



# **SASI**

## **- Integration and Configuration -**

## Inhalt

1	Introduction.....	<b>2</b>
1.1	Definition .....	2
1.2	Licence Requirements .....	2
1.3	General Features .....	2
2	Functional Basics.....	<b>3</b>
2.1	SASI Integration.....	3
2.2	Spam Detection.....	3
2.3	Technical Overview.....	4
2.3.1	To accomplish updates.....	4
2.3.2	Necessary Directories and Folders.....	5
3	3-Level-Update Scheme .....	<b>6</b>
3.1	Level 1: Update of the GROUP Download area .....	6
3.2	Level 2: Receiving files from the GROUP Download area .....	6
3.3	Level 3: Update Pattern and Engine Files.....	8
4	Configuration Options .....	<b>9</b>
4.1	Configuration: SASI-Update-Service.....	9
4.1.1	Connection settings .....	9
4.1.2	Proxy settings .....	10
4.1.3	Update settings.....	10
4.1.4	Notification settings.....	11
4.2	Configuration: Local SASI Update.....	12
5	About GROUP Technologies AG .....	<b>14</b>

## 1 Introduction

### 1.1 Definition

SASI is an **Anti Spam Interface** that is used for protection against spam and junk mails as of iQ.Suite Version 10. It is an additional product besides the automatic spam pattern checking with DCC-Analyzer and the mail content checking with iQ.Suite CORE.

It effectively protects your Lotus Notes/Domino and Exchange environment by using both

- an Anti-Spam engine and
- a pattern database to detect Spam messages.

The idea is to use SASI as an Analyzer in the iQ.Suite Wall for identification of Spam messages. This combines the existing features of the iQ.Suite for Lotus Domino and Exchange with the capabilities of SASI.

SASI is checking mails in text analysis against known so-called “patterns” of common spam mails. Because the senders of SPAM tend to work with mails that are similar in structure and design some kinds of common patterns can be defined.

Incoming mails are checked against these common patterns. The result of this check will be given as a percentage value to indicate the similarity between mail and spam patterns. If a certain threshold is reached, the mail will be declared as Spam mail. Spam mails are blocked and placed into the quarantine database.

### 1.2 Licence Requirements

SASI for spam protection is an additional module within the iQ.Suite. You need to acquire a valid iQ.Suite Wall license. Contact your sales partner for further information.

### 1.3 General Features

SASI guarantees

- high spam detection rates and prevents “false positives” (e-mails incorrectly identified as spam).
- fully-automatic engine and pattern updates through the Internet.
- the support of Proxy authentication.

## 2 Functional Basics

### 2.1 SASI Integration

SASI is implemented as a so called Wall Analyzer. Wall Analyzers are the components within the iQ.Suite where the Spam analysis is processed. As an additional Wall Analyzer, SASI can be integrated easily in existing environments and operates in combination with the existing Spam detection modules without conflict. SASI therefore completes the capabilities of the iQ.Suite modules like DCC and iQ.Suite CORE.

Furthermore all already implemented features like user quarantine, black- and whitelist functionality or notifications are available for the SASI integration initially from the beginning.

### 2.2 Spam Detection

SASI is checking mails in text analysis against known “patterns” of common spam mails. For analysis the mails must be available as EML file to work on. EML is a mail format and is used as a (Multipart-) MIME representation of a mail message. It contains ‘MIME-Header’ information about

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

Incoming mails that are original not available as EML are converted inside the iQ.Suite for further processing. This will be provided by an iQ.Suite Wall job.

SASI analyzes the patterns of the EML and compares the level of compliance. Dependent of the amount of the numeric spam probability, the following results are released:

1. [0%, 20%] good mail; the mail doesn't include spam messages and is delivered to the recipient(s).
2. [20%, 50%] in most cases good mail, the mail may contain spam messages. Wall Jobs can be configured to send these mails to quarantine. The default configuration doesn't quarantine these mails
3. [50%, 80%] spam mail (quarantine, no delivery); the mail does include spam messages and was blocked. The mail should be placed in the quarantine database and might not be delivered to the recipient(s).
4. [80%, 100%] spam mail (quarantine or deletion, no delivery); the mail does include spam messages and was blocked. The mail should be placed in the quarantine database or should be deleted. The mail might not be delivered to the recipient(s).

## 2.3 Technical Overview

### 2.3.1 To accomplish updates

Due to the quick changes in structure and design of spam mails the patterns must be updated regularly to ensure high level spam protection and continuous improved analysis results. The update has to be initiated periodically on both

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

For this purpose a synchronized download site is available by GROUP, where you can find the current file versions for Windows and Linux environments.

The update of the current file versions works as 3-Level-Update as it is mentioned in section [3-Level-Update Scheme](#) on page 6.

**NOTE:** GROUP customers only affect Level 2 and 3 of this scheme and access the GROUP server. This server is responsible for the file synchronization with a corresponding third-party website. The GROUP download site always disposes of the current file versions.

See also [Level 1: Update of the GROUP Download area](#) on page 6.

The necessary update from the GROUP website affects the files:

- a) **asdb.antisipam and db.summary** (for the patterns) and
- b) **pmx\_engine.dll** (for the engine).

Generally the update for the files 'asdb.antisipam' and 'db.summary' occurs automatically during productive operation and can be used directly after download.

The update for the file 'pmx\_engine.dll' has to be initiated by interaction.

**NOTE:** The engine has to be put out of operation. Otherwise the copy won't work and the current version of the files asdb.antisipam and db.summary will not be loaded.

The setup packages of the iQ.Suite contain a preconfigured SASI version and can be used immediately at customer site.

**NOTE:** If you decide not to install the iQ.Suite Package to folder "iQSuite" you have to adjust paths in file "<iQSuite>\SASI\Update\ntk\_sasi\_update.cmd".

During setup the customer will be asked to define configuration parameters concerning the use of a proxy server and on how to receive update notifications. To configure the SASI standard version see chapter [Configuration Options](#) on page 9.

By using a windows operating system you can run an automated SASI-Update-Service periodically (Level 2). Therefore a windows scheduled task has to be configured at customer site. See also [Level 2: Receiving files from the GROUP download area](#) on page 6.

### 2.3.2 Necessary Directories and Folders

During the update the engine searches by default for preconfigured files under `\Lotus\Notes\<iQSuite>\SASI` of the installation directory. The following folders are consulted and analyzed:

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

**NOTE:** Please make sure these directories and files are available. Otherwise no update occurs!

The necessary update from the GROUP website affects the files:

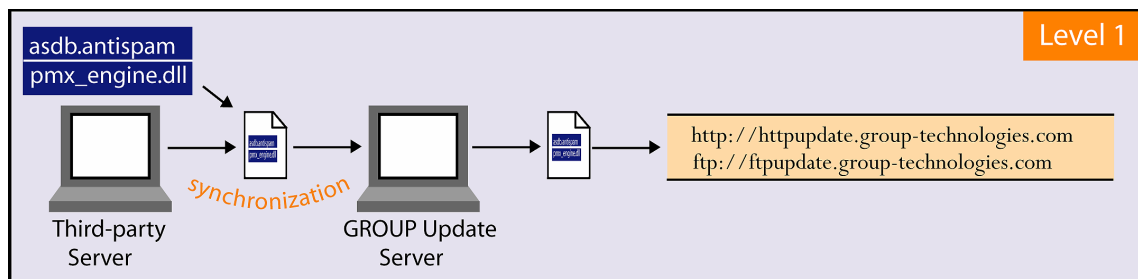
- e) **asdb.antispam** and **db.summary** (for the patterns) and
- f) **pmx\_engine.dll** (for the engine).

### 3 3-Level-Update Scheme

#### 3.1 Level 1: Update of the GROUP Download area

##### Synchronization with corresponding third-party website

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



The update of the GROUP download area is basically done by mirroring the corresponding site from the third-party to the GROUP server. The synchronization is done hourly.

#### 3.2 Level 2: Receiving files from the GROUP Download area

##### SASI-Update-Service

After having installed iQ.Suite at customer site the SASI-Update-Service will use the GROUP server to receive latest updates of all needed SASI pattern and engine files.

**NOTE:** The SASI-Update-Service is only available in Windows environment.

There are two DNS entries to enable customers to access the download area with FTP and HTTP. To be able to distinguish between the two protocols the following DNS are subsidized:

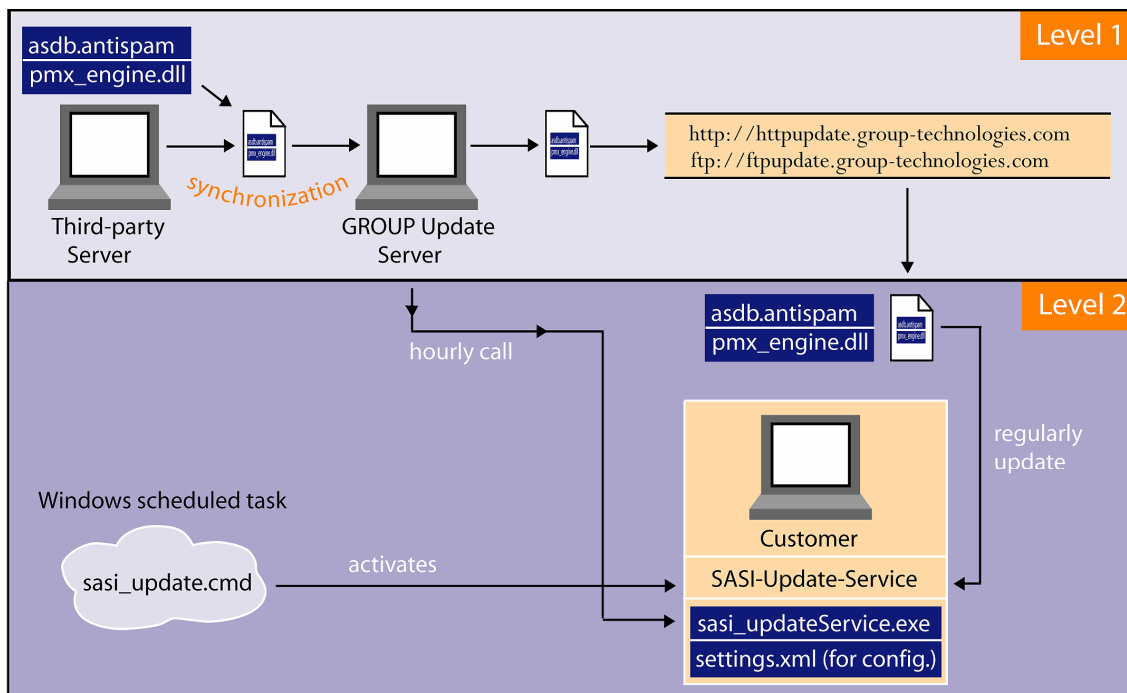
- <ftp://ftpupdate.group-technologies.com>
- <http://httpupdate.group-technologies.com>

At present both servers point to the same IP-address. With increasing load the servers might be either moved or split up.

**NOTE:** To assure the connection, use names instead of IP-addresses.

The download from the GROUP server is managed by the **sasi\_updateService.exe**. This component of the iQ.Suite is responsible for the communication with the GROUP Update server.

**NOTE:** To receive latest updates, set up an hourly call.



**NOTE:** To activate the GROUP Update Service it is necessary to configure a windows scheduled task calling the 'sasi\_update.cmd' periodically.

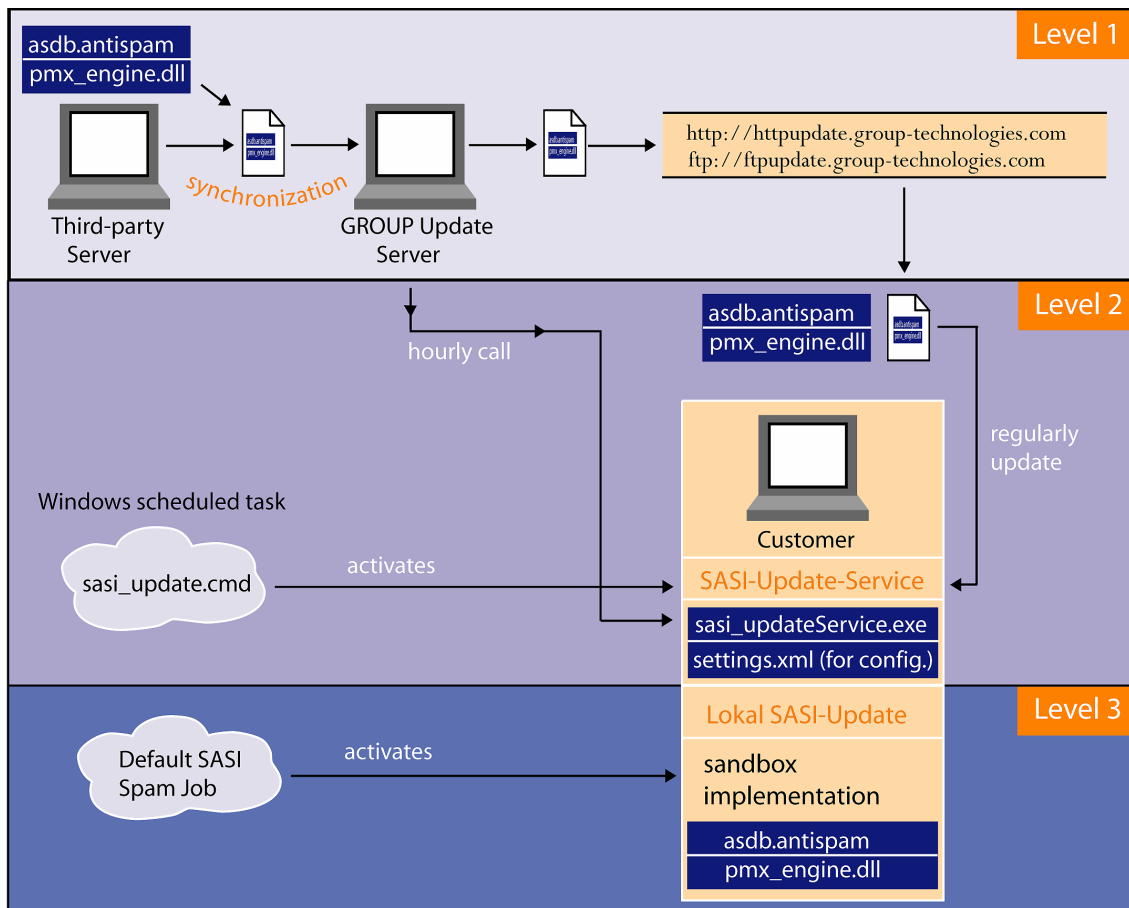
While updating files the SASI-Update-Service stores temporary files in folder <iQSuite>\SASI\Update\Temp. After receiving all necessary files they will be unzipped to folder <iQSuite>\SASI\Update\Extract.

The SASI-Update-Service stores important information in the file **settings.xml**. To configure this file see also [Configuration: SASI-Update-Service](#) on page 9.

### 3.3 Level 3: Update Pattern and Engine Files

#### Local SASI update

Finally the local update of the SASI pattern (asdb.antisipam, db.summary) and engine file (pmx\_engine.dll) is executed by a GROUP sandbox implementation. This implementation is configured to check if new files reside in the folder '<i>iQSuite>\SASI\Update\Extract'. With a positive result (new file versions available) the sandbox implementation transfers all necessary files in the SASI folder that is used by a Default SASI spam job or a Wall job.



To run the sandbox implementation, activate the preconfigured Default SASI Spam Job. The sandbox tries to update the existing pattern and engine files hourly or during a job initialization.

This 3-Level-Update-Process ensures a way to provide our customers with the latest pattern and engine files.

## 4 Configuration Options

### 4.1 Configuration: SASI-Update-Service

The SASI-Update-Service needs some information to be able to work. All needed information is stored in an XML-file called 'settings.xml' under <iQSuite>\SASI\Update'.

Most of the values are already preconfigured and ready to use after iQ.Suite installation. Just configure if you use a proxy server and if the SASI-Update-Service is intended to send notifications about success or failure of updates if you haven't already done this during iQ.Suite setup.

#### 4.1.1 Connection settings

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

<b>Url</b>	<a href="http://httpupdate.group-technologies.com">http://httpupdate.group-technologies.com</a> (default value) <a href="ftp://ftpupdate.group-technologies.com">ftp://ftpupdate.group-technologies.com</a> <a href="#">\\server\uncpath</a> Address where to get the update files at GROUP site.
<b>Username</b>	<b>sasi</b> Username needed to access the download area of GROUP.
<b>Password</b>	<b>groupsasi</b> Password needed to access the download area of GROUP.
<b>useWebDAV</b>	<b>[true   false]</b> When you supply (http/https) url, you can set this parameter to indicate that you are requesting a WebDAV connection to the server.
<b>Port</b>	<b>80</b> (default value) WebDAV or HTTP port for the connection.
<b>ftp passivePort</b>	<b>[true   false]</b> Default value: true Valid only for use of FTP mode. Use ftp 'PORT' command and 'ERPT' command. "The EPRT command allows for the specification of an extended address for the data connection - EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>"

### 4.1.2 Proxy settings

<b>Proxy enabled</b>	<b>[true   false]</b> Default value: false Will be configured during setup. Configures if a proxy server has to be used or not.
<b>Url</b>	<b>proxy</b> Defines the address of the proxy server. Will be configured during setup.
<b>Port</b>	<b>8080</b> Defines the port of the proxy server that has to be used for communication. Will be configured during setup.
<b>Username</b>	<b>proxyuser</b> Username needed to access the proxy server. Will be configured during setup.
<b>Password</b>	<b>proxypassword</b> Password needed to access the proxy server. Will be configured during setup.

### 4.1.3 Update settings

<b>Triggerfile</b>	<b>updaterequest.tmp</b> Update will only be executed if this trigger file exists.
<b>Contentfile</b>	<b>content.txt</b> This file contains all SASI files available for download at GROUP site.
<b>SourceDirectory</b>	<b>sasi/win32</b> Folder where SASI-Update-Service is looking for new files at the download area of GROUP.
<b>FilePattern</b>	<b>antispam-*-MSWin32-x86.zip</b> SASI-Update-Service will look for files with this name when searching for new files in the download area of GROUP.
<b>SourceFileMode</b>	<b>[all   newest]</b> Default value: newest [all]            receive all SASI files from the download area of GROUP. [newest]       receive only the newest files from the download area of GROUP.

<b>WorkingDirectory</b>	<b>Temp</b> Folder where SASI-Update-Service stores temporary files.
<b>Cleanup</b>	<b>[true   false]</b> Default value: true [true] SASI-Update-Service will delete old files before executing an update. [false] SASI-Update-Service will not delete old files before executing an update.
<b>TargetFileMode</b>	<b>[copy   extract]</b> Default value: extract [copy] Copies the downloaded files to the target directory. [extract] extracts the downloaded files to the target directory.
<b>TargetDirectory</b>	<b>Extract</b> Folder where new files will be extracted / copied to.

#### 4.1.4 Notification settings

<b>Email mode</b>	<b>[off   error   info   all]</b> Default value: all [off] no notifications will be sent [error] only error notifications will be sent [info] only info notifications will be sent [all] error and info notifications will be sent Will be configured during setup.
<b>Host</b>	<b>localhost</b> The address of the SMTP server. Will be configured during setup.
<b>Recipient</b>	<b>admin@myserver.de</b> The recipient of the notifications. Will be configured during setup.
<b>Sender</b>	<b>SASI-UPDATE</b> The name of the notification sender. Will be configured during setup.
<b>Authentication enabled</b>	<b>[true   false]</b> Default value: false Defines if authentication for SMTP server is needed.

<b>Encoded</b>	<b>[true   false]</b> Default value: false [true] Username and password contain Base64 encoded strings. [false] Username and password don't contain Base64 encoded strings.
<b>Username</b>	<b>user@host</b> Username needed to access the SMTP server.
<b>Password</b>	<b>password</b> Password needed to access the SMTP server.
<b>Format mode</b>	<b>[info   error]</b> Identifies areas to define the contents of error or info notifications.
<b>Subject</b>	Defines the content of the subject. Placeholders like <code>__DATE__</code> , <code>__DOWNLOADS__</code> , <code>__LOG_VIEW__</code> can be used.
<b>Body</b>	Defines the content of the body. Placeholders like <code>__DATE__</code> , <code>__DOWNLOADS__</code> , <code>__LOG_VIEW__</code> can be used.

## 4.2 Configuration: Local SASI Update

The configuration for the local update is contained in the following files:

- **<iQSuite>\SASI\ntk\_sasi\_ref.cfg**  
Within this file the following filenames are listed:
  - asdb.antispam
  - db.summary
  - pmx\_engine.dllThese files will be updated if a newer version is available. The local update process searches for new files in the folder `<iQSuite>\SASI\Extract` by analyzing the file 'soap.ntk\_sasi.dll.defaults.ini' with the parameter 'UpdateFrom'.
- **<iQSuite>\SASI\soap.ntk\_sasi.dll.defaults.ini**  
This configuration file includes settings for the sandbox implementation. The following three parameters influence the local update behavior and will be overwritten by every update installation:
  - UpdateInterval=60  
This parameter performs an update every 60 minutes.

- UpdateProgram=.\Update\ntk\_sasi\_update.cmd

This command file initiates the local SASI update process. With every execution a new file 'updaterequest.tmp' is created.

This file is configured in 'setting.xml' as trigger file and is used to detect if a full update from the GROUP download area is necessary. The SASI-Update-Service will only execute an Update if this trigger file exists. After having performed a full update the SASI-Update-Service will delete the trigger file. With the next local SASI update a new trigger file is created and the SASI-Update-Service will execute an update the next time it runs.

**NOTE: If you decided to install the iQ.Suite to another folder than "iQSuite" you have to adjust paths inside of this file manually.**

- UpdateFrom=.\Update\Extract

This parameter defines the folder where the local update is looking for new files that have to be copied to the folder <iQSuite>\SASI.

This folder has to be the same as in the configuration of the SASI-Update-Service.

- If there is a need to configure other or changed parameters than given in file '<iQSuite>\SASI\soap.ntk\_sasi.dll.defaults.ini' the customer has to configure these changes in file <iQSuite>\SASI\soap.ntk\_sasi.dll.ini.

This file reflects configuration changes at customer site and will never be overwritten by an update installation.

If a configuration parameter is given in both files the entry in file

'<iQSuite>\SASI\soap.ntk\_sasi.dll.ini' will be used to consider changes at customer site.

## 5 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](http://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](mailto:info.de@group-technologies.com)

[www.group-technologies.com](http://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](mailto:info.us@group-technologies.com)

[www.group-technologies.com](http://www.group-technologies.com)