# GBS

# Whitepaper

# iQ.Suite for Exchange/SMTP

- Comprehensive email management -

*Expertise matters*

**Contents**

*Whitepaper*

# 1    Summary

The use of email traffic has experienced explosive growth in recent years, having become an indispensable element of many business processes. The possibility of attaching files to email is also being made increasing use of. iQ.Suite for Exchange from GBS Software provides a solution to security, organization and availability issues in corporate communications structures.

GBS Software specializes in email security solutions. Its extensive experience in the fields of messaging and groupware guarantees proven, solid products. With its iQ.Suite, GROUP provides a complete email management package that protects email systems from the wide range of risks inherent in modern communications technology. iQ.Suite is available for Microsoft Exchange, SMTP Gateways and IBM Notes/Domino.

Thanks to its modular architecture, the products can be scaled and used in any combination: you simply choose the products you require, adding further components as the need arises.

All products use a common, rule-based security concept. Grouping functions together provides optimum performance and security. User-definable notification texts for senders, recipients and administrators provide transparency. All products are managed centrally using the Microsoft Management Console (MMC). Common logs, statistics and fault reports reduce administration costs.

iQ.Suite is installed on the Exchange server, where it monitors and controls all corporate email traffic (inbound, outbound and internal). It is user-configured to handle email according to corporate policies.
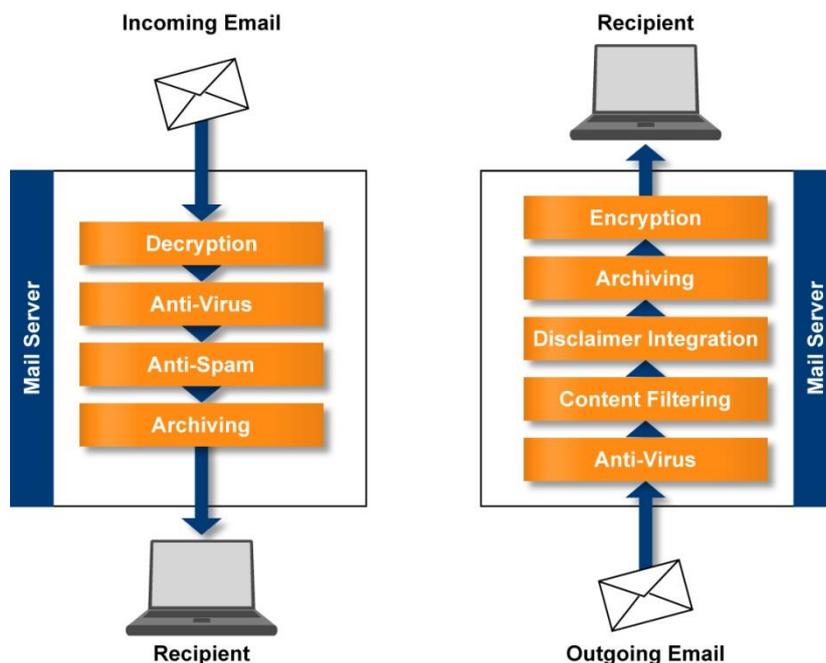
Other software publishers' products – such as virus scanners – can be incorporated in iQ.Suite to further tailor the handling of information exchange and provide effective, efficient network protection. In addition, iQ.Suite can scan email traffic for undesirable content, making it an ideal anti-spam tool.

This whitepaper describes the architecture and the function principle of iQ.Suite. It is aimed at administrators and decision-makers.

# 2    The Product's Architecture

iQ.Suite for Exchange comprises three main components:

- iQ.Suite Console

- iQ.Suite Server

- iQ.Suite Configuration

Each of these is described in detail below.

## 2.1    iQ.Suite Console

iQ.Suite Console is the user interface with which iQ.Suite is configured and managed. Implemented as a snap-in for the Microsoft Management Console (MMC), you can use iQ.Suite Console to manage both individual Exchange servers with installed iQ.Suite and whole iQ.Suite server families. Especially in multi-server environments, this simplifies routine management. iQ.Suite Console provides administrators with access to all required configuration information and to the iQ.Suite servers' quarantines.

The configuration component and the quarantine area are accessed in two ways:

- Standard Windows file access

  The iQ.Suite configuration settings are accessed through Windows file access. The iQ.Suite configuration file can be available locally or accessible on a Universal Naming Convention (UNC) path.

- Access through Simple Object Access Protocol (SOAP) and Secure Socket Layer (SSL)

  The quarantine areas are accessed with SOAP and SSL. The SOAP protocol offers simple, effective communication, but, on its own, does not fulfil the security requirements of iQ.Suite. SSL is therefore used to encrypt the communications channel. The required components are included with the package.

iQ.Suite Console supports the following operating modes:

- Local Administration

  In Local Administration mode, iQ.Suite Console is run directly on the Exchange server on which the iQ.Suite components are installed. This mode is used in smaller networks and for managing the server locally.

- Remote Administration

  In Remote Administration mode, iQ.Suite Console runs on a client operating system and configures and manages iQ.Suite by accessing one or more Exchange servers. Remote Administration is useful for central management in multi-server environments.

## 2.2    iQ.Suite Server

If iQ.Suite Console is the cockpit of iQ.Suite, iQ.Suite Server is its engine. This component carries out the functions and processes of iQ.Suite that run only on the Exchange server. The iQ.Suite Server component can be installed on an Exchange server, or a front-end or back-end server. iQ.Suite Server consists of Grabber and Service as well as the Quarantine and Unpacker modules.

### 2.2.1    iQ.Suite Grabber

The Grabber scans all messages, schedule queries, etc. sent, received or routed by the Exchange server. From Exchange 2000, Microsoft uses the Simple Mail Transport Protocol (SMTP) for transporting email, schedule queries, etc. The entire email traffic – inbound, outbound and internal – is routed through the Advanced Queue, an element of this transport protocol.

Acting as an event sink, iQ.Suite Grabber monitors the mail traffic in the Advanced Queue, for which it is registered in three locations in the Advanced Queue:

- OnSubmission

- OnPreCategorize

- OnPostCategorize

Internal Exchange information, such as replication notifications, are identified as such by the Grabber and returned unchanged to the Exchange system.

The Grabber places all messages to be processed into the iQ.Suite in-queue. Located in the `..\Grpdata\InQ` directory, the original messages are copied here as text files together with a Grabber-generated XML file for each message, which contains additional information, such as SMTP header details.

Here is an example for such a file pair:

- **2C4A14A23BD144B3ACE09E6BE2D49603000.txt**

  (contains the original message)

- **2C4A14A23BD144B3ACE09E6BE2D49603000.xml**

  (contains the additional information)

As soon as iQ.Suite Grabber is installed, all messages are copied into the iQ.Suite in-queue, from where their further processing is managed by iQ.Suite Service. If the Service has not been started, the messages, including the XML files, are buffered in the in-queue until iQ.Suite Service is running again and processing continues.

### 2.2.2 iQ.Suite Service – The Enterprise Message Handler (EMH)

iQ.Suite Service is implemented as a Windows service and runs permanently in the background. To query the Active Directory, it needs the Windows Management Instrumentation (WMI) service. On Windows servers, this service is installed and activated by default.

As soon as iQ.Suite Service receives mail from iQ.Suite Grabber, it monitors and controls all further processing throughout iQ.Suite. iQ.Suite Service has access to all process information it needs. The most important of this is:

- The configured iQ.Suite jobs
  for example for virus scanning, content checking or address filtering

- The installed iQ.Suite licence, which specifies the available modules, such as
  iQ.Suite Watchdog, iQ.Suite Wall, or iQ.Suite Trailer

- The Active Directory

- The iQ.Suite quarantine

Using this information, it scans messages for viruses, identifies and quarantines spam and adds legal liability disclaimers.

Having finished with a message, iQ.Suite Service passes it back to the Exchange server. It does that by moving the message into the Exchange pickup directory, where the Exchange server can continue processing it.

Only when iQ.Suite Server has successfully finished processing a message is it delivered to its recipient.

### 2.2.3 iQ.Suite Quarantine

One possible solution is to intercept undesired emails on the server and copy them to the iQ.Suite quarantine to prevent them reaching their intended recipients. A default quarantine is set up during installation on each iQ.Suite server. The administrator can set up additional quarantines.

An iQ.Suite quarantine consists of:

- a quarantine directory on the Exchange server (...\GrpData\Quarantine\Default-Quarantine),

- the messages copied into the quarantine,

- a quarantine database in Access format (**LocIdxDB.mdb**)

For each message placed in quarantine, iQ.Suite automatically generates an entry in the quarantine database.

Only authorized people can access the iQ.Suite quarantine. Windows user rights for the iQ.Suite quarantine can be assigned on each server. The `...\Program Files\GROUP Technologies\iQ.Suite\Appdata` directory contains the **access.acl** file, which is the iQ.Suite

quarantines on this server. Users or groups with read access to this file can access the iQ.Suite quarantines. Access rights are checked by the iQ.Suite Service module.

For a successful access, the following conditions must be fulfilled:

- The iQ.Suite Service module is running

- The communications port (default: 8008) is available

- The user has the required Windows user rights

Within a quarantine, you can filter messages according to various selection criteria.

### 2.2.4   iQ.Suite Unpacker

To ensure comprehensive email security, archived files, for example in zip-format, must also be scanned for undesired content. This task is performed by iQ.Suite Unpacker, which can be used in the following job types:

- iQ.Suite Watchdog Virus Scanning

- iQ.Suite Watchdog Attachment Filtering

- iQ.Suite Watchdog Attachment/Size Filtering

- iQ.Suite Wall Content Filtering

The following archive formats are supported:

- ACE

- ARJ, self-extracting ARJ

- CAB

- GZIP

- LZH

- RAR

- TAR

- TGZ

- UUEncoded

- ZIP, self-extracting ZIP

- ZOO

## 2.3   iQ.Suite Configuration

All information required to run iQ.Suite is saved in the iQ.Suite configuration file, **configdata.xml**.

The structure of this file is similar to that of a database: various entries exist for each configuration area. Because all configuration information is contained in a single file, it can be easily distributed and backed up. If you have a problem with your configuration, you can send the **configdata.xml** file to the GROUP support team.

Both iQ.Suite Server and iQ.Suite Console must have access to the configuration data. iQ.Suite Server needs it, for example, for information about the iQ.Suite jobs to carry out. iQ.Suite Console is used to change the configuration. The iQ.Suite configuration file can be placed in a local directory or on a shared network path.

The configuration file iQ.Suite Console or iQ.Suite Server uses is specified with an entry in the Windows Registry (see section 8). The path to the iQ.Suite configuration file is specified in the format `C:\...` or as UNC path (`\\Servername\Share\configdata.xml`).

If the specified iQ.Suite configuration file is not available, iQ.Suite uses the "last known good" configuration, which is logged in the Windows events log. This is saved locally for each server (`... Prgram files\GROUP Technologies\iQ.Suite\Appdata\LastConfig.xml`) and is updated whenever the active iQ.Suite configuration is changed and access from the configuration file to the last know good configuration is possible.

# 3 Message Processing Sequence

As described in section 2.2, iQ.Suite monitors the email traffic in the Exchange SMTP Advanced Queue. The illustration below shows the processing sequence of an email by iQ.Suite.



iQ.Suite Architecture
for Microsoft Exchange, SMTP Gateway
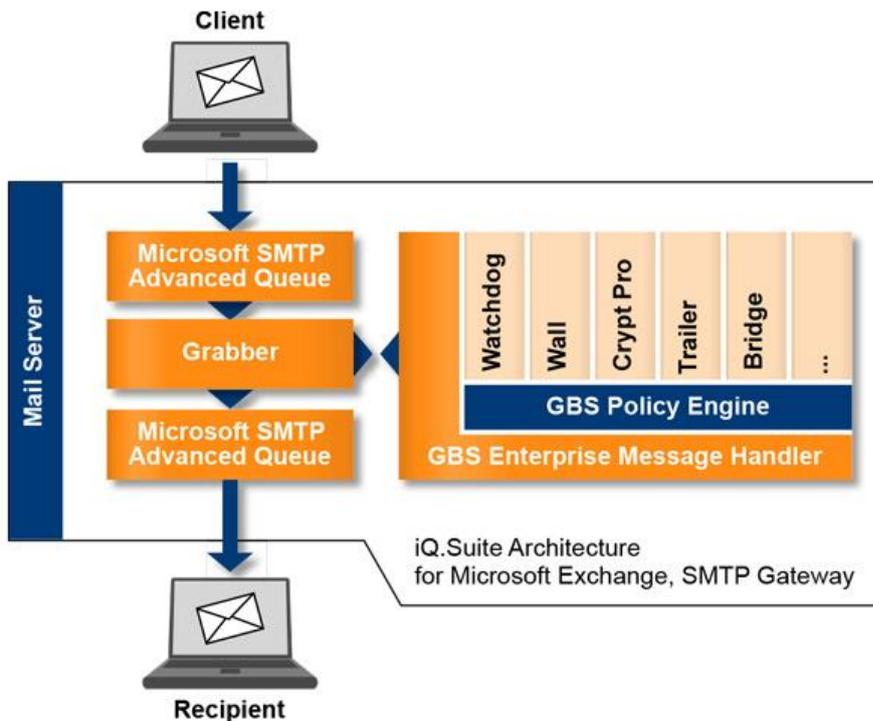
1. An email message arrives at the server.

2. The Grabber intercepts the message from the SMTP advanced queue and places it in a special folder.

3. The Enterprise Message Handler (EMH) [= iQ.Suite Service] retrieves the message from this folder.

4. Based on the configuration settings, the EMH checks whether the message is to be processed by iQ.Suite. If it is not, the message is immediately returned to the SMTP advanced queue.

5. Messages to be processed are dealt with as specified in the configuration settings (jobs by priority).

6. Having fully processed the message, the EMH releases it and makes it available to the Exchange server.

## 3.1   The Active Directory

iQ.Suite does not make any changes to the Active Directory, but does read information from it.

- ■ When it is started, iQ.Suite Service polls the available Global Catalogue server, which is used, for example for resolving addresses in distribution lists during email processing.

- ■ iQ.Suite Console uses the Active Directory to select sender/recipient conditions.

- ■ With iQ.Suite Trailer, sender details can be incorporated in outbound messages. iQ.Suite uses the Active Directory for this information .

If an Active Directory is not available – for example because the corresponding ports are not open – an LDIF file can be used, which is, for example, created through an LDAP export from an Active Directory, an Exchange 5.5 user directory or a Notes Name and Address Book (NAB).

# 4   Structure of iQ.Suite Console in Detail

The user interface of iQ.Suite Console is split into three areas, each of which contains various indication and control elements.

- ■ Basic Configuration (contains basic information, for example about scan engines and servers)

- ■ Policy Configuration (lists the iQ.Suite jobs)

- ■ iQ.Suite Monitor (provides access to the iQ.Suite quarantines and bad mail areas)

The three sections are described in more detail below.

## 4.1   Basic Configuration of iQ.Suite Servers

The Basic Configuration section contains all basic information needed by iQ.Suite to provide a secure Exchange environment. This includes the management of all folders, the dictionaries for content checking, the notification and job templates, the fingerprints and the scan engine. In addition, the settings for the iQ.Suite servers are made here. They are described in more detail below.

The Basic Configuration section for the iQ.Suite servers lists the servers that have iQ.Suite installed. The settings that apply to all servers working with the current iQ.Suite configuration can be accessed through the Properties menu. The following settings can be made:

- ■ Settings for archive files

  To prevent unpacked files using up too much disk space, an upper limit can be specified. By default, this value is set to 300 MB. This setting is especially relevant to protect against Zip of Death attacks, which expand archives of just a few kilobytes to take up several gigabytes of disk space.

■ The unpacking depth of archive files is also limited. Archive files can be nested, i.e. contain archive files, which in turn contain further archive files, and so on. Unpacking these files can cause 100 percent utilization of server resources. To prevent this, unpacking is limited by default to a nesting depth of five. Archive files exceeding this limit are classed as bad mail and are placed in the bad mail folder.

■ Communication settings

To communicate with the iQ.Suite quarantines, iQ.Suite Console uses SOAP and SSL. By default, communication takes place through port 8008, although another port can be selected. In that case, all accessing consoles must be configured to access the new port.
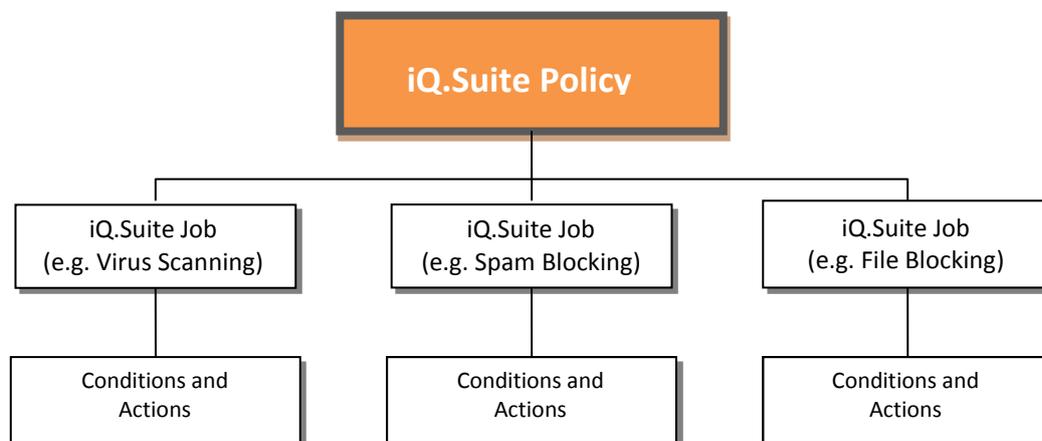
■ Email addresses

Three addresses are configured during installation.

☐ Administrator: The address(es) to which the administrator notifications are sent

☐ Notification from: This is used as the sender address for iQ.Suite notification messages

☐ Reply to: The address to which any replies to a notification are sent.

■ Internal domain

The configuration of iQ.Suite jobs can, for example, include sender/recipient rules with Sender = External and Recipient = Internal. To distinguish external and internal email addresses, the names of the internal domains are defined. During the installation, the domain name of the user performing the installation is used as internal domain.

## 4.2  iQ.Suite Policy – Configuring Policies

The iQ.Suite policy defines iQ.Suite jobs according to corporate policy. Each iQ.Suite job consists of one or more conditions and actions.

```
                        ┌──────────────────────┐
                        │   iQ.Suite Policy    │
                        └──────────────────────┘
          ┌────────────────────┼────────────────────┐
 ┌──────────────────┐ ┌──────────────────┐ ┌──────────────────┐
 │   iQ.Suite Job   │ │   iQ.Suite Job   │ │   iQ.Suite Job   │
 │(e.g. Virus       │ │(e.g. Spam        │ │(e.g. File        │
 │ Scanning)        │ │ Blocking)        │ │ Blocking)        │
 └──────────────────┘ └──────────────────┘ └──────────────────┘
          │                    │                    │
 ┌──────────────────┐ ┌──────────────────┐ ┌──────────────────┐
 │  Conditions and  │ │  Conditions and  │ │  Conditions and  │
 │     Actions      │ │     Actions      │ │     Actions      │
 └──────────────────┘ └──────────────────┘ └──────────────────┘
```

### 4.2.1    iQ.Suite Job Conditions

Various job types are available in the modules for use in policies, e.g.:

- iQ.Suite Watchdog module

  - Virus Scanning

  - Email Size Filtering

  - Attachment Filtering

  - Attachment/Size Filtering

- iQ.Suite Wall module

  - Content Filtering

  - Email Address Filtering

  - Recipient Limit Filtering

- iQ.Suite Trailer module

  - iQ.Suite Trailer

The iQ.Suite job types all have the same structure and administration. Address filtering is performed every time an iQ.Suite job is started. If a message fulfils the entry condition, further conditions, which depend on the job type, may then be checked. In iQ.Suite Watchdog you can, for example, select the desired scan engine, and in iQ.Suite Wall content filtering, you can specify which elements are to be checked with which dictionaries.

## 4.2.2    iQ.Suite Actions

If a message fulfils all conditions of an iQ.Suite job type, various actions – many of which are common to all job types – can be performed. The following overview shows examples of the conditions and actions available for each iQ.Suite job type.

| iQ.Suite Job type | Conditions | | | | | | | Actions (examples) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Sender/recipient checking | Number of recipients | Message size | Fingerprint selection | Virus scanners | Content Filtering | File type/file size | Copy message into quarantine | Start external application | Delete restricted message | Delete restricted attachments |
| iQ.Suite Watchdog Virus Scanning | x | - | - | - | x | - | - | x | x | x | x |
| iQ.Suite Watchdog Email Size Filtering | x | - | x | - | - | - | - | x | x | x | x |
| iQ.Suite Watchdog Attachment Filtering | x | - | - | x | - | - | - | x | x | x | x |
| iQ.Suite Watchdog Attachment/Size Filtering | x | - | - | x | - | | x | x | x | x | x |
| iQ.Suite Wall Content Filtering | x | - | - | x | - | x | - | x | x | x | - |
| iQ.Suite Wall Email Address Filtering | x | x | - | - | - | - | - | x | x | x | - |
| iQ.Suite Wall Recipient Limit Filtering | x | - | - | - | - | - | - | x | x | x | - |
| iQ.Suite Trailer | x | - | - | - | - | - | - | - | - | - | - |

## 4.3 iQ.Suite Monitor

iQ.Suite Monitor lets you view all servers, quarantines and bad mail folders. To be universally accessible, it must be registered under iQ.Suite Servers in the Basic Configuration.

The iQ.Suite Monitor must, in addition, be logged on as an authorized user. The corresponding access rights are entered in the security properties for the quarantine directory on each iQ.Suite Server (`..\GrpData\Quarantine` → **Properties** → **Security** tab).

You can log on to several servers at the same time.

### 4.3.1 Quarantines

All sorted messages can be placed in the iQ.Suite quarantine, where the following information, if available, is recorded for each message:

- Message Subject
- Date and time
- Message sender
- Message recipient
- Short description of the applicable restriction
- Message size
- Name of the iQ.Suite job that quarantined the message
- Name of the Exchange server
- Name of the email file
- Processing history

When you view an iQ.Suite quarantine on the iQ.Suite Console, the information from the quarantine database is shown first. You can then select a quarantine entry to view further information about the message.

For communicating with the iQ.Suite quarantine, SOAP (Simple Object Access Protocol) and SSL (Secure Socket Layer) are used. This applies both to local access on the server and to access from remote Windows workstations. By default, port 8008 is used for communication. Another port can be defined with iQ.Suite Console.

If a quarantined message is to reach its original recipient or another user, it can be forwarded directly from quarantine. The mail will then not be intercepted by an iQ.Suite job again.

### 4.3.2 Bad Mail Quarantine

Any messages that iQ.Suite cannot fully process – for example because it contains corrupt formatting – is placed in the bad mail quarantine. Messages containing password-protected archives and archives with an excessive nesting depth are also placed here. Password-protected archives can, alternatively, be routed to their recipient (see also section 8, **BadmailArchives** parameter). These messages can be processed in the same way as quarantined mail. The administrator is notified by email of every message written to the bad mail quarantine.

# 5 iQ.Suite Watchdog

iQ.Suite Watchdog checks messages for viruses, for the type and size of its attachments and for the total message size. It is called by iQ.Suite Service during mail processing.

iQ.Suite Watchdog can perform any of the following job types:

- Virus scanning using an incorporated scan engine
  Job type: iQ.Suite Watchdog Virus Scanning

- Blocking specific file types in the attachment
  Job type: iQ.Suite Watchdog Attachment Filtering

- Limiting message size
  Job type: iQ.Suite Watchdog Email Size Filtering

- Limiting attachment type and/or size
  Job type: iQ.Suite Watchdog Attachment/Size Filtering

The following sections deal in more detail with virus scanning and attachment filtering using fingerprints.

## 5.1 Virus Scanning

Virus scanning is performed using one or more third-party scan engines, which must be either installed on the Exchange server or accessible through the network. Once configured correctly, iQ.Suite Watchdog calls the scan engine through the GROUP AV interface – a DLL file usually located in the same directory as the scan engine pattern file.

iQ.Suite Watchdog supports scan engines from the leading vendors, e.g. Avira and Sophos.

### 5.1.1 The Virus Scanning Process

The iQ.Suite Watchdog Virus Scanning job starts the selected scan engines as defined in the configured conditions. If several scan engines have been selected, the messages are scanned by each scan engine in turn.

iQ.Suite Watchdog can handle mail in one of two ways:

■ Perform virus scan and remove infected attachments

■ Perform virus scan and clean infected attachments

**Processing sequence for scanning and removing infected attachments**

1. The active scan engines scan messages in the order specified in the Watchdog job. If a scan engine finds a virus, scanning is stopped.

2. Watchdog removes the infected attachment from the message. Optionally, the complete message is copied into quarantine.

Processing sequence for scanning and cleaning infected attachments

1. The active scan engines scan messages in the order specified in the Watchdog job. If a scan engine finds a virus, scanning is stopped.

2. The scan engine that has found the virus is now used to clean the infected file.

3. The active scan engines rescan the message in the specified order to ensure that the virus has been removed. If it has, message processing continues as normal. If the attachment is still infected, the scan and remove attachment sequence is performed.

## 5.2 Fingerprints

iQ.Suite Watchdog uses **fingerprints** to identify file types. Fingerprints consist of a name pattern and/or a binary pattern.

■ Filename pattern: can be used to define file types by filenames and file extensions

(*.exe, etc.)

■ Binary pattern: can be used to define file types using unique binary file information.

Malicious users can manipulate filenames by simply changing the extension to a different file type. To prevent file type filtering being fooled by this type of manipulation, you can use the binary pattern which uniquely identifies file formats. The binary pattern is therefore the most reliable method of identifying file types.

Filename patterns, however, can be used to quickly react to new virus attacks:

As soon as the extension of the file containing a virus is known (for example Nimda Virus = readme.exe), a virus can be intercepted even before a virus pattern update is available from the

publisher of your antivirus application. A new fingerprint with the filename pattern is simply created to identify the virus.

If a company employs custom software that uses its own file format, fingerprints can also be created for these files. You can use these fingerprints, for example, to prevent files of this type being sent to recipients outside the company as email attachments.

The binary pattern contains three items of information:

- Start position: Specifies the start position for the pattern search within the file.

    - "1", "2"... : Start at the first, second, etc. byte

    - "-1", "-6"... : Start at the last, sixth from last, etc. byte

- End position: Specifies the end position for the pattern search within the file.

    - "-1": Search to the end of the file

    - "1", "2": Search up to the first, second,etc. byte

- Hexadecimal value: Describes the pattern to be searched for between the start and end positions.

Fingerprints can consist of several binary patterns. A Zip file, for example, has the following pattern:

- Start: 1      End: 4          Hex.: 504B0304

A Windows Meta File (WMF) has a more complex structure:

- Start: 1      End: -1 Hex: 576F72642E446F63756D656E74

- Start: 1      End: -1 Hex: 57006F007200640044006F00630075006D0065006E0

- Start: 1      End: 10 Hex: D0CF11E0A1B11AE10000

The fingerprint list of iQ.Suite contains about 350 entries, including about 100 with binary patterns. It is grouped into a range of categories – such as email attachments, executables, ASCII, sound, images, and fonts. You can add your own categories to this list. Thanks to the open fingerprint architecture, you can modify existing ones fingerprints as well as creating new ones.


# 6    iQ.Suite Trailer

The iQ.Suite Trailer module centrally generates email signatures using Exchange user information from the Active Directory (AD). In addition to personal user signatures, it can, for example, add legal disclaimers. Its central approach guarantees that signatures are standardized and always up-to-date throughout the company.

The Active Directory is used because of the simple maintenance of its domain structure and the ease with which objects and properties can be added. Information from other domains is provided by the Global Catalogue – an index containing the required information of all users within an Active Directory. The Active Directory itself is read only and remains unaffected by the use of the Global Catalogue.

Any information available for a user can be used for that user's email signature. Which information is used is specified in the iQ.Suite Trailer configuration settings. The administrator defines user signatures using the MMC, for which the following information is available:

Department
Title
Display name
State/Province
Office
Email address
Fax
Company
Country/Region
Last name
City
PO Box
Zip Code
Street Address
Phone (office)
Phone (mobile)
Phone (home)
First name
Web Page

Signatures have the following structure:

[VAR]Active Directory attribute name;default value[/VAR]

Example of a sender signature:

[VAR]givenName[/VAR] [VAR]sn[/VAR]
[VAR]physicalDeliveryOfficeName;[/VAR]
Telephone: [VAR]telephoneNumber;0123-456[/VAR]
Fax: [VAR]facsimileTelephoneNumber;987-6543[/VAR]
Email: [VAR]mail[/VAR]

You can also use any other value from the Active Directory and the Global Catalogue. If, for example, a company employs user-defined attributes for personnel numbers in the Active Directory, iQ.Suite Trailer can also use this information. If a value does not exist for a particular user, a default value can instead be used. The field names of the Active Directory can, for example, be determined with the ADSI Edit tool from the Windows 2000 Resource Kit.

When you use iQ.Suite Trailer, the Outlook sender signatures should be disabled to ensure that no other signatures are appended to messages. This can be done centrally through the Windows 2000 Group Policies.

The illustration below shows the basic sequence for adding a user signature.
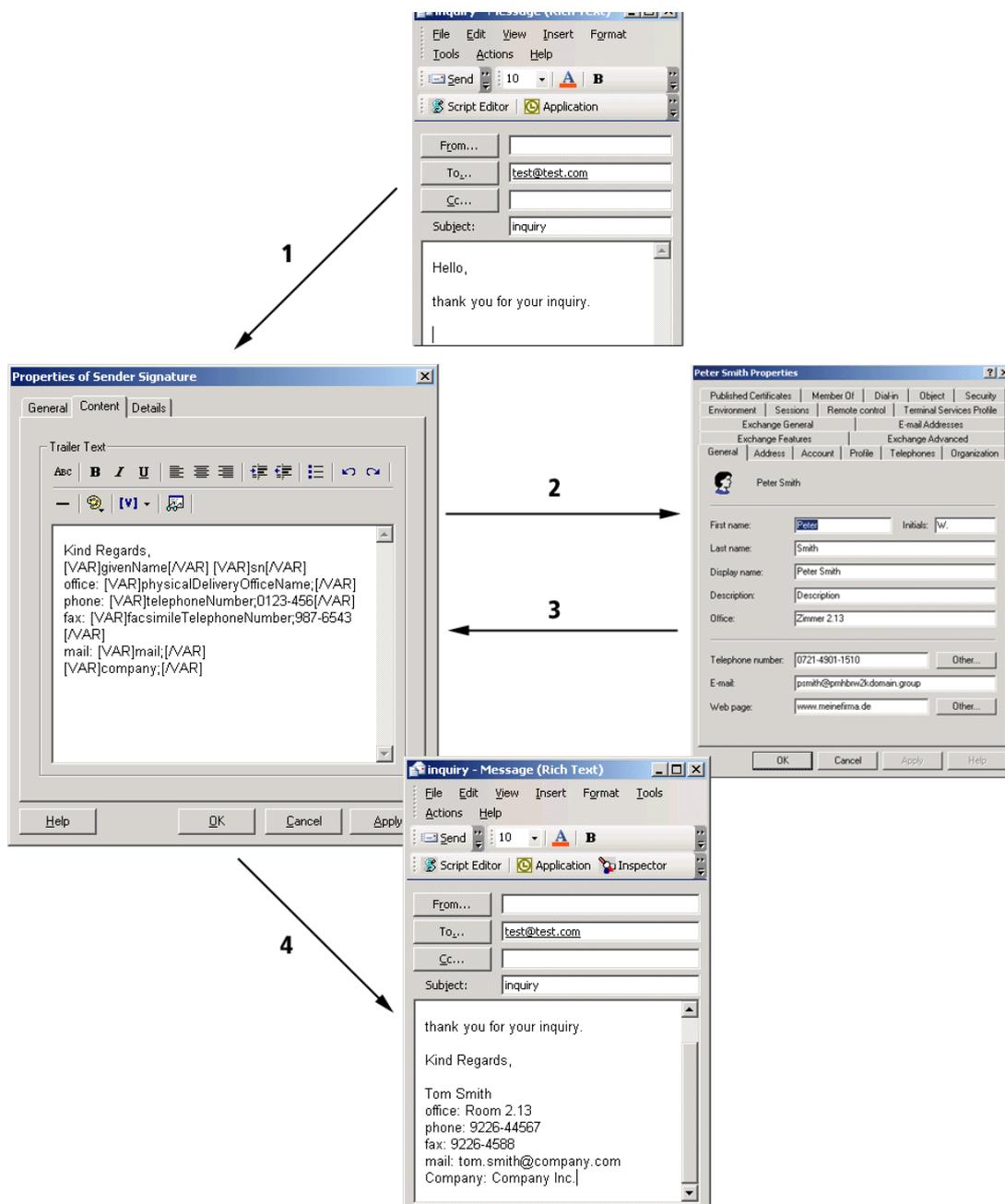
1. The user writes and sends a message (unsigned).

2. iQ.Suite Trailer appends the specified signature and queries the Active Directory for the required user information.

3. The Active Directory supplies the requested content. If this information is not available, iQ.Suite Trailer uses default values.

4. The information is inserted at the correct places in the signature and the message is sent.

# 7    System Requirements

To install iQ.Suite, your system must meet the following requirements:

- RAM: Microsoft Exchange recommendation plus additionally 512 MB. Further memory is needed for third-party systems such as virus scanners as well asfor database access (OLEDB driver).

- Hard disk: Minimum 400 MB for installation. Additional space for quarantine.

- Microsoft .Net Framework 2.0.

- Microsoft .Net Framework 4.0 (Client Profile and Microsoft Redistributable Packages). If not installed yet, the components are installed in the course of iQ.Suite installation.

- Windows Scripting (for installation only)

- Supported operating systems:

- Windows 2000 Server > Service Pack 4

    - ☐ Windows Server 2003 (32-bit and 64-bit)

    - ☐ Windows Server 2003 R2 (32-bit and 64-bit)

    - ☐ Windows Small Business Server 2003 as of SP 1 (32-bit and 64-bit)

    - ☐ Windows Server 2008 (32-bit and 64-bit)

    - ☐ Windows Server 2008 R2 (64-bit)

    - ☐ Windows Small Business Server 2008 (32-bit and 64-bit)

    - ☐ Windows Small Business Server 2011 (64-bit)

    - ☐ Windows Server 2012 (64-bit)

- Supported Microsoft Exchange servers:

    - ☐ Microsoft Exchange Server 2003

    - ☐ Microsoft Exchange Server 2007 from SP 1 with the roles:
        - ► Hub Transport Server
        - ► Mailbox Server

&#9658; Edge Transport Server

As a minimum, "Update Rollup 4 for Exchange 2007 SP1" installed.

&#9633; Microsoft Exchange Server 2010 (64-bit) on Windows Server 2008 R2 with the roles:

&#9658; Hub Transport Server

&#9658; Mailbox Server

&#9658; Edge Transport Server

&#9633; Microsoft Exchange Server 2013 (64-bit) on Windows Server 2012

&#9658; iQ.Suite is installed on the ‚Mailbox Server' role.

■ Supported languages: German, English

■ Further system requirements apply if using the SASI Engine[1].

# 8 The Windows Registry

A number of Registry keys are created when you install iQ.Suite. These entries are used by both the iQ.Suite server and the iQ.Suite console.

The key is located under HKEY_LOCAL_MACHINE\SOFTWARE\GROUP TECHNOLOGIES\iQ.Suite and contains further keys.

    a. General (for example default paths)

    b. Grabber (configuration of the iQ.Suite event sinks in the SMTP Advanced Queue)

    c. Inject (path of the Exchange pickup directory)

    d. Logging (Debug log settings)

Below is a list of the most important keys.

---

[1] **For further Information, please refer to the separate SASI document. Download on www.gbs.com.**

## 8.1 General

| Parameter name | Type | Possible values | Description |
| --- | --- | --- | --- |
| Code | STRING | Path | Path of program directory |
| Data | STRING | Path | Path of data directory |
| InQ | STRING | Path | iQ.Suite in-queue |
| Config | STRING | Path | Path of configuration file |
| Language | STRING | Path | Path of language version file |
| ADContextResetTime | DWORD | Positive integer | Refresh interval for the information from the Active Directory (such as users and groups). Default: 3600 = 1 hour |
| LDIF | STRING | Path | Path of the LDIF file. By default configured for iQ.Suite for SMTP. Can also be set for iQ.Suite for Exchange. |
| BadmailArchives | DWORD | 0, 1 | Archives that can not be unpacked are moved to the bad mail area (1, default) or delivered to the recipient (0). This parameter is defined internally. To change it, you have to manually add it to the Registry. |

## 8.2 Grabber

| Parameter name | Type | Possible values | Description |
| --- | --- | --- | --- |
| ActiveEvent | DWORD | 1=OnSubmission 2=OnPreCategorize 3=OnPostCategorize | Parameter for the actual starting point for processing. Default = 3. |
| ActionMode | DWORD | 0=OFF 1=NORMAL | 0: iQ.Suite on the server is completely deactivated. 1: Normal processing by iQ.Suite |
| Logging | DWORD | 1=ACTIVE 0=INACTIVE | Grabber log mode. The log is written to `<CODE>\LOG\GRABBER.LOG`. Default = 0 |
| ADFilterActive | DWORD | 1=ACTIVE 0=INACTIVE | Search request to Active Directory whether the mail is a system mail. Default Exchange = 1 Default SMTP = 0 |

| Parameter name | Type | Possible values | Description |
|---|---|---|---|
| ADFilterActive | DWORD | 1=ACTIVE<br>0=INACTIVE | Search request to Active Directory whether the mail is a system mail.<br><br>Default Exchange = 1<br>Default SMTP = 0 |

## 8.3 Inject

| Parameter name | Type | Possible values | Description |
|---|---|---|---|
| PickUp | STRING | Path | Path to the Exchange server pickup directory |

## 8.4 Logging

| Parameter name | Type | Possible values | Description |
|---|---|---|---|
| Enabled | DWORD | 0=OFF, 1=ON | Enables and disables iQ.Suite Service Debug mode. Log written to `<CODE>\LOG\EMH.LOG`. Default = 0 |
| Loglevel | DWORD | Positive integer up to 255 | General log level entries based on a bit mask. The individual entries have the following meanings:<br><br>0 = no log entry<br><br>1= fatal error<br><br>2 = critical error<br><br>4 = important information<br><br>8 = error<br><br>16 = information<br><br>32 = warnings<br><br>64 = details<br><br>128 = comprehensive details<br><br>Default = 15, which means the first four items (1, 2, 3 and 4) are logged. |

**About GBS**

GROUP Business Software is a leading vendor of solutions and services in the fields of messaging security and workflow for the IBM and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

Further information at [www.gbs.com](http://www.gbs.com)