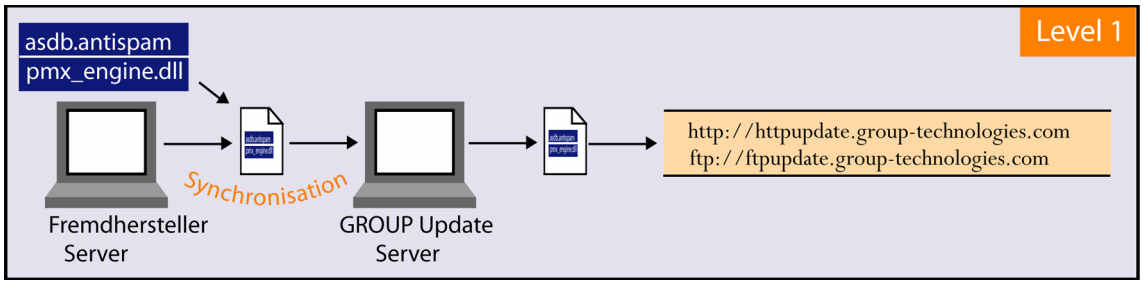


Fig. 1 SASI Update Level 1

Basically, updating the GROUP download area is done by mirroring the corresponding site from the third-party server to the GROUP server. This synchronization is performed on an hourly basis.

4.2 Level 2: Fetching the Files From the GROUP Download Area

SASI Update Service

After having installed iQ.Suite at the customer site, the SASI Update Service will use the GROUP server to fetch the latest updates of all SASI pattern and program files required.

NOTE: The SASI Update Service is available in Windows environments as of Version 10, under Linux as of Version 10.1.

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.

The download from the GROUP server is performed by the **sasi_updateService.exe** program, an iQ.Suite component responsible for the communication with the GROUP update server.

NOTE: To be sure to receive the latest updates, set up hourly calls.

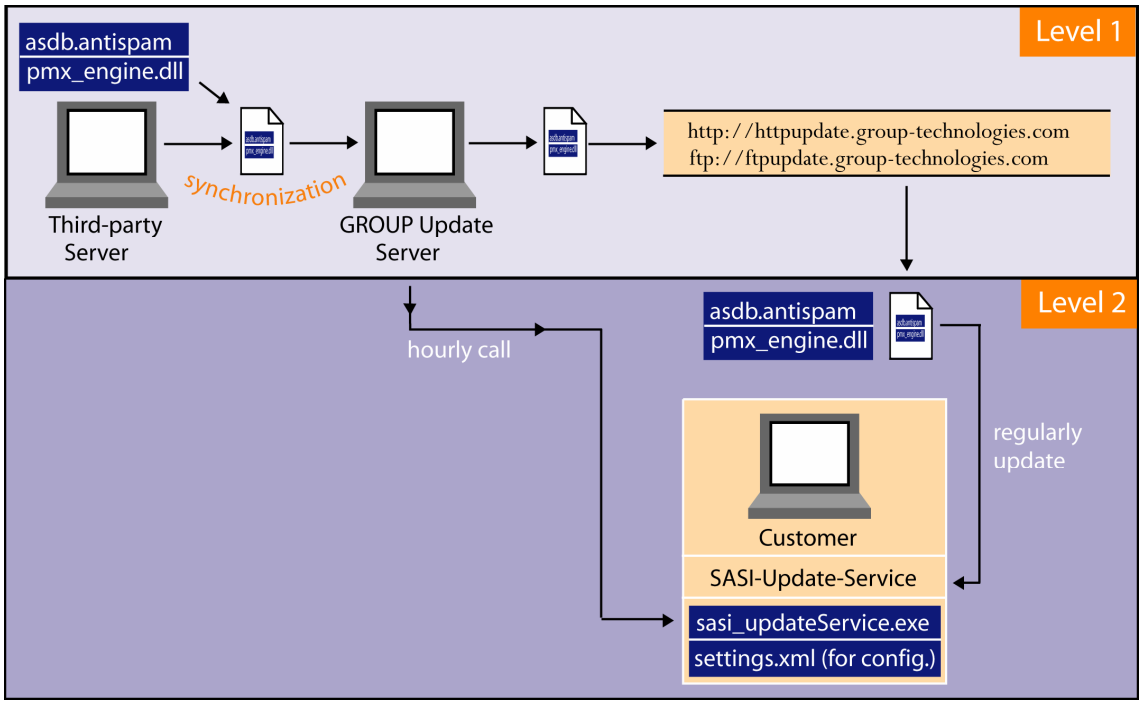


Fig. 2 SASI Update Level 2

While updating files, the SASI Update Service stores temporary files in the <iQSuite> or <grptools> \SASI\Update\Temp directory. After having fetched all of the files needed, they are extracted to the \SASI\Update\Extract directory.

The **settings.xml** file contains the update information required to run the SASI Update Service. To configure this file, refer to Configuration of the SASI Update Service on page 13.

4.3 Level 3: Updating Pattern and Engine Files

Local SASI update

In the third and last step, the local update of the SASI pattern files (asdb.antispam, db.summary) and the engine file (pmx_engine.dll) is performed by a GROUP sandbox implementation. This implementation is configured to check for new files in the <iQSuite> or <grptools> \SASI\Update\Extract directory. Whenever files are found (i.e. new file versions available), the sandbox implementation transfers all necessary files to the SASI folder used by a default SASI spam job or a Wall job.

To run the sandbox implementation, enable the preconfigured default SASI Spam job. The sandbox tries to update the existing pattern/engine files every hour or during a job initialization.

This 3-level update process ensures that our customers are always provided with the latest pattern and program files.

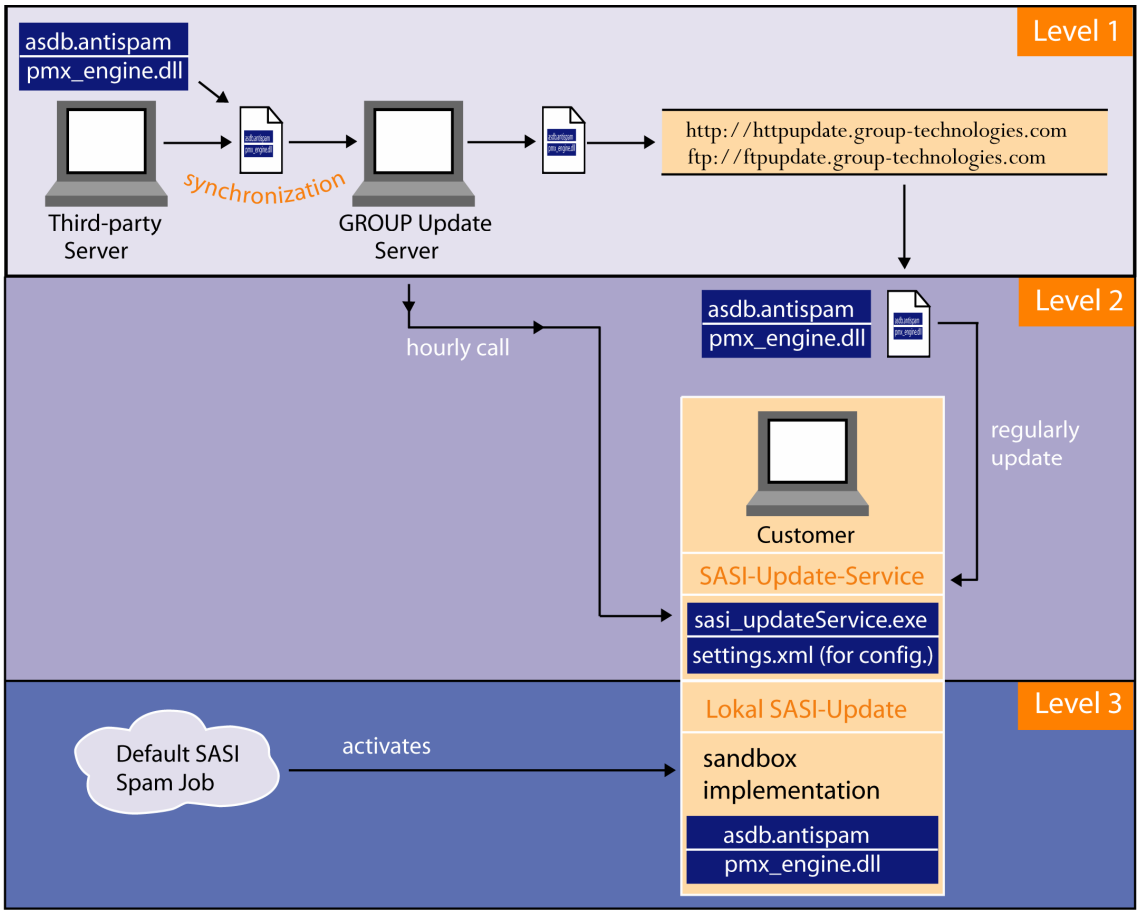


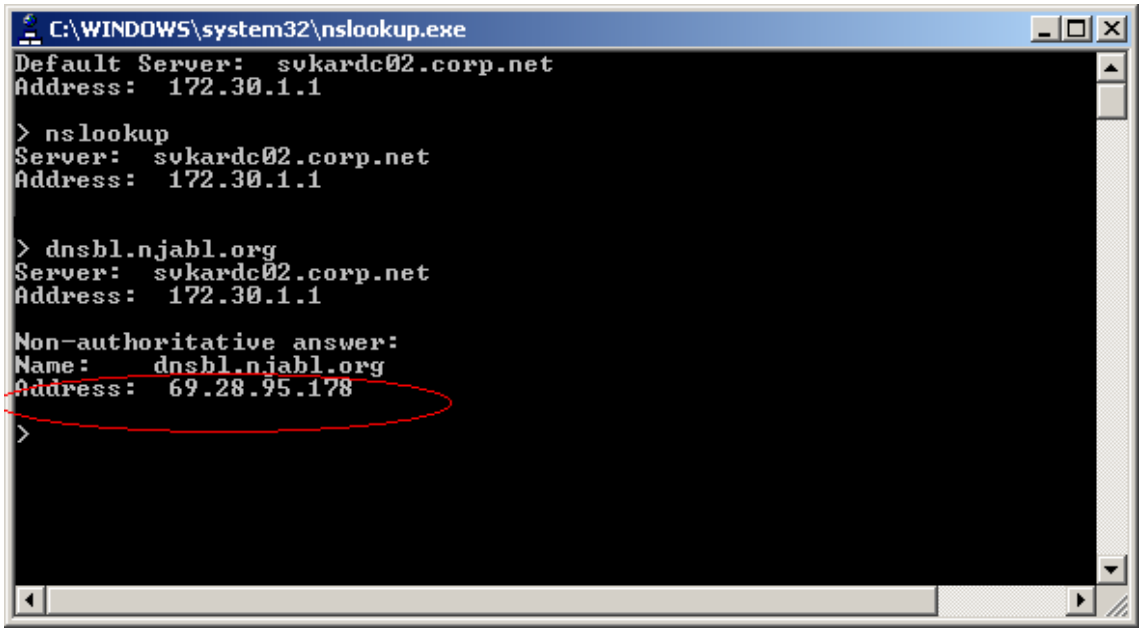
Fig. 3 SASI Update Level 3

5 Test-Scenarios

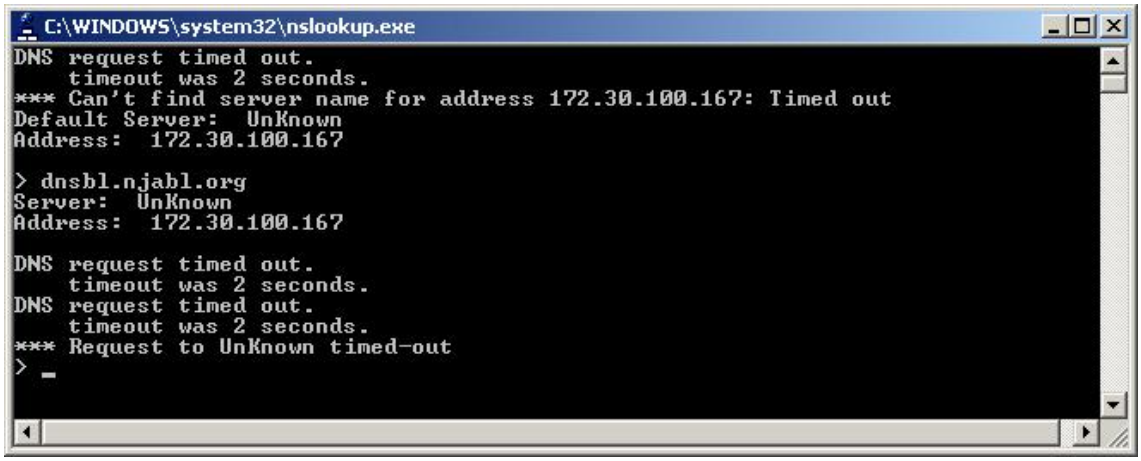
5.1 Testing DNS

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 SASI Job

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

1. Import the test license (...iQ.Suite\License).
2. Where required, adjust the **settings.xml** configuration file in the <iQSuite> or <grptools> \SASI\Update directory, refer to Configuration of the SASI Update Service on page 13.
3. Test the pattern update by double-clicking the update script **start-update.cmd**.
4. Create a new SASI quarantine for the SASI test.
5. In the sample job **Default – Antispam: Check Spam Pattern by SASI** select the newly created SASI quarantine as the database where e-mails classified as spam are to be stored.
6. Enable the sample job and give it the highest priority (to be run before all other spam jobs).
7. Start the SASI test by resending e-mails already stored in a quarantine.
8. Check which e-mails are moved to the new SASI quarantine by SASI.

6 Configuration Options

6.1 Configuration of the SASI Update Service

SASI for iQ.Suite Wall uses configuration information from the **settings.xml** file located in the <iQSuite> or <grptools> \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** Defines the port of the proxy server to be used for communication. Configured 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.

6.2 Configuration of the Local SASI Update

The configuration for the local update is stored in the following files in the directory <iQSuite> or <grptools>.

NOTE: If you decide to install iQ.Suite to a directory other than "iQSuite" or "grptools", you need to adjust the paths in this file manually.

- \SASI**ntk_sasi_ref.cfg**
  Within this file, the following filenames are referred to:
  - asdb.antispam
  - db.summary
  - pmx_engine.dll

  These files are updated whenever a newer version is available. The local update process searches for new files in the \SASI\Extract folder by analyzing the **soap.ntk_sasi.dll.defaults.ini** file and the 'UpdateFrom' parameter.
- \SASI**soap.ntk_sasi.dll.defaults.ini**
  This configuration file contains settings for the sandbox implementation. The following three parameters have an impact on the local update behavior and will be overwritten by every update installation:
  - UpdateInterval=60
    With this setting, an update is run every 60 minutes.
  - UpdateProgram=**.\Update\ntk_sasi_update.cmd** (Windows)
    UpdateProgram=**.\Update\ntk_sasi_update.sh** (Linux)
    This command file initiates the SASI Update Service and the local SASI update process. With every execution a new 'updaterequest.tmp' file is created.
    This file is configured in 'setting.xml' as trigger file and used to determine whether a full update from the GROUP download area is required. The SASI Update Service will only execute an update if this trigger file exists. After having performed a full update, the SASI Update Service deletes the trigger file. A new trigger file is created with the next local SASI update and the SASI Update Service will execute an update the next time it is run.
  - UpdateFrom=**.\Update\Extract**
    This parameter defines the folder where the local update will look for new files that need to be copied to the \SASI folder.
    This folder must be the same as in the SASI Update Service configuration.
- In case it is necessary to change settings or set other parameters than those set in the '\SASI\soap.ntk_sasi.dll.defaults.ini' file, the customer has to enter these changes in the \SASI**soap.ntk_sasi.dll.ini** file.
  This file reflects configuration changes at the customer site and will NOT be overwritten by any update installation.
  As a general rule, if a configuration parameter is set in both files, the entry in the ‚\SASI\soap.ntk_sasi.dll.ini' (changes at customer site) has priority.

© 2008 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 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