



# **GROUP.Sandbox**

**Prinzip, Parameter und Konfiguration der  
GROUP.Sandbox.  
Einsatz in iQ.Suite für Lotus Domino**

**Dokumentversion 2.0**

*Think Lotus Think GROUP*

 **GROUP**  
TECHNOLOGIES  
*Email simplified*

## Inhalt

|       |   |    |
|-------|---|----|
| 1     | Aufgabenstellung und Lösung .....                                     | 2  |
| 2     | Manuelle Konfigurationen .....  | 3  |
| 2.1   | Sandbox aktivieren .....  | 3  |
| 2.2   | Sandbox deaktivieren .....  | 3  |
| 3     | Sandbox-Prinzip bei Virensclannern.....                               | 4  |
| 3.1   | Bestandteile der Sandbox.....   | 4  |
| 3.2   | Verarbeitungsablauf.....  | 4  |
| 3.3   | Parameter der SOAP.Defaults.INI und SOAP.INI .....                    | 6  |
| 3.3.1 | Allgemeine Parameter.....   | 6  |
| 3.3.2 | Parameter für temporäre Verzeichnisse.....                            | 9  |
| 3.3.3 | Parameter für das Zeitverhalten der Sandbox-Client-DLL.....           | 10 |
| 3.3.4 | Parameter für das Zeitverhalten der Sandbox-Server-EXE.....           | 13 |
| 3.4   | Automatisches Virenpattern-Update.....                                | 14 |
| 3.4.1 | Besonderheiten der Virensclanner McAfee, Norman und Trend Micro ..... | 14 |
| 3.4.2 | Besonderheiten des Virensclanners Avira AntiVir (SAVAPI3).....        | 15 |
| 3.4.3 | Besonderheiten des Virensclanners Norton (Symantec Scan Engine) ..... | 16 |
| 3.4.4 | Besonderheiten des Virensclanners Sophos AntiVirus unter Windows..... | 16 |
| 3.4.5 | Besonderheiten des Virensclanners Sophos AntiVirus unter Unix .....   | 17 |
| 4     | Besonderheiten bei partitionierten Servern unter Unix .....           | 18 |

## 1 Aufgabenstellung und Lösung

Die *GROUP.Sandbox* ist eine iQ.Suite-Lösung, um Komponenten wie Konverter, Entpacker, Virens Scanner oder Spamanalyzer vollfunktionsfähig in die iQ.Suite zu integrieren. Für jede anzubindende Komponente existiert eine eigene *GROUP.Sandbox*, die als Schnittstelle zum MailGrabber bzw. DatabaseGrabber agiert.

Mithilfe der *GROUP.Sandbox* lässt sich ein Stabilitätsgewinn der Systemumgebung erzielen, indem kritische Prozesse wie Virenprüfung oder Dateianalyseprozesse von der Verarbeitung der Grabber getrennt werden. Ein Absturz oder Deadlock (Verklemmung) des Virens Scanners hat somit keine fatalen Auswirkungen auf die Stabilität des Domino Servers.

Für folgende Komponenten ist in der iQ.Suite eine Sandbox-Lösung implementiert:

| Komponente                                     | iQ.Suite Modul                    |
|--|-----------------------------------|
| Virens Scanner - Integration und Patternupdate | iQ.Suite Watchdog                 |
| Spamanalyzer - Integration und Patternupdate   | iQ.Suite Wall                     |
| Konverter                                      | iQ.Suite Wall                     |
| Entpacker (tk_unpack2.dll)                     | iQ.Suite Wall / iQ.Suite Watchdog |
| S/MIME   | iQ.Suite Crypt                    |
| Textanalyzer                                   | iQ.Suite Wall                     |
| Grafikanalyzer                                 | iQ.Suite Wall                     |
| Anbindung von iQ.Suite Store (tk_archive.dll)  | iQ.Suite Bridge                   |

Die Implementierung und Funktionalität der *GROUP.Sandbox* variiert bei den einzelnen Komponentenarten. In diesem Dokument wird das Sandbox-Prinzip für Virens Scanner sowie der Ablauf beim Virenpattern-Update beschrieben.

## 2 Manuelle Konfigurationen

### 2.1 Sandbox aktivieren

Nach der Installation der iQ.Suite sind die Sandboxes bereits aktiviert und die Sandbox-Dateien im iQ.Suite-Datenverzeichnis installiert, z.B. %ExecDir%\<Virens Scanner>.

Die Virens Scanner werden über die sog. GROUP-Interface-DLL angesprochen. Modifikationen sind im Regelfall nicht erforderlich, außer es handelt sich um

- Komponenten, die regelmäßige Patternupdates oder Engine Updates erfordern (Virens Scanner/Spamanalyzer). Siehe [Automatisches Virens Scanner Update](#).
- Partitionierte Umgebungen. Siehe [Besonderheiten bei partitionierten Servern unter Unix](#).

### 2.2 Sandbox deaktivieren

Konfigurationsdokumente von Sandbox-Komponenten wie z.B. Virens Scanner sollten normalerweise nicht deaktiviert werden, da damit auch der Virens Scanner selbst abgestellt wird. Um eine Sandbox kurzzeitig zu Testzwecken deaktivieren zu können, ohne dass der Virens Scanner ebenfalls deaktiviert wird, gehen Sie wie folgt vor:

1. Öffnen Sie die iQ.Suite.
2. Kopieren Sie das Konfigurationsdokument der Sandbox-Komponente die Sie deaktivieren möchten. Um beispielsweise die Sandbox des Virens Scanners Trend Micro zu deaktivieren, kopieren Sie unter **Watchdog --> Utilitys --> Virens Scanner** das Konfigurationsdokument „TrendMicro (scan engine)“.
3. Ändern Sie in der Kopie unter **Settings --> Aufruf Scan** den Pfad der Sandbox-Client-DLL, z.B. von %ExecDir%\trend\soap.ntk\_trend.dll auf %ExecDir%\trend\ntk\_trend.dll.
4. Aktivieren Sie die Kopie und deaktivieren Sie das Original-Konfigurationsdokument.

Durch Umschalten zwischen den Konfigurationsdokumenten kann die Sandbox aktiviert bzw. deaktiviert werden.

### 3 Sandbox-Prinzip bei Virensclannern

Das Sandbox-Prinzip und der Verarbeitungsablauf der einzelnen Sandbox-Bestandteile wird anhand des Virensclanners Trend Micro (<trend>) beschrieben.

#### 3.1 Bestandteile der Sandbox

Eine Virensclanner-Sandbox besteht mindestens aus den in der Tabelle beschriebenen Dateien:

| Nr | Dateien - Windows                 | Dateien - Unix                   | Aufgabe   |
|----|-----------------------------------|----------------------------------|---|
| 1  | ntk_<trend>.dll                   |                                  | GROUP-Interface-DLL; Schnittstelle zum Drittherstellerprodukt   |
| 2  | soap.ntk_<trend>.dll              | soap.tk_<trend>.dll              | Sandbox-Client-DLL  |
| 3  | ntk_<trend>.dll.exe               | soap.tk_<trend>.dll.srv          | Sandbox-Server-EXE  |
| 4  | soap.ntk_<trend>.dll.defaults.ini | soap.tk_<trend>.dll.defaults.ini | SOAP.Defaults.INI; GROUP-Konfigurationsdatei mit den Defaulteinstellungen der Sandbox   |
| 5  | soap.ntk_<trend>.dll.ini          | soap.tk_<trend>.dll.ini          | SOAP.INI; (optional) Modifizierbare Version der SOAP.Defaults.INI zur Anpassung der Default-Einstellungen der Sandbox         |
| 6  | ntk_<trend>_ref.cfg               | tk_<trend>_ref.cfg               | Komponentenspezifische Konfigurationsdatei, die von der Sandbox-Server-EXE über ein Updateprogramm aufgerufen wird (optional) |

#### 3.2 Verarbeitungsablauf

Die Sandbox-Server-EXE führt Engine Updates selbständig durch:

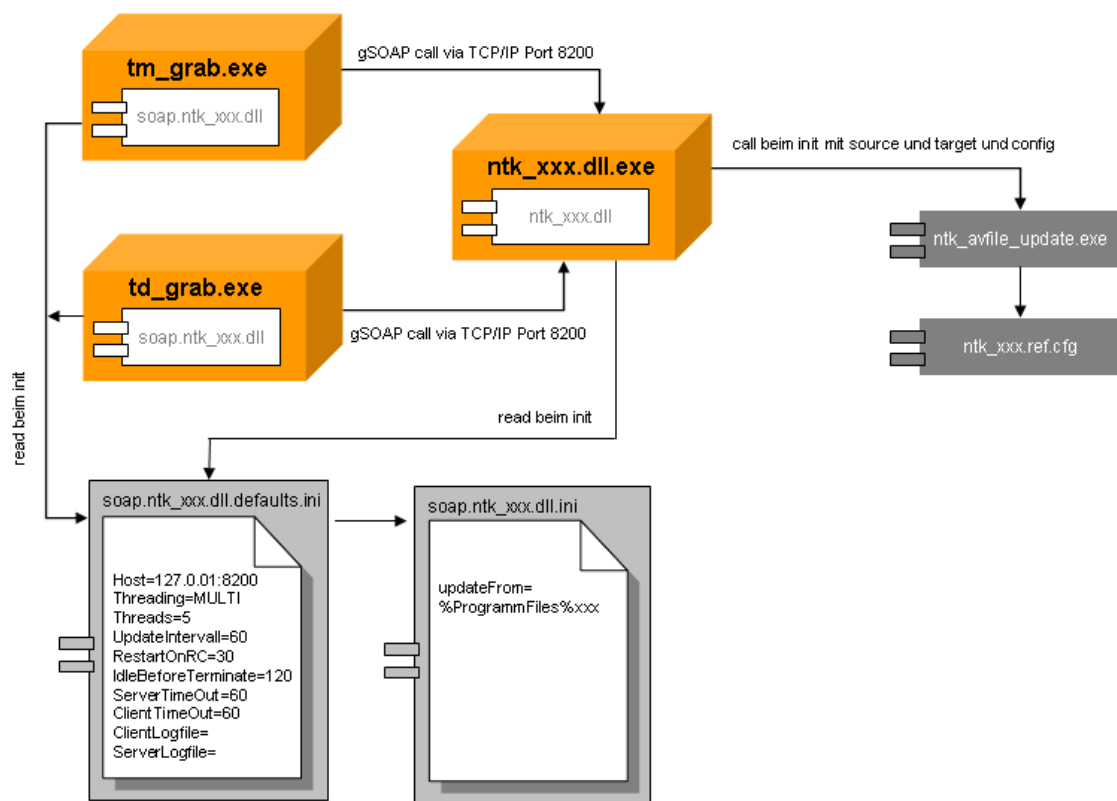
1. Sobald der für den Virensclanner erforderliche Watchdog-Job startet, wird die Sandbox-Client-DLL (**2**) vom Grabber angesprochen und automatisch geladen.
2. Die Sandbox-Client-DLL sorgt für den Start der Sandbox-Server-EXE (**3**). Die Kommunikation beider Dateien erfolgt via TCP/IP mithilfe der sog. gSOAP-Implementierung des SOAP-Protokolls<sup>1</sup>. Bei der Verarbeitung übernimmt die Sandbox-Server-EXE die Rolle eines Sandbox Servers und die Sandbox-Client-DLL die eines Sandbox Clients.
3. Beim Start der Sandbox-Server-EXE wird die GROUP-Interface-DLL (**1**) geladen, z.B. GAPI (**GROUP Application Programming Interface**), GAVI (**GROUP AntiVirus Interface**), Entpacker, o.a. Diese sorgt für die Kommunikation mit dem Drittherstellerprodukt.

<sup>1</sup> Ausführliche Informationen zu gSOAP finden Sie unter <http://qsoap2.sourceforge.net>

4. Sandbox-Server-EXE (3) und Sandbox-Client-DLL (2) laden die SOAP.Defaults.INI (4) sowie die SOAP.INI (5) und werten die darin enthaltenen Sandbox-Einstellungen aus. (4) enthält voreingestellte Konfigurationen, die bei jedem iQ.Suite Update automatisch mit den Defaultwerten überschrieben werden. (5) können Sie modifizieren, um die für Ihre Umgebung relevanten Einstellungen vorzunehmen. Die Einstellungen in (5) haben dabei Vorrang vor denen der (4).
5. Falls eine Konfigurationsdatei (6) enthalten ist (hier: (n)tk\_trend\_ref.cfg), dann wird auch diese von der Sandbox-Server-EXE über ein Updateprogramm aufgerufen.

Pro Sandbox wird unabhängig der Anzahl an konfigurierten iQ.Suite-Jobs immer nur eine Sandbox-Server-EXE gestartet. In iQ.Suite-Konfigurationen, in denen z.B. für einen Virenschanner sowohl ein Mail-Job als auch ein Datenbank-Job konfiguriert ist, wird die Sandbox-Server-EXE nur einmal gestartet und von MailGrabber und DatabaseGrabber gemeinsam genutzt. Die Sandbox-Client-DLL wird dagegen sowohl vom MailGrabber als auch vom DatabaseGrabber separat geladen.

**Hinweis:** Wenn  $n$  verschiedene Virenschanner auf demselben System verwendet werden, werden auch  $n$  Sandbox-Server-EXE gestartet. Hierzu sind in den Standardkonfigurationen der Sandboxes  $n$  TCP-Ports vorkonfiguriert, z.B. Port 8200 für Trend Micro, Port 8210 für McAfee VirusScan, etc.



### 3.3 Parameter der SOAP.Defaults.INI und SOAP.INI

Mit der SOAP.Defaults.INI (*soap.ntk\_<xxx>.dll.defaults.ini*) und der SOAP.INI (*soap.ntk\_<xxx>.dll.ini*) wird das Verhalten der Sandbox konfiguriert.

Die SOAP.Defaults.INI enthält die Default-Einstellungen der Sandbox inkl. der Standard-Portnummer. Wenn Sie das Sandbox-Verhalten ändern möchten, nehmen Sie diese Änderungen in der SOAP.INI statt der SOAP.Defaults.INI vor. Anderenfalls werden Ihre Änderungen nach einem Update der iQ.Suite mit den Default-Werten der SOAP.Defaults.INI überschrieben.

Die Einstellungen in der Datei SOAP.INI haben Vorrang vor denen in der SOAP.Defaults.INI. In beiden Dateien können die im Folgenden beschriebenen Parameter gesetzt werden.

**Hinweis:** Bei Parametern für Datei- und Verzeichnisnamen kann ein absoluter oder relativer Name angegeben werden. Relative Namen werden als relativ zur Parameterdatei interpretiert.

#### Beispiel:

Relativer Pfad: %ExecDir%\trend\soap.ntk\_trend.dll.ini

Angegebene Logdatei: ..\logs\trendmicro.log

Resultat: Es wird nach %ExecDir%\logs\trendmicro.log geloggt.

#### 3.3.1 Allgemeine Parameter

Je nachdem, ob mit der Sandbox ein Entpacker, Virenschanner oder Analyzer angesprochen wird, stehen in dieser Datei unterschiedliche Parameter zur Verfügung. Zu den Parametern, die im Regelfall in jeder SOAP.Defaults.INI oder SOAP.INI enthalten sind, gehören:

- Host=<IP-Adresse>:<TCP-Portnummer>  
IP-Adresse und TCP-Portnummer, die von der Sandbox genutzt werden. Die IP-Adresse lautet 127.0.0.1, da nur lokale Verbindungen erlaubt sein sollen. Der TCP-Port muss sich zwischen verschiedenen Sandboxes unterscheiden, damit sie sich nicht gegenseitig behindern. Siehe [Besonderheiten bei partitionierten Servern unter Unix](#).
- Threading=[MULTI | SINGLE]
- Threads=<Anzahl möglicher Threads bei Multithreading>  
Stellt den Grad der Parallelverarbeitung in der Sandbox-Server-EXE ein. Default: 5
- ClientLogFile=<Name der Logdatei>  
Protokolliert Meldungen der Sandbox-Client-DLL.
- ServerLogFile=<Name der Logdatei>

Protokolliert Meldungen der Sandbox-Server-EXE. Falls kein absoluter Dateiname angegeben ist, werden beide Parameter im selben Verzeichnis angelegt, in dem sich auch die anderen Sandbox-Dateien befinden.

Relative Dateinamen beziehen sich auf den Ablageort der INI-Datei.

Zur Fehleranalyse kann im Dateinamen das Metasymbol %ID% verwendet werden, das beim Anlegen der Logdatei durch eine zeitabhängige Zeichenkette ersetzt wird. Dadurch wird verhindert, dass vorhandene Logdateien beim Start von Sandbox-Client-DLL und Sandbox-Server-EXE überschrieben werden. Beachten Sie, dass der Bestand an Logdateien manuell bereinigt werden muss.

**Beispiel 1:**

```
ClientLogFile=tk_trend_client_%ID%.log  
ServerLogFile=tk_trend_server_%ID%.log
```

**Beispiel 2:**

Um das Logging zu deaktivieren, setzen Sie den Dateiname auf einen Leerstring:

```
ClientLogFile=  
ServerLogFile=
```

- `ServerDirectory=<Name des Verzeichnisses der Sandbox-Server-EXE>`  
(optionaler Parameter) Da bestimmte Dateien im selben Verzeichnis abgelegt sein müssen, werden Server- und Clientdateien standardmäßig im selben Verzeichnis abgelegt. Um Server- und Clientkomponenten dennoch trennen zu können, empfehlen wir, den Parameter `ServerDirectory` zu verwenden. Wenn Sie diesen Parameter in einer der INI-Dateien setzen, müssen lediglich die INI-Dateien im gleichen Verzeichnis wie die Sandbox-Client-DLL abgelegt sein.

**Hinweis:** Über eigene Konfigurationsparameter verfügende Dateien, z.B. Logdateien, sind von diesem Parameter nicht betroffen. Sie müssen bei Bedarf einzeln im Serververzeichnis abgelegt werden. Alle anderen Dateien werden im angegebenen Serververzeichnis erwartet. Das sind insbesondere die GROUP-Interface-DLL, die in der Sandbox laufen soll und die Sandbox-Server-EXE. Beachten Sie, dass ggf. auch in anderen Parametern die Pfadangaben angepasst werden müssen.

- `LibraryPath=<Pfadangabe zum gewünschten Verzeichnis>`  
(nur in Unix-Systemen) Ermöglicht die Verwendung zusätzlicher Verzeichnisse im Bibliothekssuchpfad. Unter Linux/Solaris: `LD_LIBRARY_PATH`, unter AIX: `LIBPATH`. Standardmäßig ist das Verzeichnis angegeben in dem die `SOAP.Defaults.INI` bzw. `SOAP.INI` abgelegt ist (`LibraryPath=.`). Geben Sie bei Bedarf den Pfad zum Verzeichnis an.

**Beispiel:**

```
LibraryPath=/opt/<virusscanner>/lib
```

Mehrere Verzeichnisse werden mit Doppelpunkt getrennt.

**■ EnvVar=<Name>=<Value>**

Setzt in der Sandbox-Server-EXE die Umgebungsvariable "Name" auf den Wert "Value".

**■ EnvPath=<Name>=<Pfadname>**

Setzt in der Sandbox-Server-EXE die Umgebungsvariable "Name" auf den Wert „Pfadname“. Wenn kein absoluter Pfad angegeben ist, so wird er relativ zur SOAP.Defaults.INI bzw. SOAP.INI interpretiert und in einen absoluten Pfad umgewandelt.

**Beispiel:**

```
EnvPath=MyDir=.
```

```
in C:\lotus\domino\data\iQ.Suite\subdir
```

entspricht `EnvVar=MyDir=C:\lotus\domino\data\iQ.Suite\subdir`

### 3.3.2 Parameter für temporäre Verzeichnisse

- `TmpDir=<Name des neuen temporären Verzeichnisses der Sandbox>`

Dieser Parameter ergänzt in der Sandbox die Umgebungsvariablen `TEMP`, `TMP` und `TMPDIR`. Es sollte auf diesem Verzeichnis kein On-Access-Virens Scanner laufen.

Default=Leerstring

**Beispiel:** `TmpDir=`
- `CleanTmpDir=<Wert>`

Bei jedem Start der Sandbox-Server-EXE werden die Inhalte des bei `<TmpDir>` angegebenen Verzeichnisses gelöscht. Voraussetzung ist, dass das bei `<TmpDir>` angegebene Verzeichnis „tmp“ oder „temp“ heißt oder auf „.tmp“ endet.

Mögliche Werte: „yes“, „no“; Default: „no“

**Hinweis:** Konfigurieren Sie bei `<TmpDir>` ein eigenes exklusives Verzeichnis, um Datenverlust zu vermeiden.
- `ExtraTmpVariable=<Name der Umgebungsvariablen>`

(nur in Einzelfällen einzusetzen) Mit diesem Parameter kann eine weitere Umgebungsvariable angegeben werden, die zusätzlich zu `TEMP`, `TMP` und `TMPDIR` gesetzt wird.

Zum Beispiel können Sie bei Einsatz des Virens Scanners Sophos AntiVirus den Parameter folgendermaßen setzen: `ExtraTmpVariable=SAV_TMP`.

Default=Leerstring
- `OnAccessScanCheck=<Wert>`

Dieser Parameter bewirkt auf On-Access-Virens Scannern eine Prüfung des bei `<TmpDir>` angegebenen Verzeichnisses. Mögliche Werte: „yes“, „no“; Default: „yes“

### 3.3.3 Parameter für das Zeitverhalten der Sandbox-Client-DLL

Timeouts der Sandbox-Client-DLL treten auf, wenn der konfigurierte Zeitraum zur Verarbeitung von Aktionen der Sandbox-Server-EXE überschritten wird. Zu den Aktionen der Sandbox-Server-EXE zählen Virenprüfung, Spamprüfung, Entpacken, Initialisieren von Virenschannern und Analyzern, etc.

Das Zeitverhalten der Sandbox-Client-DLL wird im Regelfall durch nachfolgende Parameter konfiguriert:

- `ClientTimeoutIO`=<Zeit in Sekunden bis zum Timeout durch den Client>  
Wenn die Sandbox-Server-EXE bei der Ausführung einer Aktion das hier angegebene Zeitintervall überschreitet, beendet die Sandbox-Client-DLL die Sandbox-Server-EXE und führt einen Neustart der Sandbox-Server-EXE durch.  
**Hinweis:** Da erfahrungsgemäß die Initialisierung von Virenschannern oder Analyzern am zeitintensivsten ist, empfehlen wir die kalkulierte Initialisierungszeit als Zeitintervall anzugeben. Mit der Defaulteinstellung wird nach 120 Sekunden abgebrochen.
- `ClientTimeoutMin`=<Zeit in Sekunden bis der Client einen Fehler feststellt>  
Wenn Aktionen nicht ausgeführt werden können, z.B. bei Überschreitung des Parameters `ClientTimeoutIO`, durch Absturz der Sandbox-Server-EXE oder aufgrund eines schwerwiegenden Serverfehlers, wird die Aktion wiederholt.  
Mit den beiden Parametern `ClientTimeoutMin` und `ClientTimeoutMax` können Sie das Zeitintervall für diesen Versuch angeben. Mit der Defaulteinstellung wird im Zeitraum von 360 Sekunden versucht, die Aktion doch noch auszuführen.  
**Hinweis:** Nach Ablauf dieser Frist meldet die Sandbox-Client-DLL einen Fehler, der im Notes-Log vermerkt wird. Temporäre Probleme, die bei einer Wiederholung der Aktion nicht mehr auftreten, erscheinen nur in den Logdateien der Sandbox-Client-DLL und der Sandbox-Server-EXE.
- `ClientTimeoutMax`=<Zeit in Sekunden bis der Client einen Fehler feststellt>  
Default: 360 Sekunden. Standardmäßig ist bei `ClientTimeoutMin` und `ClientTimeoutMax` der gleiche Wert angegeben.

Um die drei zuvor beschriebenen Parameter automatisch setzen zu lassen, verwenden Sie folgenden Parameter:

- `ClientTimeout=<Wert>`

Der Parameter `ClientTimeoutIO` wird auf den angegebenen `<Wert>` gesetzt. `ClientTimeoutMin` und `ClientTimeoutMax` werden auf den dreifachen Wert von `ClientTimeoutIO` gesetzt.

**Hinweis:** Wenn der Parameter `ClientTimeout` sowie einer der anderen Parameter gesetzt ist, gilt der letzte in der Datei angegebene Parameter. D.h., wenn sich der Parameter `ClientTimeout` an letzter Stelle befindet, dann werden alle anderen Parameter ignoriert.

### Besondere Konfiguration

Im Einzelfall kann es sinnvoll sein, für `ClientTimeoutMin` einen kleineren Wert als für `ClientTimeoutMax` anzugeben. In diesem Fall tritt folgendes Timeout-Verhalten auf:

- Beim Start der Sandbox wird davon ausgegangen, dass die Sandbox-Server-EXE funktioniert (Modus 1). Für das Timeout gilt das bei `ClientTimeoutMax` angegebene Zeitintervall.
- Sobald dieses Zeitintervall durch eine nichtausführbare Aktion überschritten und ein Timeout ausgelöst wird, erfolgt ein Wechsel in Modus 2.
- In Modus 2 gilt für das Timeout das bei `ClientTimeoutMin` angegebene Zeitintervall. Bei Ausführung der nächsten Aktion wird folglich schneller ein Timeout ausgegeben, wenn Verzögerungen bei der Ausführung der Aktion auftreten.
- Wird die Aktion dagegen erfolgreich ausgeführt, wird wieder in Modus 1 gewechselt. Als erfolgreich ausgeführte Aktion gilt z.B. eine erfolgreiche Viren- oder Spamprüfung. Eine erfolgreiche Initialisierungsaktion allein führt **nicht** zum Wechsel in Modus 1.

## Beispielkonfigurationen

**Beispiel 1:** Timeout nach einer Minute (Einzelaktion).

```
ClientTimeout=60
```

**Beispiel 2:** Timeout nach einer Minute (Einzelaktion) bzw. drei Minuten (bei Wiederholungen).

```
ClientTimeoutIO=60  
ClientTimeoutMin=180  
ClientTimeoutMax=180
```

**Beispiel 3:** Timeout nach 20 Minuten (Einzelaktion) bzw. drei Minuten (bei Wiederholungen)  
Die Einstellung eines langen Timeouts für Einzelaktionen, aber eines kurzen Timeouts für Wiederholungen kann bei Einsatz des CORE-Analyzers sinnvoll sein. Da der Analyzer zur Ausführung bestimmter Aktionen wie Initialisierung, Teachen, etc längere Zeit braucht, kann die Wartezeit so reduziert werden.

```
ClientTimeoutIO=1200  
ClientTimeoutMin=180  
ClientTimeoutMax=180
```

### 3.3.4 Parameter für das Zeitverhalten der Sandbox-Server-EXE

Das Zeitverhalten der Sandbox-Server-EXE kann mittels nachfolgender Parameter modifiziert werden:

- `IdleBeforeTerminate=<Zeit in Sekunden bis zum Beenden der Sandbox>`  
Wenn im hier angegebenen Zeitraum keine Aktionen ausgeführt werden müssen, dann wird die Sandbox-Server-EXE automatisch beendet. Default: 120 Sekunden.
- `ServerTimeout=<Zeitintervall in Sekunden bis zum Timeout des Servers>`  
Im hier angegebenen Zeitraum prüft die Sandbox-Server-EXE, ob sie noch von einer Sandbox-Client-DLL genutzt wird und ob der bei `IdleBeforeTerminate` eingestellte Zeitraum überschritten ist. Default: 60 Sekunden.

**Hinweis:** Wenn folgende Fehlermeldung in die Server-Logdatei geschrieben wird, dann wurde das Zeitintervall bis zum Timeout des Servers überschritten.

*SOAP FAULT: SOAP-ENV:Server*

*"Timeout"*

*Detail: TCP accept failed in soap\_accept()*

Der Zeitraum ist abgelaufen, ohne dass die Sandbox-Server-EXE eine neue Aktion gestartet hat. Die Meldung führt zu keinem Fehlverhalten der Sandbox-Server-EXE und kann ignoriert werden.

- `TimeLimit=<Zeitintervall in Minuten bis zum Beenden der Sandbox-Server-EXE>`  
Nach Ablauf der angegebenen Frist wird die Sandbox-Server-EXE unabhängig von der Arbeitsauslastung beendet und neu gestartet.
- `CallLimit=<Max. Anzahl an Sandbox-Anfragen>`  
Nach Ablauf der angegebenen Frist wird die Sandbox-Server-EXE unabhängig von der Arbeitsauslastung beendet und neu gestartet. Je nach Typ der Sandbox sind eine oder mehrere Sandbox-Anfragen für eine zu bearbeitende E-Mail oder ein zu bearbeitendes Dokument notwendig.

### 3.4 Automatisches Virenpattern-Update

Die zur Virenprüfung erforderlichen regelmäßigen Virenpattern-Updates stellen ein zentrales Problem dar, da das Updateverfahren vom eingesetzten Virens Scanner abhängt. Wenn erforderlich, werden bestimmte Dateien aus der Installation des Virens Scanners in das iQ.Suite-Verzeichnis des jeweiligen Virens Scanners kopiert. Damit wird erreicht, dass die Originaldateien des Virens Scanners an ihrem ursprünglichen Speicherort nicht durch die iQ.Suite blockiert werden. Der im Virens Scanner enthaltene Updatevorgang – oder ein anderer entsprechender Updatevorgang – sorgt so problemlos für die Dateienaktualisierung.

Sobald neue Dateien vorhanden sind, wird bei der zyklischen Überprüfung des iQ.Suite-Verzeichnisses durch die *GROUP.Sandbox* der Updatevorgang ausgelöst und die Virens Scanner-Dateien in der Sandbox ausgetauscht. Für diesen Prozess muss weder iQ.Suite Watchdog noch der Mail- bzw. DatabaseGrabber neu gestartet werden.

Die für das automatische Virenpattern-Update erforderlichen Parameter sind voreingestellt und müssen im Regelfall nicht angepasst werden. Beachten Sie die Beschreibungen zu den Besonderheiten des jeweiligen Virens Scanners in den Folgekapiteln.

#### 3.4.1 Besonderheiten der Virens Scanner McAfee, Norman und Trend Micro

Die Parameter für das Virenpattern-Update sind zusätzlich zu den regulären Parametern in der SOAP.Defaults.INI und SOAP.INI enthalten. Siehe [Parameter der SOAP.Defaults.INI und SOAP.INI](#) ab Seite 6.

In Windows Systemen sind folgende Parameter für das Update relevant:

- UpdateFrom =<Quellverzeichnis für das Update>  
Die Pfadangabe kann je nach Installationsort des Virens Scanners variieren.
- UpdateInterval=<Prüfintervall für das Update in Minuten>  
Nach Ablauf der angegebenen Frist wird das Virenpattern-Update ausgeführt.  
Default: 60 Minuten.
- UpdateProgram =<Programm, das das Update durchführt>  
Kontrollieren Sie die Pfadangaben zum Updateprogramm.
- UpdateConfig =<Name der Konfigurationsdatei>  
Wenn Sie eine andere Konfigurationsdatei (.cfg) verwenden möchten als die, die im Virens Scannerverzeichnis abgelegt ist, tragen Sie diesen Parameter manuell in die SOAP.INI ein und geben den Namen der gewünschten Konfigurationsdatei an.

Zusätzlich werden für die hier beschriebenen Virens Scanner folgende Dateien für das automatische Update benötigt:

- *ntk\_<Virens Scannername>\_ref.cfg*  
Die in dieser Konfigurationsdatei aufgelisteten Dateien werden aus dem Virens Scannerverzeichnis kopiert. Passen Sie diese Datei nur in Rücksprache mit dem GROUP-Support an.
- *ntk\_avfile\_update.bat* (Windows) bzw. *tk\_avfile\_update.sh* (Unix)  
Programm, das das Programm *ntk\_avfile\_update.exe* aufruft.
- *ntk\_avfile\_update.exe*  
Updateprogramm, das im `bin`-Verzeichnis des iQ.Suite-Programmverzeichnisses abgelegt ist und die Dateien aus dem Virens Scannerverzeichnis kopiert.

**Hinweis:** Alle für den Virens Scanner benötigten Dateien müssen im Unterverzeichnis des jeweiligen Virens Scanners im iQ.Suite-Programmverzeichnis abgelegt sein, z.B. `<iQSuiteProgram>\trend`.

### 3.4.2 Besonderheiten des Virens Scanners Avira AntiVir (SAVAPI3)

In Windows Systemen sind folgende Parameter für das Virenpattern-Update in der SOAP.Defaults.INI und SOAP.INI enthalten:

- `UpdateFrom =<Quellverzeichnis für das Update>`  
Die Pfadangabe kann je nach Installationsort des Virens Scanners variieren.
- `UpdateInterval=<Prüfintervall für das Update in Minuten>`  
Nach Ablauf der angegebenen Frist wird das Virenpattern-Update ausgeführt.  
Default: 60 Minuten.
- `UpdateProgram =<Programm, das das Update durchführt>`  
Kontrollieren Sie die Pfangaben zum Updateprogramm.
- `UpdateConfig =<Name der Konfigurationsdatei>`  
Wenn Sie eine andere Konfigurationsdatei (.cfg) verwenden möchten als die, die im Virens Scannerverzeichnis abgelegt ist, tragen Sie diesen Parameter manuell in die SOAP.INI ein und geben den Namen der gewünschten Konfigurationsdatei an.

- `DownloadFrom`=<Zieladresse des Avira Internet Update Managers>  
Wenn Sie die Updates über einen zentralen Server steuern möchten, dann können Sie den *Avira Internet Update Manager* verwenden. Ein zentraler Server lädt die Updates aus dem Internet und stellt sie als Webserver den einzelnen Clientrechnern zur Verfügung. Die Clientrechner laden die Updates vom zentralen Server.<sup>2</sup>

### 3.4.3 Besonderheiten des Virens scanners Norton (Symantec Scan Engine)

Für den Virens scanner Norton von Symantec verläuft das Virenpattern-Update ohne aktive Interaktion der iQ.Suite. Neue Virenpattern werden automatisch geladen und von der iQ.Suite verwendet. Eine Konfiguration des Updateverfahrens ist nicht nötig.

### 3.4.4 Besonderheiten des Virens scanners Sophos AntiVirus unter Windows

Die Parameter für das Virenpattern-Update sind zusätzlich zu den regulären Parametern in der `SOAP.Defaults.INI` und `SOAP.INI` enthalten. Siehe [Parameter der SOAP.Defaults.INI und SOAP.INI](#) ab Seite 6.

Um das Updateverfahren der *GROUP.Sandbox* zu modifizieren, kopieren Sie in Windows Systemen nachfolgende Parameter aus der `SOAP.Defaults.INI` in die `SOAP.INI`:

- `UpdateFrom` =<Quellverzeichnis für das Update>  
Die Pfadangabe kann je nach Installationsort des Virens scanners variieren.
- `UpdateInterval`=<Prüfintervall für das Update in Minuten>  
Nach Ablauf der angegebenen Frist wird das Virenpattern-Update ausgeführt.  
Default: 60 Minuten.
- `RestartonRc` =<Rückgabewert des Virens scanners>  
Wert: 547; Anhand dieses Rückgabewerts wird die Sandbox neu gestartet
- `DependsOnService` =<ServiceName>  
Name: SAVSERVICE; wird für Sophos AntiVirus (nur WIN32 Plattformen) genutzt, um den Zustand des Update Service prüfen zu können.

---

<sup>2</sup> Weiterführende Informationen zur Installation und Einrichtung des *Avira Internet Update Managers* erhalten Sie auf der Website von Avira [www.avira.com](http://www.avira.com).

**Hinweis:** Alle für den Virenschanner Sophos AntiVirus benötigten Dateien können im Verzeichnis <iQSuite>\sophos abgelegt werden.

### Ablauf des Updates

Da während des Updateprozesses keine Virenprüfung stattfinden darf, wird in diesem Zeitraum der Sophos Service „**SavService.exe**“ gestoppt und erst nach dem Beenden des Updates wieder gestartet. Auf WIN32 Plattformen wird der Status des Services regelmäßig geprüft und die Sophos Scan Engine nur dann initialisiert bzw. aufgerufen, wenn der Service zur Verfügung steht.

Zusätzlich wird ein spezieller Rückgabewert abgefragt. Die Sophos Scan Engine meldet über den Rückgabewert 547, dass ein Update erfolgt ist und die Sandbox-Server-EXE, die den Virenschanner verwendet, neu gestartet werden muss. Dies wird über den Parameter `RestartOnRc` in der `SOAP.Defaults.INI` gesteuert. Wird nun der entsprechende Rückgabewert bei der Virenprüfung zurückgeliefert, wird die Sandbox-Server-EXE beendet und beim nächsten Aufruf automatisch neu gestartet.

## 3.4.5 Besonderheiten des Virenschanners Sophos AntiVirus unter Unix

Die Parameter für das Virenpattern-Update sind in der `SOAP.Defaults.INI` und `SOAP.INI` enthalten. Um das Updateverfahren zu modifizieren, orientieren Sie sich an den Angaben unter [Besonderheiten der Virenschanner McAfee, Norman und Trend Micro](#).

Folgende Parameter sind für das Update relevant:

- `UpdateFrom` =<Quellverzeichnis für das Virenschannerupdate>  
Passen Sie mind. diesen Parameter an. Anderenfalls ist kein Update möglich. Die Pfadangabe kann je nach Installationsort des Virenschanners variieren.
- das Bibliotheksverzeichnis von Sophos AntiVirus darf nicht in der Umgebungsvariablen `LD_LIBRARY_PATH` (Linux/Solaris) bzw. `LIBPATH` (AIX) enthalten sein.

**Hinweis:** Alle für den Virenschanner Sophos AntiVirus benötigten Dateien können im Verzeichnis <iQSuite>\sophos abgelegt werden.

### Ablauf des Updates

Unter Unix werden für das Virenpattern-Update Shell-Skripte statt des Sophos Service verwendet. Die Virenpattern werden selbständig von Sophos AntiVirus aktualisiert und im Installationsverzeichnis von Sophos abgelegt. Die Konfigurationsdatei `ntk_sophos_ref.cfg`

kopiert die Datei *libsavi.so.3* (Linux/Solaris) bzw. *libsavi.a* (AIX) in das iQ.Suite-Programmverzeichnis. Außerdem wird geprüft, ob sich aktualisierte Virenpattern im Verzeichnis befinden. Ist dies der Fall, wird die Sandbox neu gestartet und anschließend die neuen Virenpattern zur Virenprüfung verwendet.

## 4 Besonderheiten bei partitionierten Servern unter Unix

Wenn auf einem Unix-System mehrere Serverinstanzen mit unterschiedlichen Unix-User-IDs betrieben werden, dann läuft die Sandbox-Server-EXE mit der User-ID der Sandbox-Client-DLL, die die Sandbox-Server-EXE gestartet hat. Da jede Sandbox-Client-DLL die Sandbox-Server-EXE bei Bedarf starten kann, kann dessen User-ID variieren.

Allerdings wird auch temporären Dateien eine User-ID zugeordnet, wenn sie E-Mails oder Teile einer E-Mail enthalten und von einer in der Sandbox-Server-EXE laufenden DLL untersucht werden. Beide Faktoren führen zu folgenden Rahmenbedingungen und Beschränkungen:

- Alle Serverinstanzen müssen Schreibzugriff auf die Verzeichnisse haben, in die die Sandbox-Logdateien und die temporären Dateien geschrieben werden.
- Alle Serverinstanzen müssen Lesezugriff auf die temporären Dateien aller anderen Serverinstanzen haben.
- Je nach Implementierung der Reinigungsfunktion kann es erforderlich sein, dass alle Serverinstanzen Schreibzugriff auf die temporären Dateien aller anderen Serverinstanzen haben.
- Falls eine Sandbox-Server-EXE nicht mehr reagiert, kann sie nur von der Sandbox-Client-DLL terminiert werden, die sie gestartet hat.

Um diese Probleme zu umgehen, teilen Sie jeder Serverinstanz eine eigene Sandbox zu. Passen Sie in jeder SOAP.INI den TCP-Port an, indem Sie im Parameter `Host` eine fortlaufende Portnummer für jede Serverinstanz vergeben. Wenn z.B. `Host=127.0.0.1:8200` in jeder SOAP.Defaults.INI voreingestellt ist, dann tragen Sie in der zweiten Serverinstanz `Host=127.0.0.1:8201` und in der dritten Serverinstanz `Host=127.0.0.1:8202` ein.

## Über GROUP Technologies

*GROUP Technologies ist der Geschäftsbereich E-Mail, Archiving & Administration der GROUP Business Software AG*

Durchgängige Kommunikation ist ein wesentliches Kriterium für den Erfolg von Unternehmen. Effiziente E-Mail-Korrespondenz mit Kunden und Geschäftspartnern, aber auch intern entscheidet darüber, ob sich ein Unternehmen von der großen Masse erfolgreich absetzen kann oder ob es lediglich standardisierte Kommunikationsprozesse anwendet.

E-Mail ist nicht mehr nur Mittel zum Zweck der Kommunikation, sondern längst das wichtigste Instrument zur konstruktiven Zusammenarbeit über eine zeitliche bzw. räumliche Distanz hinweg. Gerade diese Tatsache macht E-Mail-Management zu der unternehmenskritischsten Anwendung überhaupt. Zahlreiche interne und externe Risiken, gesetzlichen Vorgaben, Unternehmenspolicies und -standards sind damit verbunden.

GROUP Technologies hat sich deshalb auf die Entwicklung prozessorientierter, zentraler und wartungsfreundlicher E-Mail-Management-Lösungen für die weit verbreiteten Plattformen Lotus Domino und Microsoft Exchange spezialisiert und sich als Anbieter dieser Lösungen weltweit etabliert.

### *GROUP Technologies – Kompetenzen*

**Kompetent:** GROUP Technologies ist für seine Kunden der alleinige Ansprechpartner, wenn es im Bereich E-Mail um Sicherheit, Compliance oder IT-Effizienz geht. Alle unternehmerischen Herausforderungen werden auf Basis eines zentralen und regelbasierten E-Mail-Managements zuverlässig gelöst.

**Zentral:** Umfassender Viren- und Spam-Schutz, automatische Ver- und Entschlüsselung, Durchsetzung von unternehmerischen sowie gesetzlichen Vorgaben und die Realisation einer Echtzeit-Archivierung im kompletten Unternehmen – GROUP Technologies macht die Verwaltung all dieser Prozesse an zentraler Stelle möglich.

**Unkompliziert:** Die E-Mail-Lösungen von GROUP Technologies zeichnen sich durch eine hohe Benutzerfreundlichkeit und einzigartige Effizienz aus. Die serverbasierten Lösungen reduzieren Aufwand und Interaktion seitens der E-Mail-Anwender auf ein absolutes Minimum. Denn die unternehmensweite Einbeziehung der E-Mail-Aktivitäten aller Nutzer geschieht serverseitig und kann auf diese Weise zentral über nur eine einzige Konsole administriert werden.

**Konform:** Zentral definierte Prozesse gewährleisten die Einhaltung von unternehmenseigenen Policies und gesetzlichen Vorgaben bei der E-Mail-Kommunikation. Intuitive Konfigurationsmöglichkeiten erlauben es, die E-Mail-Infrastruktur ohne weiteres an die Anforderungen des Marktes, des Unternehmens oder neuer Gesetze anzupassen.

### *GROUP Technologies – Kunden*

Zu den Kunden des Geschäftsbereiches GROUP Technologies zählen weltweit namhafte Konzerne, wie die Deutsche Bank, Ernst & Young, Honda, Heineken, Allianz und Miele. Mehr als drei Millionen Anwender und über 3.000 Unternehmen weltweit vertrauen die Sicherheit und die Organisation ihrer Systeme den Lösungen der GROUP Technologies an.

© 2010 GROUP Business Software AG

Die Produktbeschreibungen haben lediglich allgemeinen und beschreibenden Charakter. Sie verstehen sich weder als Zusicherung bestimmter Eigenschaften noch als Gewährleistungs- oder Garantieerklärung. Spezifikationen und Design unserer Produkte können ohne vorherige Bekanntgabe jederzeit geändert werden, insbesondere, um dem technischen Fortschritt Rechnung zu tragen. Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der GROUP Business Software AG zum Zeitpunkt der Veröffentlichung dar. Da GROUP Business Software AG auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens der GROUP Business Software AG dar und GROUP kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren. Dieses Dokument dient nur zu Informationszwecken. Die GROUP Business Software AG schließt für dieses Dokument jede Gewährleistung aus, sei sie ausdrücklich oder konkludent. Dies umfasst auch Qualität, Ausführung, Handelsüblichkeit oder Eignung für einen bestimmten Zweck. Alle in diesem Dokument aufgeführten Produkt- oder Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

#### European Headquarters

**GROUP Business Software AG**  
MesseTurm  
60308 Frankfurt/Germany  
Phone: +49 69 789 8819-0  
Fax: +49 69 789 8819-99

#### North American Headquarters

**GROUP Business Software Corporation**  
40 Wall Street, 33rd Floor  
New York, NY 10005/USA  
Phone: +1 212 995-2900  
Fax: +1 212 995-2206

#### Email Main Office

**GROUP Technologies**  
Ottostrasse 4  
76227 Karlsruhe /Germany  
Phone: +49 721 4901-0  
Fax: +49 721 4901-199

#### UK Office

**GROUP Business Software (UK) Ltd.**  
97 Buttermarket Street  
Warrington WA1 2NL/UK  
Phone: +44 1925 624950  
Fax: +44 1925 240211

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



*A Division of GROUP Business Software*