iQ.Suite für Exchange/SMTP

- Durchgängige E-Mail-Prozesse -

Das führende Programmpaket zur Realisierung
von E-Mail-Management

Expertise matters

Inhalt

1 Zusammenfassung

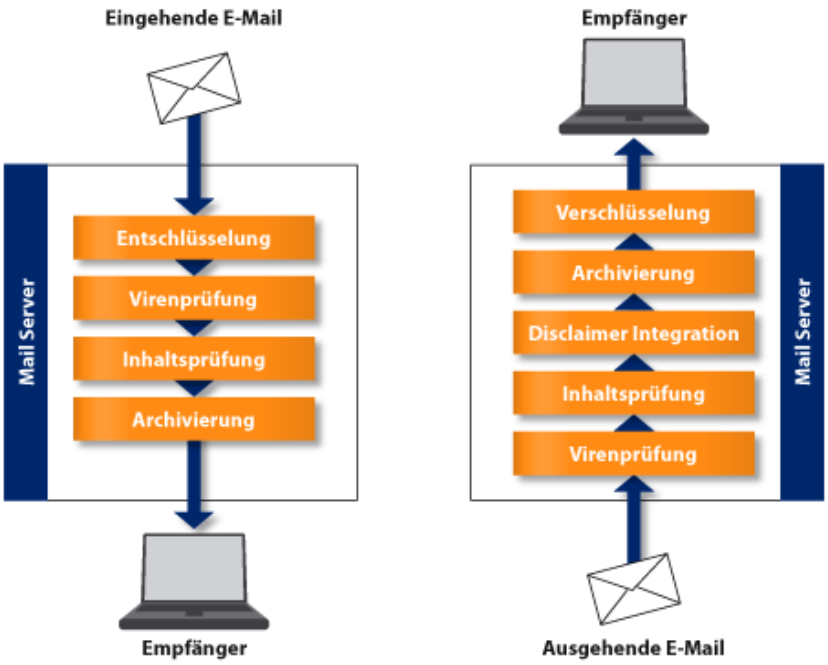
Das E-Mail Aufkommen ist in den letzten Jahren nahezu explosionsartig gestiegen. Mittlerweile ist E-Mail integraler Bestandteil vieler Geschäftsprozesse. Auch die Möglichkeit, Dateien an E-Mails anzuhängen, wird immer stärker genutzt. Aufkommende Fragen zur Sicherheit, Organisation und Verfügbarkeit der Kommunikationsstruktur können mit der iQ.Suite für Exchange von GBS Software (GBS) beantwortet werden.

GBS Software ist Spezialist für E-Mail-Sicherheits- und Managementlösungen. Die langjährige Erfahrung im Messaging- und Groupware-Bereich garantiert praxiserprobte und robuste Produkte. GBS bietet mit der iQ.Suite ein komplettes E-Mail-Management, das vor den drohenden Gefahren beim Einsatz von E-Mail schützt. Die iQ.Suite ist für die Plattformen Microsoft Exchange, SMTP Gateways und IBM Notes/Domino verfügbar.

Aufgrund der modularen Architektur können die Produkte beliebig kombiniert und skaliert werden. Die gewünschten Komponenten kommen je nach Anforderung zum Einsatz. Weitere Komponenten können einfach hinzugefügt werden.

Alle Produkte nutzen ein gemeinsames, regelbasiertes Sicherheits- und Managementkonzept. Der Zusammenschluss aller Funktionen gewährleistet optimale Leistung und Sicherheit. Konfigurierbare Benachrichtigungen an Absender, Empfänger und Administrator liefern Transparenz. Alle Produkte werden einheitlich und zentral über die Microsoft Management Console (MMC) verwaltet. Gemeinsame Protokolle, Statistiken und Fehlerreports verringern die Kosten für die Administration erheblich.

Die iQ.Suite wird auf dem Exchange-Server installiert, um den gesamten E-Mail-Verkehr eines Unternehmens (ins Internet, vom Internet, intern) zu kontrollieren. Genauere Informationen zu den Systemvoraussetzungen finden Sie auf unserer Webseite. Anschließend wird sie entsprechend den firmeneigenen Richtlinien zum Umgang mit E-Mails konfiguriert.



Durch die Integration von Produkten anderer Hersteller, z.B. Virenscannern, kann der elektronische Informationsaustausch individuell organisiert und das Netzwerk effektiv und effizient geschützt werden. Außerdem kann die iQ.Suite den E-Mail-Verkehr auf unerwünschte Inhalte prüfen und so beispielsweise zur Spam-Abwehr genutzt werden.

In diesem White Paper wird der architektonische Aufbau und die Funktionsweise der iQ.Suite erläutert. Das White Paper richtet sich an Administratoren und Entscheider, die gerne einen Blick „unter die Motorhaube“ werfen.

2 Die Produktarchitektur

Die iQ.Suite für Exchange besteht aus drei Hauptkomponenten:

- iQ.Suite Konsole
- iQ.Suite Server
- iQ.Suite Konfiguration

Im Folgenden werden die einzelnen Komponenten erläutert.

2.1 iQ.Suite Konsole

Die iQ.Suite Konsole ist das „Cockpit“, aus dem heraus die iQ.Suite konfiguriert und administriert wird. Es handelt sich hierbei um ein Snap-In für die Microsoft Management Console (MMC). Mit der iQ.Suite Konsole können sowohl einzelne Exchange-Server mit installierter iQ.Suite als auch ganze „iQ.Suite Serverfarmen“ administriert werden. Dies erleichtert speziell in einer Multiserver-Umgebung die tägliche Administration. Mit der iQ.Suite Konsole hat der Administrator Zugriff auf alle erforderlichen Konfigurationsinformationen und auf die iQ.Suite Quarantänebereiche der iQ.Suite Server.

Folgende Methoden für die Zugriffe auf die Konfiguration und auf die Quarantänebereiche werden verwendet:

- Standard Windows Dateizugriff

  Für den Zugriff auf die iQ.Suite Konfiguration ist ein Windows Dateizugriff erforderlich. Hierbei kann die iQ.Suite Konfiguration lokal zur Verfügung stehen oder über einen Universal Naming Convention (UNC) Pfad erreicht werden.

- Zugriff über Simple Object Access Protocol (SOAP) und Secure Socket Layer (SSL)

  Der Zugriff auf die Quarantänebereiche erfolgt über SOAP und SSL. Das SOAP Protokoll bietet eine einfache und effektive Kommunikation, genügt alleine jedoch nicht den Sicherheitsanforderungen der iQ.Suite. Daher wird mit Hilfe von SSL der Kommunikationskanal verschlüsselt. Während der Installation werden hierfür alle notwendigen Komponenten bereitgestellt.

Die iQ.Suite Konsole unterstützt folgende Betriebsmodi:

- Lokale Administration

  Bei der lokalen Administration wird die iQ.Suite Konsole direkt auf dem Exchange-Server betrieben, auf dem alle Komponenten der iQ.Suite installiert sind. Dieser Modus ist für kleinere Netzwerke und für die Vor-Ort Administration am Server geeignet.

- Remote Administration

  Bei der Remote Administration greift die iQ.Suite Konsole von einem Client Betriebssystem auf einen oder mehrere Exchange-Server zu, um die iQ.Suite zu konfigurieren und administrieren. Die Remote Administration ist für die zentrale Administration in Multiserver Umgebungen geeignet.

2.2 iQ.Suite Server

So wie die iQ.Suite Konsole das Cockpit der iQ.Suite ist, so ist der iQ.Suite Server der Motor. Mit iQ.Suite Server werden die Funktionen und Prozesse der iQ.Suite bezeichnet, die ausschließlich auf dem Exchange-Server laufen. Hierbei kann der iQ.Suite Server auf einem Exchange-Server, Frontend-Server oder Backend-Server installiert werden. Der iQ.Suite Server besteht aus den Hauptkomponenten iQ.Suite Grabber und iQ.Suite Service sowie den weiteren Komponenten iQ.Suite Quarantäne und iQ.Suite Unpacker.

2.2.1 iQ.Suite Grabber

Der iQ.Suite Grabber „greift“ alle E-Mails, Terminanfragen, etc. ab, die der Exchange-Server versendet, empfängt oder weiterleitet. Ab Exchange 2000 verwendet Microsoft für den gesamten Transport von E-Mails, Terminanfragen, etc. das Simple Mail Transport Protocol (SMTP). Ein Bestandteil dieses Transportprotokolls ist die Advanced Queue („erweiterte Warteschlange“). Durch diese Advanced Queue wird der komplette E-Mail-Verkehr geleitet. Dabei ist es unerheblich, ob die E-Mails zwischen Postfächern auf dem gleichen Postfachspeicher oder Server gesendet werden oder via Internet hinein- oder hinausgehen.

Der iQ.Suite Grabber überwacht als registrierte Ereignissenke (Event Sink) in der Advanced Queue den E-Mail-Verkehr. Dazu ist er in der Advanced Queue an drei Stellen registriert:

- OnSubmission
- OnPreCategorize
- OnPostCategorize

Exchange-interne Informationen, wie z.B. Replikationsnachrichten, werden vom iQ.Suite Grabber erkannt und sofort unverändert an das Exchange-System zurückgegeben.

Alle zu verarbeitenden E-Mails werden vom iQ.Suite Grabber in die iQ.Suite In-Queue gestellt. Diese befindet sich im Verzeichnis `..\Grpdata\InQ`. Hier sind zum einen die Original E-Mails als Textdateien hinterlegt und zum anderen erstellt der iQ.Suite Grabber zu jeder E-Mail eine XML-Datei

mit Zusatzinformationen wie beispielsweise Angaben aus dem SMTP Header. Beispiel für ein solches Dateipaar:

- **2C4A14A23BD144B3ACE09E6BE2D49603000.txt**
  (Enthält die Original E-Mail)
- **2C4A14A23BD144B3ACE09E6BE2D49603000.xml**
  (Enthält die Zusatzinformationen)

Sobald der iQ.Suite Grabber installiert ist, werden alle E-Mails in die iQ.Suite In-Queue kopiert. Von dort aus sorgt der iQ.Suite Service für die Weiterverarbeitung. Ist der iQ.Suite Service nicht gestartet, werden die E-Mails inkl. der XML-Dateien in der iQ.Suite In-Queue so lange gespeichert, bis der iQ.Suite Service gestartet und die Weiterverarbeitung fortgesetzt wird.

2.2.2 iQ.Suite Service = Enterprise Message Handler (EMH)

Der iQ.Suite Service ist als Windows Dienst permanent gestartet. Um Anfragen an das Active Directory durchführen zu können, benötigt er den Windows Management Instrumentation (WMI) Service. Der WMI Service ist grundsätzlich auf Windows Servern verfügbar und aktiviert.

Sobald der iQ.Suite Service die E-Mails vom iQ.Suite Grabber übernommen hat, überwacht und steuert er die gesamte Weiterverarbeitung durch die iQ.Suite. Der iQ.Suite Service hat dazu Zugriff auf alle notwendigen Prozessinformationen.

Die wichtigsten sind:

- Die konfigurierten iQ.Suite Jobs
  z.B. zur Virenprüfung, Inhaltsprüfung oder Adressprüfung
- Die installierte iQ.Suite Lizenz, die festlegt, welche Module der iQ.Suite für die Prüfungen zur Verfügung stehen, z. B. iQ.Suite Watchdog, iQ.Suite Wall, iQ.Suite Trailer
- Das Active Directory
- Die iQ.Suite Quarantäne

Mit Hilfe dieser Informationen werden die E-Mails nun beispielsweise auf Viren untersucht, Spam-Mails identifiziert und in Quarantäne gestellt oder Haftungsausschlusserklärungen integriert.

Nach der Bearbeitung gibt der iQ.Suite Service die E-Mails an den Exchange-Server zurück. Dazu werden die E-Mails in das Exchange Pickup-Verzeichnis verschoben und der Exchange-Server kann die Weiterverarbeitung der E-Mails übernehmen.

Eine E-Mail wird erst dann zugestellt, wenn die gesamte Verarbeitung durch den iQ.Suite Server erfolgreich beendet ist.

2.2.3 iQ.Suite Quarantäne

Als eine mögliche Option können unerwünschte E-Mails auf dem Server gestoppt und in die iQ.Suite Quarantäne kopiert werden. Damit wird verhindert, dass diese E-Mails bei den entsprechenden Empfängern ankommen.

Auf jedem iQ.Suite Server steht nach der Installation eine Standardquarantäne zur Verfügung. Weitere Quarantänen können vom Administrator angelegt werden.

Eine iQ.Suite Quarantäne besteht aus:

- Einem Quarantäneverzeichnis auf dem Exchange-Server

  (...\GrpData\Quarantine\Standard-Quarantaene)
- Den E-Mails, die in diese Quarantäne kopiert wurden
- Einer Quarantänedatenbank im Access-Datenbankformat (**LocIdxDB.mdb**)

Für jede in Quarantäne gestellte E-Mail erstellt die iQ.Suite automatisch einen Eintrag in der Quarantänedatenbank.

Auf die iQ.Suite Quarantänen können nur autorisierte Personen zugreifen. Pro Server können Windows Benutzerberechtigungen für die iQ.Suite Quarantäne vergeben werden. Im Verzeichnis `...\Program Files\GROUP Technologies\iQ.Suite\Appdata` befindet sich die Datei **access.acl**. Diese steht stellvertretend für die iQ.Suite Quarantänen auf diesem Server. Die Benutzer bzw. Gruppen, die auf diese Datei Leseberechtigungen besitzen, haben Zugriff auf die iQ.Suite Quarantänen. Diese Berechtigungen werden durch den iQ.Suite Service geprüft.

Für den erfolgreichen Zugriff müssen folgende Bedingungen erfüllt sein:

- Der iQ.Suite Service ist gestartet
- Der Kommunikations-Port (Standard: 8008) ist verfügbar
- Der Benutzer besitzt die erforderlichen Windows Benutzerberechtigungen

Innerhalb einer Quarantäne ist es möglich, die E-Mails nach verschiedenen Auswahlkriterien zu filtern.

2.2.4 iQ.Suite Unpacker

Für umfassende E-Mail Sicherheit müssen auch Archivdateien, wie z.B. ZIP-Dateien, nach unerwünschten Inhalten durchsucht werden können. Diese Aufgabe übernimmt der iQ.Suite Unpacker. Der Unpacker kann in den Jobtypen

- iQ.Suite Watchdog Virus Scanning
- iQ.Suite Watchdog Attachment Filtering
- iQ.Suite Watchdog Attachment/Size Filtering
- iQ.Suite Wall Content Filtering

aktiviert werden.

Folgende Archivformate können bearbeitet werden:

- ACE
- ARJ, Selfextracting ARJ
- CAB
- GZIP
- LZH
- RAR
- TAR
- TGZ
- UUEncoded
- ZIP, Selfextracting ZIP
- ZOO

2.3 iQ.Suite Konfiguration

Alle Informationen, die zum Betreiben der iQ.Suite erforderlich sind, werden in der iQ.Suite Konfiguration gespeichert. Sie liegt in Form einer XML-Datei (**configdata.xml**) vor.

Die **configdata.xml** ist wie eine Datenbank aufgebaut. Für jeden Konfigurationsbereich sind verschiedene Einträge vorhanden. Da die Konfiguration in einer einzigen Datei gespeichert ist, kann die Konfiguration einfach verteilt und gesichert werden. Zur Unterstützung bei Konfigurationsproblemen kann die **configdata.xml** an das GROUP Support-Team gesendet werden.

Sowohl der iQ.Suite Server als auch die iQ.Suite Konsole müssen auf die Konfigurationsdaten zugreifen können. Der iQ.Suite Server erhält daraus z. B. die Informationen über die auszuführenden iQ.Suite Jobs. Mit der iQ.Suite Konsole kann die Konfiguration geändert werden. Die iQ.Suite Konfiguration kann sowohl in einem lokalen Verzeichnis als auch auf einem Netzwerkshare gespeichert werden.

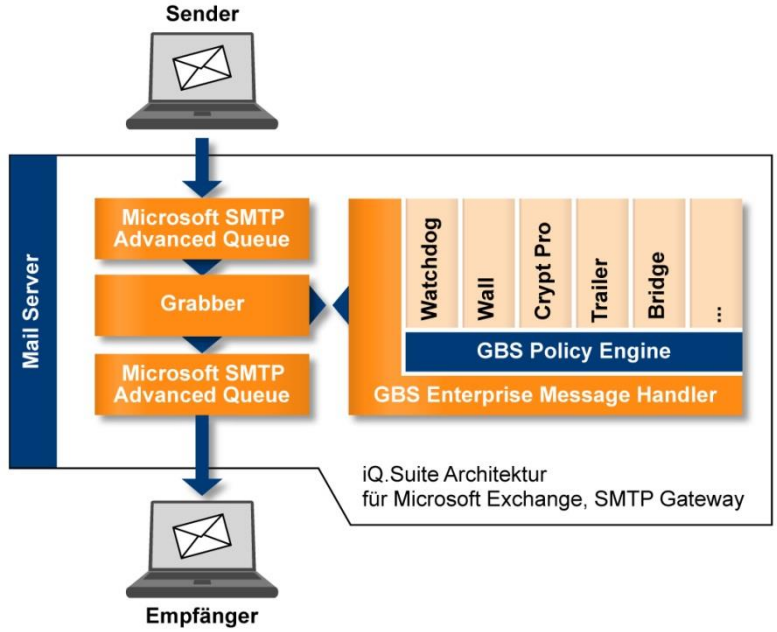
Welche iQ.Suite Konfiguration die iQ.Suite Konsole bzw. der iQ.Suite Server verwendet, wird durch einen Eintrag in der Registry festgelegt (siehe Kapitel 7). Der Pfad zur iQ.Suite Konfiguration kann im Format `C:\ ...` oder als UNC Pfad

(\\Servername\Share\configdata.xml) angegeben werden.

Falls die angegebene iQ.Suite Konfiguration nicht verfügbar ist, verwendet die iQ.Suite die sogenannte „Last-Known-Good“ Konfiguration. Dies wird in der Windows Ereignisanzeige protokolliert. Die Last-Known-Good Konfiguration ist pro Server lokal gespeichert (`... Program files\GROUP Technologies\iQ.Suite\Appdata\LastConfig.xml`) und wird immer dann aktualisiert, wenn Veränderungen an der aktiven iQ.Suite Konfiguration vorgenommen wurden und der Zugriff auf die Last-Known-Good Konfiguration möglich ist.

3 Ablauf der E-Mail Verarbeitung

Wie in Kapitel 2.2 beschrieben, überwacht die iQ.Suite den E-Mail Verkehr an der Exchange SMTP Advanced Queue. Anhand der folgenden Abbildung wird der Ablauf der E-Mail-Verarbeitung durch die iQ.Suite beschrieben.



1. Eine E-Mail trifft auf dem Server ein.
2. Die E-Mail wird durch den Grabber aus der SMTP Advanced Queue abgefangen und in einen speziellen Ordner gestellt.
3. Der Enterprise Message Handler (EMH) [= iQ.Suite Service] holt sich die E-Mail aus dem Ordner.
4. Der EMH überprüft anhand der Konfiguration, ob die E-Mail durch die iQ.Suite zu bearbeiten ist. Ansonsten wird die Mail sofort wieder der SMTP Advanced Queue zugeführt.
5. Zu bearbeitende Mails werden gemäß der Konfiguration (Jobs nach ihrer Priorität) abgearbeitet.
6. Der EMH gibt nach vollständiger Bearbeitung die E-Mail frei und stellt die Mail dem Exchange-Server zur Verfügung.

3.1 Active Directory

Die iQ.Suite nimmt keine Veränderungen oder Erweiterungen im Active Directory vor. Informationen aus dem Active Directory werden jedoch an verschiedenen Stellen von der iQ.Suite ausgelesen:

- Beim Starten fragt der iQ.Suite Service den verfügbaren Global Catalog Server an. Dieser wird z. B. bei der Adressauflösung von Verteilerlisten während der E-Mail-Verarbeitung verwendet.
- Die iQ.Suite Konsole verwendet das Active Directory bei der Auswahl von Sender-/Empfänger-Bedingungen.
- Mit iQ.Suite Trailer können Absenderinformationen in ausgehende E-Mails integriert werden. Dabei sucht die iQ.Suite im Active Directory nach den entsprechenden Angaben.

Steht kein Active Directory zur Verfügung, da z. B. die entsprechenden Ports nicht offen sind, kann mit einer LDIF-Datei gearbeitet werden. Diese wird beispielsweise durch einen LDAP-Export aus einem Active Directory, Exchange Benutzerverzeichnis oder einem Notes Namens- und Adressbuch (NAB) erzeugt.

4 Aufbau der iQ.Suite Konsole im Detail

Die Benutzeroberfläche der iQ.Suite Konsole ist in drei Bereiche unterteilt. Jeder Bereich beinhaltet verschiedene Einstellmöglichkeiten und Informationen.

- Basis-Konfiguration (enthält Basis-Informationen z.B. über Virenscanner, Server)
- Richtlinien-Konfiguration (enthält die iQ.Suite Jobs)
- iQ.Suite Monitor (ermöglicht Zugriff auf die iQ.Suite Quarantänen und Bad-Mails)

Im Folgenden werden die drei Bereiche näher beschrieben.

4.1 Basis-Konfiguration der iQ.Suite Servers

Die Basis-Konfiguration hält alle grundsätzlichen Informationen bereit, die von der iQ.Suite benötigt werden, um eine sichere Exchange-Umgebung zu schaffen. Dazu gehört die Verwaltung aller Ordner, der Wortlisten für die Inhaltsprüfung, der Benachrichtigungs- und Jobvorlagen, der Fingerprints und der Virenscanner. Außerdem werden die Einstellungen für die iQ.Suite Servers vorgenommen, die im Folgenden erläutert werden.

In der Basis-Konfiguration der iQ.Suite Servers sind die Server mit installierter iQ.Suite aufgeführt. Über das Eigenschaften-Menü von iQ.Suite Servers werden die serverübergreifenden Einstellungen erreicht. Diese Einstellungen gelten grundsätzlich für alle Server, die mit dieser iQ.Suite Konfiguration arbeiten.

Folgende Einstellungen sind möglich:

- Einstellungen für gepackte Dateien (Archivdateien)

  Um zu verhindern, dass entpackte Dateien die Festpatte blockieren, kann eine Obergrenze eingestellt werden. Standardmäßig ist der Wert auf 300 MB gesetzt. Insbesondere als Schutz vor „ZIP of Death“-Attacken ist diese Begrenzung wichtig, da hierbei die Dateien gepackt nur wenige Kilobyte groß sind, entpackt jedoch mehrere Gigabyte auf der Festplatte einnehmen.

  Des Weiteren ist die Entpackungstiefe von Archivdateien limitiert. Archivdateien können, wie die russische Matrjoschka, aus vielen ineinander verschachtelten Archivdateien (rekursiv gepackte Dateien) bestehen. Das Entpacken dieser Dateien kann zu einer 100%-Auslastung des Servers führen. Um das zu verhindern, ist die maximal erlaubte Entpackungstiefe standardmäßig auf 5 eingestellt. Archivdateien, die dieses Limit überschreiten, werden als Bad-Mail klassifiziert und in die Bad-Mail-Quarantäne gestellt.

- Kommunikationseinstellungen

  Zur Kommunikation mit iQ.Suite Quarantänen verwendet die iQ.Suite Konsole SOAP und SSL. Diese Kommunikation geschieht grundsätzlich über Port 8008, der Port kann aber an dieser Stelle geändert werden. Allerdings müssen nach einer Änderung alle zugreifenden iQ.Suite Konsolen angepasst werden.

- E-Mail-Adressen

  Drei verschiedene Adressen werden während der Installation konfiguriert.

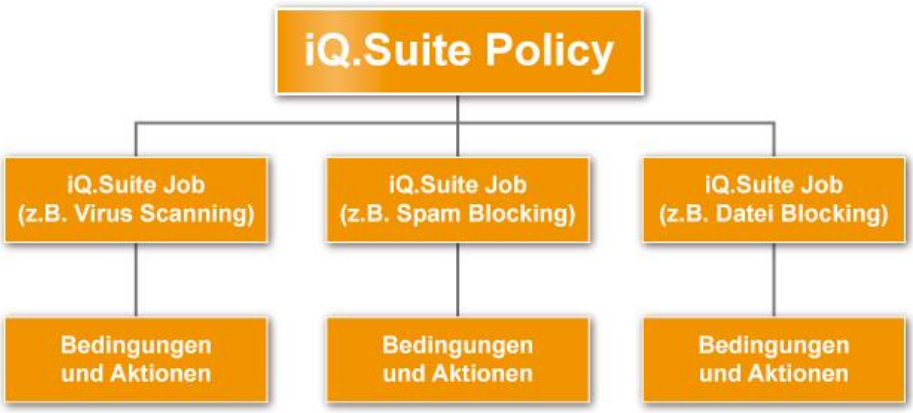
  - Administrator: An diese Adresse(n) werden die iQ.Suite Administratorbenachrichtigungen gesendet
  - Benachrichtigung von: Diese Adresse erscheint als Absender der iQ.Suite Benachrichtigungen
  - Antwort an: An diese Adresse werden eventuelle Antworten auf eine Benachrichtigung gesendet.

- Interne Domäne

  Bei der Konfiguration von iQ.Suite Jobs können z. B. Absender-/Empfänger-Regeln mit Sender = Extern und Empfänger = Intern angelegt werden. Damit die iQ.Suite weiß, was interne und externe E-Mail-Adressen sind, werden die Namen der internen Domänen festgelegt. Während der Installation wird der Domänenname des installierenden Benutzers als interne Domäne eingesetzt.

4.2 iQ.Suite Policy – Richtlinienkonfiguration

In der iQ.Suite Policy werden iQ.Suite Jobs basierend auf firmeneigenen Richtlinien definiert. Jeder iQ.Suite Job besteht aus einer oder mehreren Bedingungen und Aktionen.



4.2.1 iQ.Suite Job Bedingungen

Für die erforderlichen Jobs der iQ.Suite Policy stehen in den Modulen der iQ.Suite verschiedene Jobtypen zur Verfügung, z.B.:

- Modul iQ.Suite Watchdog
  - Virus Scanning
  - E-Mail Size Filtering
  - Attachment Filtering
  - Attachment/Size Filtering
- Modul iQ.Suite Wall
  - Content Filtering
  - E-Mail Address Filtering
  - Recipient Limit Filtering
- Modul iQ.Suite Trailer
  - iQ.Suite Trailer

Der Aufbau und die Administration der iQ.Suite Jobtypen sind einheitlich gestaltet. Für jeden iQ.Suite Jobtyp wird beim Eintritt grundsätzlich die Adressprüfung durchgeführt. Erfüllt eine E-Mail die Eintrittsbedingung, dann werden ggf. weitere Bedingungen geprüft. Diese weiteren Bedingungen sind abhängig vom jeweiligen iQ.Suite Jobtyp. Im iQ.Suite Watchdog können z.B. die gewünschten Virenscanner gewählt oder beim iQ.Suite Wall Content Filtering kann eingestellt werden, welcher Teil mit welchen Wortlisten auf Inhalt geprüft werden soll.

4.2.2 iQ.Suite Aktionen

Erfüllt eine E-Mail alle Bedingungen eines iQ.Suite Jobtyps, so können unterschiedliche Aktionen ausgeführt werden. Die Aktionen sind für die iQ.Suite Jobtypen in vielen Bereichen identisch. Die folgende Übersicht zeigt ein paar Beispiele für die Bedingungen und Aktionen je iQ.Suite Jobtyp.

	Bedingungen							*Aktionen (Auszug)*			
iQ.Suite Jobtyp	**Absender/Empfänger Prüfung**	**Anzahl Empfänger**	**E-Mail Größe**	**Fingerprint Auswahl**	**Virenscanner**	**Inhaltsprüfung**	**Dateityp/Grösse**	**E-Mail in Quarantäne kopieren**	**Externe Anwendung starten**	**Betroffene E-Mail löschen**	**Betroffene Anhänge löschen**
iQ.Suite Watchdog Virus Scanning	X	-	-	-	X	-	-	X	X	X	X
iQ.Suite Watchdog E-Mail 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 E-Mail 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

Im iQ.Suite Monitor werden alle Server, Quarantänen und Bad-Mails beobachtet. Um einen Server überall im Zugriff zu haben, muss er in der Basis-Konfiguration unter iQ.Suite Servers eingetragen sein.

Der iQ.Suite Monitor erfordert außerdem eine Anmeldung als autorisierter Benutzer. Diese Berechtigung wird in den Security-Eigenschaften des Quarantäneverzeichnisses auf jedem iQ.Suite Server eingetragen (`.. \GrpData\Quarantine` → **Eigenschaften** → Registerkarte **Sicherheit**).

Die Anmeldung auf mehreren Servern gleichzeitig ist möglich.

4.4 Quarantänen

Alle aussortierten E-Mails können in die iQ.Suite Quarantäne gestellt werden. An dieser Stelle werden folgende verfügbaren Informationen zu den einzelnen Mails hinterlegt:

- E-Mail-Betreff
- Datum/Uhrzeit
- E-Mail-Sender
- E-Mail-Empfänger
- Kurzbeschreibung der entdeckten Restriktion
- E-Mail-Größe
- Name des iQ.Suite Jobs, der diese E-Mail in Quarantäne stellte
- Name des Exchange-Servers
- Name der E-Mail-Datei
- Bearbeitungshistorie

Beim Anzeigen einer iQ.Suite Quarantäne mit der iQ.Suite Konsole werden zunächst die Informationen aus der Quarantänedatenbank angezeigt. Beim Öffnen eines Quarantäneeintrags werden weitere Informationen aus der E-Mail-Datei geladen.

Die Kommunikation mit der iQ.Suite Quarantäne erfolgt mit Hilfe von SOAP (Simple Object Access Protocol) und SSL (Secure Socket Layer). Dies gilt sowohl für den lokalen Zugriff auf den Server als auch für den Zugriff von einer entfernten Windows Workstation. Dabei wird für die Kommunikation standardmäßig der Port 8008 verwendet, der in der iQ.Suite Konsole verändert werden kann.

Wenn eine E-Mail aus der Quarantäne wieder dem ursprünglichen oder einem weiteren Empfänger zukommen soll, kann Sie direkt aus der Quarantäne versendet werden, ohne dass sie erneut von einem iQ.Suite Job abgefangen wird.

4.5 Bad-Mail Quarantäne

E-Mails, die z. B. auf Grund korrupter Formatierung nicht vollständig von der iQ.Suite verarbeitet werden können, werden in die Bad-Mail Quarantäne gestellt. Darüber hinaus werden dort E-Mails abgelegt, die die maximal erlaubte Entpackungstiefe überschreiten oder passwortgeschützte Archive beinhalten. Passwortgeschützte Archive können auch an den Empfänger durchgeleitet werden (siehe dazu auch Kapitel 7.1, Parameter **BadmailArchives**). Diese Mails können analog der iQ.Suite Quarantäne weiterverarbeitet werden. Über jede E-Mail, die in die Bad-Mail Quarantäne gestellt wird, erhält der Administrator eine E-Mail-Benachrichtigung.

5 iQ.Suite Watchdog

iQ.Suite Watchdog überprüft E-Mails auf Viren, auf Typ und Größe eines Anhangs sowie auf die Gesamtgröße. iQ.Suite Watchdog wird von iQ.Suite Service während der Mailverarbeitung aufgerufen.

Folgende Jobtypen können im iQ.Suite Watchdog konfiguriert werden:

- Virenprüfung mit Hilfe von eingebundenen Virenscannern

  Jobtyp: iQ.Suite Watchdog Virus Scanning

- Sperren von bestimmten Dateitypen im Anhang

  Jobtyp: iQ.Suite Watchdog Attachment Filtering

- Beschränkung der E-Mail-Größe

  Jobtyp: iQ.Suite Watchdog E-Mail Size Filtering

- Beschränkung von Typ und/oder Größe der Anhänge

  Jobtyp: iQ.Suite Watchdog Attachment/Size Filtering

In den nachfolgenden Abschnitten wird das Virus Scanning und das Attachment Filtering mit Hilfe von Fingerprints näher erläutert.

5.1 Virus Scanning

Die Virenprüfung erfolgt grundsätzlich durch einen oder mehrere Virenscanner von Drittherstellern. Diese Virenscanner sind entweder auf dem Exchange-Server installiert oder über eine Netzwerkverbindung erreichbar und werden nach entsprechender Konfiguration von iQ.Suite Watchdog gestartet. iQ.Suite Watchdog ruft die Virenscanner durch das sogenannte GROUP Anti-Virus Interface - eine DLL-Datei - auf, die sich im gleichen Verzeichnis befinden muss wie die Pattern-Datei des Virenscanners.

iQ.Suite Watchdog unterstützt Virenscanner führender Hersteller, wie z.B. Sophos und Avira.

5.1.1 Ablauf des Virus Scanning

Der iQ.Suite Watchdog Virus Scanning Job startet gemäß den konfigurierten Bedingungen die oder den ausgewählten Virenscanner. Sind mehrere Virenscanner ausgewählt, so werden die E-Mails nacheinander von den ausgewählten Scannern auf Viren geprüft.

Bei der Bearbeitung durch iQ.Suite Watchdog Virus Scanning Job stehen grundsätzlich zwei Möglichkeiten zur Verfügung:

- Scannen nach Viren und entfernen der virulenten Anhänge
- Scannen nach Viren und reinigen der virulenten Anhänge

Schritte beim Scannen und Entfernen der virulenten Anhänge

1. Die aktivierten Virenscanner prüfen entsprechend der Reihenfolge im iQ.Suite Watchdog Job nach Viren. Sobald eine Virenscanner einen Virus entdeckt, wird das Scannen beendet.
2. Der als virulent erkannte Anhang wird aus der E-Mail herausgelöst. Je nach Konfiguration wird die komplette E-Mail zusätzlich in Quarantäne gestellt.

Schritte beim Scannen und Reinigen der virulenten Anhänge

1. Die aktivierten Virenscanner prüfen entsprechend der Reihenfolge im iQ.Suite Watchdog Job nach Viren. Sobald ein Virenscanner einen Virus erkannt hat, wird das Scannen beendet.
2. Dieser Virenscanner wird nun verwendet, um den Virus zu entfernen.
3. Die aktivierten Virenscanner prüfen nun entsprechend der festgelegten Reihenfolge, ob der Virus tatsächlich entfernt wurde. Ist dies der Fall, wird entsprechend der Konfiguration die E-Mail zugestellt oder weitere Aktionen ausgelöst. Wird in dem geprüften Anhang nach wie vor ein Virus entdeckt, so werden die Aktionen bzgl. der Scannen-/Entfernen-Modi ausgeführt.

5.2 Fingerprints

Fingerprints werden von iQ.Suite Watchdog zur Dateityperkennung benutzt. Ein Fingerprint besteht aus einem Namensmuster und/oder einem Binärmuster.

- Namensmuster: Damit können Fingerprints anhand von Dateinamen und -erweiterung (*.exe, ...) konfiguriert werden.
- Binärmuster: Damit können Fingerprints anhand von eindeutigen binären Dateiinformationen konfiguriert werden.

Mit dem Namensmuster sind natürlich auch Manipulationen möglich, da (wenn die Anwender davon wissen) einfach die Erweiterung geändert werden kann. Das Binärmuster ist eine eindeutige Zuordnung zu einem Format und lässt sich in der Datei nicht manipulieren. Somit ist der sichere Weg, ein Dateiformat zu erkennen, die Eingabe eines Binärmusters.

Mit Namensmustern ist es aber möglich, auf neue Virusattacken schnell zu reagieren:

Sobald bekannt ist, mit welchen Anhansnamen ein neuer Virus verbreitet wird (Beispiel: Nimda Virus = readme.exe) kann die Virusattacke abgewehrt werden, noch bevor ein Virus Pattern Update des Anti-Virus Herstellers verfügbar ist. Der Dateiname wird einfach mit dem Namensmuster als neuer Fingerprint angelegt.

Setzt ein Unternehmen Individualsoftware ein, die ein eigenes Dateiformat erzeugt, kann dafür ebenfalls ein Fingerprint erstellt und somit beispielsweise verhindert werden, dass solche Dateien das Unternehmen per E-Mail verlassen.

Im Binärmuster sind drei Angaben enthalten:

- Startposition: Legt innerhalb der Datei die Anfangsposition für die Suche nach einem Muster fest.
  - "1", "2"... : Beginn mit dem ersten, zweiten ... Byte
  - "-1", "-6"... : Beginn mit dem letzten, sechstletzten ... Byte
- Endposition: Legt innerhalb der Datei die Position fest, bis zu der nach einem Muster gesucht werden soll.
  - "-1": Suche bis zum Ende der Datei
  - "1", "2": Suche bis zum ersten, zweiten ... Byte
- Hexadezimaler Wert: Beschreibt das Muster, nach dem zwischen Start- und Endposition gesucht wird.

Ein Fingerprint kann aus mehreren Binärmustern bestehen. Eine ZIP-Datei etwa ergibt folgendes Muster:

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

Komplexer ist da schon ein Windows Meta File (WMF):

- Start: 1 Ende: -1 Hex: 576F72642E446F63756D656E74
- Start: 1 Ende: -1 Hex: 57006F007200640044006F00630075006D0065006E0
- Start: 1 Ende: 10 Hex: D0CF11E0A1B11AE10000

Die Fingerprint-Liste der iQ.Suite enthält etwa 350 Einträge, darunter ca. 100 mit Binärmuster. Die Liste ist in verschiedene Kategorien unterteilt z.B. E-Mail-Anhänge, Executables, ASCII, Sound, Images, Fonts. Neue Kategorien können nach Belieben hinzugefügt werden. Dank der offenen Fingerprint-Architektur können auch eigene Fingerprints erstellt werden oder bestehende geändert werden.

6 iQ.Suite Trailer

Mit dem Modul iQ.Suite Trailer werden zentral generierte E-Mail-Signaturen auf Basis der im Active Directory (AD) hinterlegten Exchange-Nutzerinformationen erzeugt. Dies können beispielsweise Benutzersignaturen oder auch Haftungsausschlüsse sein. iQ.Suite Trailer garantiert Aktualität, Richtigkeit und vor allen Dingen die Einheitlichkeit der Informationen.

Das Active Directory wird verwendet, weil seine Domänenstruktur einfach zu pflegen und leicht um Objekte und Eigenschaften zu erweitern ist. Für den Zugriff auf domänenübergreifende Informationen steht der Global Catalog zur Verfügung. Dieser entspricht einem Index, der die relevanten Informationen aller Benutzer eines Active Directories beinhaltet. Der iQ.Suite Trailer verwendet den Global Catalog, um die gewünschten Benutzerinformationen zu erhalten. Es werden dabei keinerlei Veränderungen am Active Directory vorgenommen. Vielmehr handelt es sich um rein lesende Zugriffe.

Alle Informationen, die rund um den einzelnen Benutzer vorhanden sind, können für die E-Mail-Signatur genutzt werden. Welche Informationen letztlich in die E-Mails integriert werden, hängt von der Konfiguration von iQ.Suite Trailer ab.

Der Administrator kann über die MMC die gewünschte Benutzersignatur zusammenstellen. Dabei stehen zunächst die folgenden Informationen zur Verfügung:

```
Abteilung
Anrede
Anzeigename
Bundesland
Büro
E-Mail
Fax
Firma
Land/Region
Nachname
Ort
Postfach
Postleitzahl
Straße
Telefon (Büro)
Telefon (mobil)
Telefon (privat)
Vorname
Webseite
```

Der Aufbau sieht grundsätzlich wie folgt aus:

[VAR]Active Directory Attributname;Standardwert[/VAR]

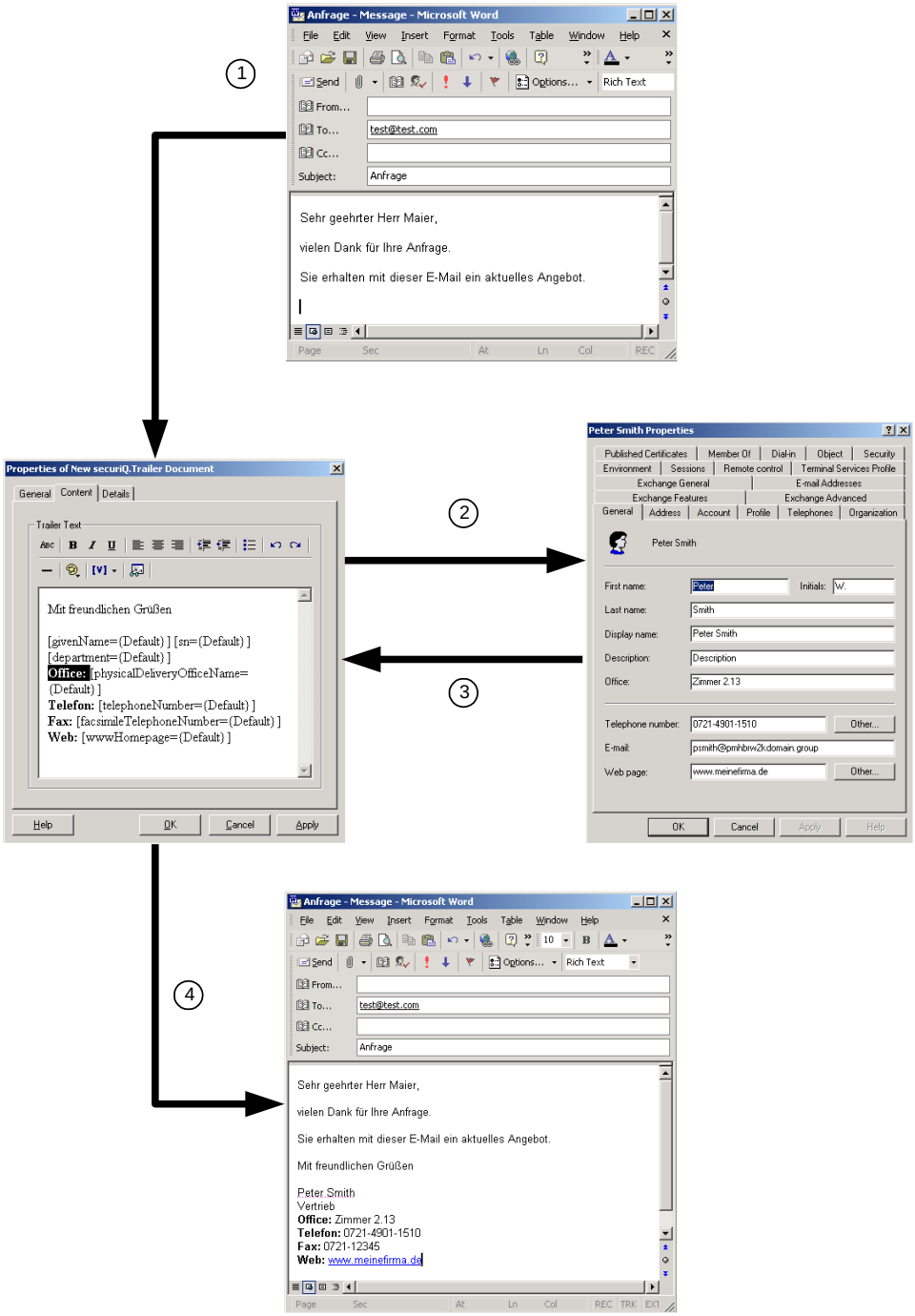
Beispiel für eine Absendersignatur:

[VAR]givenName[/VAR] [VAR]sn[/VAR]
[VAR]physicalDeliveryOfficeName;[/VAR]
Telefon: [VAR]telephoneNumber;0123-456[/VAR]
Fax: [VAR]facsimileTelephoneNumber;987-6543[/VAR]
E-Mail: [VAR]mail[/VAR]

Darüber hinaus kann jeder andere Wert aus dem Active Directory bzw. Global Catalog „angezapft“ werden. Verwendet ein Unternehmen beispielsweise benutzerdefinierte Attribute im AD um die Personalnummern zu hinterlegen, können auch diese Informationen von iQ.Suite Trailer genutzt werden. Ist ein Wert für den Benutzer nicht vorhanden, lässt sich ein Standardwert einfügen. Die Feldbezeichnungen des Active Directories können beispielsweise mit dem Windows 2000 Resourcekit Tool „ADSI Edit“ recherchiert werden.

Beim Einsatz von iQ.Suite Trailer sollten die Outlook-basierten Absendersignaturen deaktiviert werden. Damit wird gewährleistet, dass keine individuellen Signaturen in die E-Mails integriert werden. Dies kann über die Windows Group Policies zentral erreicht werden.

Anhand der folgenden Abbildung wird der prinzipielle Ablauf beim Einfügen einer Benutzersignatur beschrieben.



1. Der Benutzer verfasst und versendet eine E-Mail (ohne Signatur).
2. Der iQ.Suite Trailer hängt die vorgesehene Signatur an und "fragt" das Active Directory nach den betreffenden Benutzerinformationen.

3. Das Active Directory liefert die gewünschten Inhalte. Falls keine Informationen vorhanden sind, verwendet iQ.Suite Trailer die Standardwerte.
4. Die Informationen werden an die richtige Stelle in der Signatur integriert; die E-Mail wird verschickt.

7 Windows Registry

Bei der Installation der iQ.Suite werden einige Registryschlüssel erstellt. Diese Einträge verwendet sowohl der iQ.Suite Server als auch die iQ.Suite Konsole.

Die Schlüssel befinden sich unter

```
HKEY_LOCAL_MACHINE\SOFTWARE\GROUP TECHNOLOGIES\iQ.Suite
```

Darunter existieren weitere Schlüssel

a. General (z.B. Standardpfade)
b. Grabber (Konfiguration der iQ.Suite Event Sinks in der SMTP Advanced Queue)
c. Inject (Pfad zum Exchange Pickup-Verzeichnisses)
d. Logging (Debuglog Einstellungen)

Im Folgenden eine Liste der wichtigsten Schlüssel.

7.1 General

Parameter Name	*Typ*	*Mögliche Werte*	*Beschreibung*
Code	STRING	Pfad	Pfad zum Programmverzeichnis
Data	STRING	Pfad	Pfad zum Datenverzeichnis
InQ	STRING	Pfad	iQ.Suite In-Queue
Config	STRING	Pfad	Pfad zur Konfigurationsdatei
Language	STRING	Pfad	Pfad zur Sprachversionsdatei
ADContextResetTime	DWORD	Positive Zahl	Intervall für die Aktualisierung der Informationen aus dem Active Directory (z.B. Benutzer und Gruppen). Default: 3600 = 1 Stunde
LDIF	STRING	Pfad	Pfad zur LDIF-Datei. Standardmäßig konfiguriert für die iQ.Suite für SMTP. Kann für die iQ.Suite für Exchange ebenfalls gesetzt werden.

Parameter Name	Typ	Mögliche Werte	Beschreibung
BadmailArchives	DWORD	0, 1	Archive, die nicht ausgepackt werden können, werden in den Bad-Mail-Bereich verschoben (1, Default) oder an den Empfänger durchgeleitet (0). Der Parameter wird versteckt per Default gesetzt und muss bei gewünschter Änderung manuell in die Registry eingetragen werden.

7.2 Grabber

Parameter Name	Typ	Mögliche Werte	Beschreibung
ActiveEvent	DWORD	1=OnSubmission 2=OnPreCategorize 3=OnPostCategorize	Parameter für den tatsächlichen Verarbeitungsstartpunkt. Default = 3.
ActionMode	DWORD	0=OFF 1=NORMAL	0: Komplettes Deaktivieren der iQ.Suite auf dem Server. 1: Normale Verarbeitung durch die iQ.Suite
Logging	DWORD	1=ACTIVE 0=INACTIVE	Grabber Protokollmodus. Es wird in `<CODE>\LOG\GRABBER.LOG` protokolliert. Default = 0
ADFilterActi	DWORD	1=ACTIVE 0=INACTIVE	Suchanfrage an das Active Directory, ob die Mail eine Systemmail ist. Default Exchange = 1 Default SMTP = 0

7.3 Inject

Parameter Name	Typ	Mögliche Werte	Beschreibung
PickUp	STRING	Pfad	Pfad zum Exchange-Server Pickup-Verzeichnis

7.4 Logging

Parameter Name	Typ	Mögliche Werte	Beschreibung
Enabled	DWORD	0=OFF, 1=ON	Ein- bzw. Ausschalten des iQ.Suite Service Debugger Modus. Es wird in `<CODE>\LOG\EMH.LOG` protokolliert. Default = 0
LogLevel	DWORD	Positive Zahl bis 255	Allgemeine Protokollstufeneinträge basierend auf einer Bit Maske. Die einzelnen Einträge in ihrer Bedeutung: 0= kein Eintrag im Protokoll 1= sehr kritische Fehler 2= kritische Fehler 4= wichtige Informationen 8= Fehler 16= Informationen 32= Warnungen 64= Details 128= umfassende Details Default = 15. Das bedeutet, die ersten vier Einträge (1, 2, 3 und 4) werden protokolliert.

Über GBS

GROUP Business Software ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die IBM und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Weitere Informationen unter www.gbs.com