



Installation iQ.Suite 7 for DOMINO R5 AND 6

Editor's Note

All rights reserved. This manual and the programs described therein are copyright-protected products of GROUP Technologies AG, Karlsruhe, Deutschland.

No part of this publication may be reproduced without written permission from GROUP Technologies AG.

All hardware and software names used are registered names and/or trademarks of the manufacturer/proprietor concerned.

Copyright © 2003 GROUP Technologies AG,
Ottostrasse 4, 76227, Karlsruhe, Deutschland

Issue: Mai 2003

 **Contents**

1 Preface	1
1.1 Quality Assurance.....	1
1.2 Hotline	1
1.3 What to Do in the Event of a Fault.....	1
1.4 Copyright	2
1.5 Warranty.....	2
1.6 License Agreement.....	2
1.7 Third-Party Copyright Notes	2
2 Introduction	3
2.1 The Aim of this Guide	3
2.2 Structure of this Guide.....	3
2.3 Product Overview	4
2.3.1 iQ.Suite	4
2.3.1.1 securiQ.....	4
2.3.1.2 organiziQ.....	5
2.3.1.3 managiQ.....	5
3 Quickstart Guide	7
3.1 Preliminary Steps.....	7
3.2 Installation	7
3.3 Follow-up Steps.....	7
4 Preliminary Steps	9
4.1 Installation Requirements	9
4.1.1 For All Operating Systems.....	9
4.1.2 For Windows NT/2000	10
4.1.3 For Unix Platforms	10
4.1.4 For AS/400.....	10
4.2 Measures	10
4.2.1 Version Control	10
4.2.2 Rights and Data Backups	11
5 Installation	13
5.1 General.....	13
5.1.1 Using External Programs.....	13
5.1.1.1 Virus Scanners.....	13
5.1.1.2 Decompression Tools	14
5.1.2 Starting the Installation	14
5.1.3 Language Independence	14
5.2 Installation Under Windows	15
5.2.1 Start the Installation Routine.....	15
5.2.2 Set Path	15

- 5.2.3 Enter iQ.Suite Administrator Group..... 15
- 5.2.4 Enter the Program Group..... 15
- 5.2.5 Installation Sequence..... 16
- 5.3 "Silent Installation" under Windows..... 16
 - 5.3.1 General..... 16
 - 5.3.2 Running the Installation..... 16
- 5.4 Installation Under IBM AIX, Linux and SUN Solaris..... 18
 - 5.4.1 Sample Installation..... 23
- 5.5 Installation Under OS/400 (Version 5.2 Only)..... 26
 - 5.5.1 Requirements..... 26
 - 5.5.2 Products..... 26
 - 5.5.3 Running the Installation..... 27
- 5.6 Installation in Replicated Environments..... 29
 - 5.6.1 General..... 29
 - 5.6.2 Running the Installation..... 30
 - 5.6.2.1 Standard Installation..... 30
 - 5.6.2.2 Installation on Partitioned Servers..... 30
- 5.7 Deinstallation..... 31
 - 5.7.1 Windows NT/2000..... 31
 - 5.7.1.1 Standard Deinstallation..... 31
 - 5.7.1.2 Deinstallation on Partitioned Servers..... 31
 - 5.7.2 Unix..... 31
 - 5.7.3 AS/400..... 31
- 6 Follow-Up Steps..... 33**
 - 6.1 Symantec AVF for Domino (Parallel Use) Configuration..... 33
- 7 iQ.Clustering..... 35**
 - 7.1 General..... 35
 - 7.1.1 High-Availability and Fail-Safety..... 35
 - 7.1.1.1 High-Availability Example..... 35
 - 7.1.1.2 Fail-Safety Example..... 36
 - 7.1.2 Load Balancing..... 36
 - 7.1.2.1 Load Balancing Example..... 36
 - 7.1.3 Distributed Computing..... 36
 - 7.1.3.1 Distributed Computing Example..... 36
 - 7.1.4 Mailbox Checking..... 37
 - 7.1.5 Grabber Checking..... 38
 - 7.1.6 Miscellaneous..... 39
 - 7.2 iQ.Suite Installation for Using iQ.Clustering..... 39
 - 7.2.1 Installation Requirements..... 39
 - 7.2.2 Running the Installation - Application Examples..... 40
 - 7.2.2.1 Case 1, example:
OS/390 = monitored server, NT = monitoring server..... 40

7.2.2.2 Case 2, example: Server1 (NT) + Server2 (NT) - mutual monitoring.....	40
7.3 iQ.Clustering Configuration.....	42
8 Appendix	45
8.1 Access Rights Configuration Databases	45
8.1.1 Basics	45
8.1.2 Using Predefined Groups.....	45
8.1.3 Using Your Own Groups.....	45
8.1.3.1 ... for the Server	46
8.1.3.2 ... for the Administrator/Manager.....	46
8.1.3.3 ... for the End User	46
8.1.3.4 ... for Administrator Notifications	46
8.2 Mail.Box Design.....	46
8.3 Notes Log Database Design.....	47
8.4 Entries in notes.ini	49
8.5 Support for Multiple Mail.Boxes.....	49
8.6 List of Files.....	50
8.6.1 grptools Directory.....	51
8.6.2 Lotus Notes Program Directory.....	51
8.7 organiziQ.Clerk and Data Protection	52
9 Notes	55

1 Preface

1.1 Quality Assurance

We thank you for choosing iQ.Suite. Before being released, all of our products pass through rigorous tests. No product is issued without having been subjected to an extensive test performed by our QA Team.

1.2 Hotline

If problems arise, you can contact us at any time.

We are available from 8:30 to 18:00.

- Europe, Asia, others:
 - Tel.: +49 721 49 01 112
 - Fax: +49 721 49 01 1912
 - e-mail D: hotline@group-technologies.com
- USA & Canada:
 - Toll free: 877 476 8755
 - Local: +1 508 473 3332
 - Fax: +1 508 473 9940
 - e-mail: hotline@group-software.com

Please find our current FAQs on our website under:

www.group-technologies.com

1.3 What to Do in the Event of a Fault

In the event of a fault, we require the following information in order to provide you with optimum support:

- Product version
- Your license number
- Domino server version
- Operating system and version
- Log Book entries generated at log level 8 (for run errors)
- Any RIP files
- Configuration files

We recommend e-mailing this information to us now. Otherwise keep this information at hand.

1.4 Copyright

GROUP Technologies AG, hereafter referred to as GROUP, is the owner of the full commercial copyright of this documentation protected by law. All rights not explicitly granted remain the property of GROUP.

Copyright 1992-2002 GROUP Technologies AG.

All rights reserved.

1.5 Warranty

GROUP is unable to guarantee, either explicitly or tacitly, the quality, execution, standardization or suitability for a specific purpose.

The product descriptions are general and descriptive in nature. They can be interpreted neither as a promise of specific properties nor as a declaration of guarantee or warranty. The specifications and design of our products can be changed at any times without prior notice, especially to keep pace with technical developments. For information updates, please contact our Sales Department.

1.6 License Agreement

Please read our license agreement supplied with the product CD.

1.7 Third-Party Copyright Notes

IBM, AIX, OS/390, OS/400 and OS/2 are trademarks of the International Business Corporation.

Lotus, Lotus Notes and Lotus Domino are registered trademarks of the Lotus Development Corporation.

Microsoft, MS, MS-DOS, Windows, Windows NT and Windows 2000 are registered trademarks of the Microsoft Corporation.

Solaris is the registered trademark of Sun Microsystems, Inc.

2 Introduction

2.1 The Aim of this Guide

As you will naturally want to make optimum and skilful use of your new application software, we wish to give you the help you need. We have therefore tried to make this guide as easy to use and as understandable as possible. We would be grateful for any suggestions you have on how we can make further improvements. Please send an e-mail to:

manual@group-technologies.com

2.2 Structure of this Guide

This guide uses the following conventions:

Bold Menu names and entries, window names, entry and list boxes, messages, file names and important information are shown in **bold** type.

Italics Entries that the Administrator must make are written in *italics*.

Fixed width Program code and paths are written in fixed width font.

Links Underlined text is a [hyperlink](#). It is usually blue.

The following symbols are used:



The info symbol is used to indicate special points that must be observed for trouble-free use of your system.



The eye means "Attention!" Be careful! It indicates important passages in the text that must be observed in order to avoid any loss of data, damage to your system or any other unpleasant occurrences. Read these passages with particular care and attention.



A little gift to help you! Here, we give you support on particular problems, we provide tips and tricks or alternative solutions and special points.

2.3 Product Overview

2.3.1 iQ.Suite

e-mail and messaging are integral components of many business processes today.

The highest degree of security and availability of the communications infrastructure is thus important to the very existence of a company. Any misuse or irregularity in e-mail communication causes considerable direct and indirect costs. In addition, e-mail and messaging servers are exposed to a wide variety of hazards.

The GROUP iQ.Suite offers a complete security and organizational package that protects users from all e-mail-related risks. The iQ.Suite consists of the product lines securiQ, organiziQ, and managiQ. It can be used with the leading platforms, Lotus Notes/Domino and Microsoft Exchange.

2.3.1.1 securiQ

The Complete Security Package reliably protects your e-mail environment against:

- dangerous viruses of all kinds
- unwanted spam e-mail
- pornographic and racist content
- industrial espionage via e-mail
- data loss and liability risks

2.3.1.2 **organiziQ**

This comprehensive Organization Package saves you valuable time and increases productivity every day:

- Time-optimized sending of e-mail
- Advanced forwarding and delegation control
- Ability to prioritize delivery of e-mails
- Ability to delegate administration

2.3.1.3 **managiQ**

This intelligent Management Package lets you efficiently monitor and manage your e-mail traffic:

- Real-time cost calculation
- Flexible budget management
- Policy and certificate management

3 Quickstart Guide



This chapter contains the most important installation instructions.

Please read this chapter without fail!

This quickstart guide is designed for all those administrators, who studiously avoid reading manuals. Please at least read this chapter, which we have kept as short and concise as possible.

3.1 Preliminary Steps

For a detailed description of the necessary preliminaries, please refer to Section [“Preliminary Steps” on page 9](#).

1. Shut down the server.
2. Make a backup copy of the Domino server.

3.2 Installation

For a detailed description of the installation procedure and licensing information, please refer to Section [“Installation” on page 13](#).

1. Select the setup routine according to your operating system.
2. Select the modules to be installed.
3. Run the entire installation.

3.3 Follow-up Steps

For a detailed description of the necessary follow-up steps, please refer to Section [“Follow-Up Steps” on page 33](#).

1. Start the Domino server.
2. Install and enable the external programs.
3. Configure and enable the jobs. For a detailed description of job configuration options, please refer to your Administration Guide.

4 Preliminary Steps



These steps have to be performed before running the installation!

4.1 Installation Requirements

4.1.1 For All Operating Systems

Make sure the following requirements are met:

- Domino server version 5.07 or higher
- One of the following operating systems:
 - Windows NT 4.0 Intel SP3
 - Windows 2000
 - OS/2 Warp4
 - AIX 4.2.3 or higher
 - SUN Solaris 8
 - Red Hat Linux 6.0 Intel x86 or higher
 - SuSE Linux 7.1 or higher
 - OS/400 V4R4 or higher
- CD-ROM drive or access to network
- RAM: Notes/Domino plus additional 64 MB minimum, 128 MB recommended (RAM depends on the number of modules used and supported applications installed)
- Hard Disk: 250 MB minimum, 500 MB recommended

The disk space actually required cannot be determined accurately as it depends on the following factors:

- a) Log level for Grabber and jobs → size of **log.nsf**
- b) Frequency and size of alarm mails → size of **g_arch.nsf**
- c) Archival frequency when using securiQ.Safe and size of archived mails → size of archival databases
- d) Single logging when using managiQ.Budget → size of **g_prot.nsf** (in which case the size can easily reach 2 - 3 GB)

The Domino server should already have been installed. Check the **notes.ini** file to determine the path of your installation.

4.1.2 For Windows NT/2000

To install the modules you need to have write access to the Windows **Registry** on the Windows NT/2000 server. Administrators usually have these rights.

4.1.3 For Unix Platforms

Root rights are required to run the installation.

4.1.4 For AS/400

To unpack the data files, you need a Windows computer as well as an opportunity to upload data to the AS/400 (FTP, Operations Navigator, Terminal, etc.). For detailed information on data file uploads to the AS/400 please refer to the installation description for AS/400 in Section [“Installation Under OS/400 \(Version 5.2 Only\)” on page 26](#).

4.2 Measures

4.2.1 Version Control

Use the following table to check whether you are about to install the correct iQ.Suite version for your Domino server:

OS system	Domino Server Version		
	6	R 5.0.7 +	R 5.0 - R 5.0.6
Windows 2000 (Intel)	R 6.2 iQ.Suite 7 for Domino 6	R 5.2 iQ.Suite 7 for Domino R5	R 5.1
Red Hat as of 6.0 / SuSE Linux as of 7.1	iQ.Suite 7 for Domino 6	R 5.2 iQ.Suite 7 for Domino R5	R 5.1
SUN Solaris 8	iQ.Suite 7 for Domino 6	R 5.2 iQ.Suite 7 for Domino R5	R 5.1

OS system	Domino Server Version		
	6	R 5.0.7 +	R 5.0 - R 5.0.6
IBM AIX as of 4.2.3	iQ.Suite 7 for Domino 6	R 5.2 iQ.Suite 7 for Domino R5	R 5.1
OS/400 V4R4	* iQ.Clustering version	R 5.2	--
OS/2 4.0	--	R 5.2	R 5.1
OS/390	* iQ.Clustering version	* iQ.Clustering version	* iQ.Clustering version

All indications refer to the server platform, regardless of the versions and operating systems used on the workstations.

4.2.2 Rights and Data Backups

1. Be sure to read the **Release Notes** file which may contain important additional information.
2. Log on to your system as Administrator.
3. Create a **multi-purpose** group in the NAB (Notes Name and Address Book) with Manager access rights to the iQ.Suite databases. Members of this group will receive all automatic notifications issued by iQ.Suite. For further information please refer to your Notes/Domino documentation.
4. Shut down the Domino server.
5. Before starting the installation, make a backup copy of the **log.ntf**, **mailbox.ntf** and **statrep.nsf** files. Your own templates will be preserved during the installation. iQ.Suite will add the necessary extensions to any existing templates.



5 Installation

5.1 General

5.1.1 Using External Programs

iQ.Suite uses a number of external programs - these have to be installed and licensed separately. Standard configurations are provided for the most currently used external programs. These configurations can easily be adapted to your specific needs.



If you wish to use external programs not supported by iQ.Suite, please contact your supplier's Support Service.

5.1.1.1 Virus Scanners

Watchdog uses external virus-scanners to check for viruses. These programs are **not delivered with the iQ.Suite** and must therefore be purchased separately.

The Watchdog Windows version includes a demo version of the SOPHOS Anti-Virus software. This software is **not licensed** and must be purchased separately if it is to be used on a permanent basis.

Within Germany, this software can be obtained from

Sophos GmbH, Am Hahnebusch 21, 55268 Nieder-Olm.

Outside of Germany, it can be obtained from

SOPHOS Plc, 21 The Quadrant, Abingdon OX12 3YS, England.

For further information visit <http://www.sophos.com>.



In order to correctly initialize the pre-configured iQ.Suite virus scan job, a virus scanner has to be installed and configured, and the virus scanner document has to be enabled under **Utilities** → **Virus Scanner**. Otherwise, you will receive an error message. For configuration details please refer to your Administration Manual.



Please note that we supply three test viruses with the software!

For test purposes, the Watchdog delivery includes test viruses.

- grptools\test\g_tstvir.com Jerusalem test pattern
- grptools\test\g_tstvir.exe Jerusalem test pattern
- grptools\test\leicartst.exe Eicar test pattern

These are modified viruses. **These virus files are not executable and have no functionality whatsoever. The test viruses supplied can neither replicate, spread, nor cause any damage.** Parts of the binary pattern have simply been retained to simulate a virus.

5.1.1.2 Decompression Tools

To unpack archives, the iQ.Suite also uses external programs. These are **not delivered with the iQ.Suite** and must therefore be purchased separately and enabled in the configuration databases.

5.1.2 Starting the Installation



Close all programs that are not required, in particular Domino and Notes! Otherwise, some of the files may not be installed correctly if they are being used by another program.



If you do not want to install the databases supplied with the installation package but your own ones (with the same name), please copy these databases to the installation directory.

5.1.3 Language Independence

As of Version 7, the iQ.Suite installation package includes all available languages. The desired language is selected at the beginning of the installation.



The language setting can be changed at a later stage by assigning the appropriate value (*en*, *de*) to the `ToolKit_ServerLanguage` configuration parameter set during installation in the **notes.ini** file.

5.2 Installation Under Windows

5.2.1 Start the Installation Routine

Run the following file in the installation package:

■ **ntsetup.exe** (Win NT/Win 2000)

iQ.Suite is always installed as a whole, i.e. including all modules. In the window displayed next, agree with the license terms.



The installation has to be started from a local directory or from a connected network directory.

Starting the installation via a UNC path (\\computer\directory\dir) is no longer supported!

5.2.2 Set Path

You are then prompted for the path of the executable files of the Domino server or the path of the **notes.ini** file.



If the **notes.ini** file is located in the search path, the installation routine will use the corresponding directory as default value.

5.2.3 Enter iQ.Suite Administrator Group

In the **Toolkit_Admin** dialog box (also refer to [“Entries in notes.ini” on page 49](#)), enter the name of the group as specified under [“Rights and Data Backups” on page 11](#) (also refer to [“Access Rights Configuration Databases” on page 45](#)). The name of the administrator group will be entered in the **notes.ini** file. Additionally, this name is also stored as Administrator in the Access Control List (ACL) of the iQ.Suite configuration databases.

5.2.4 Enter the Program Group

In the last dialog box, you are prompted for the iQ.Suite program group. Choose a name and click **Next**. You may then choose between standard installation and replicated environment installation (please refer to [“Installation in Replicated Environments” on page 29](#)). Then click **Next** to run the installation and complete the setup procedure.

5.2.5 Installation Sequence

The installation routine first creates a subdirectory named `grptools` under the data directory of your server. It then copies all files and Notes databases to the appropriate directories, modifies various standard databases, and modifies a number of entries in the `notes.ini` file. For details refer to:

- [“Entries in notes.ini” on page 49](#)
- [“List of Files” on page 50](#)
- [“Mail.Box Design” on page 46](#)
- [“Notes Log Database Design” on page 47](#)

5.3 “Silent Installation” under Windows

5.3.1 General

Silent Installation is an installation routine without user interaction for identical installation on different computers. Typically, it is used if you wish to install iQ.Suite on several servers and to distribute a customized configuration (different from the installation package) without replicating the databases.

This not only reduces the installation time, it also ensures that no errors occur due to wrong dialog entries.

5.3.2 Running the Installation

1. Open a DOS window.
2. Change to the iQ.Suite installation directory.
3. Start the appropriate command procedure:

silent_inst_rec.cmd d (German) or

silent_inst_rec.cmd e (English)

All subsequent dialog entries are now recorded and stored in the **setup.iss** file. After installation is complete, the **setup.iss** file is automatically copied to the installation directory.

4. Now check this new **setup.iss** file. If another path (for the Notes program directory and the `notes.ini` file) is needed for the subsequent installations (run without dialog entries), the **setup.iss** file has to be adapted accordingly.

5. Example:

```
[SdAskDestPath-0]
szDir=c:\lotus\domino (Notes programm directory)
Result=1
[SdAskDestPath-1]
szDir=c:\lotus\domino (position of notes.ini file)
```

6. Copy the entire installation directory to the computer where iQ.Suite is to be installed next.
7. On that computer, open a DOS window.
8. Change to the installation directory.
9. Start the appropriate command procedure:
 - silent_inst_run.cmd d* (German) or
 - silent_inst_run.cmd e* (English)

The Silent Installation will now be started, with iQ.Suite installed according to the settings in the **setup.iss** file.

10. The **setup.log** file created by the installation provides information on whether the installation was successful or not, e.g.:

```
...
[ResponseResult]
ResultCode=0
→ Installation successful

...
[ResponseResult]
ResultCode=-12
→ Installation failed
```

11. More detailed information on the installation is provided in the **tk_inst.log** file created in the `grptools` directory.
12. Repeat this procedure (as of step 5) for every computer iQ.Suite is to be installed on.

5.4 Installation Under IBM AIX, Linux and SUN Solaris

This section provides instructions to install the iQ.Suite under Domino 5 on IBM AIX, Linux and SUN Solaris platforms.

The installation consists of the following steps:

1. Copy files to server

Login as *root*

Copy the tar file (e.g. **d52.tar**) to /tmp

call *tar -xvf d52.tar*

All of the files required for installation are now located in

/tmp/install

2. Close all Domino servers on all partitions!

Please make sure that no Domino servers are running!

3. Backup the files which will be changed by installation

Back up some files from the Notes data directory

cp mailbox.ntf log.ntf statrep5.ntf notes.ini /tmp

4. Verify access rights

The installing user (root) must have sufficient access rights to copy files to the following directories:

- a) Notes program directory

(e.g.: /opt/lotus/notes/latest/sunspa)

- b) Notes data directory

(e.g.: /home/export/domino)

5. Set environment variables

The following entries must be added to the **.profile** of the Notes user:

export PATH=\$PATH:<grptools-dir>/bin

where <grptools-dir> is the path to the

<notesdata>/grptools/bin directory.

This entry is needed to run securiQ.Wall and other modules and to start external programs.

Depending on the Unix platform, the following environment variables should also be set:

 Solaris:

In the **.profile**

```
export LD_LIBRARY_PATH=/opt/lotus/notes/latest/sunspa
```

 AIX:

In the **.profile**

```
export LIBPATH=/opt/lotus/notes/latest/ibmpow
```

 Linux:

In the **/etc/ld.so.conf** file, add the following line:

```
/opt/lotus/notes/latest/linux
```

6. Initial check of notes.ini

The following entry must be present:

```
ServerKeyFileName=server.id
```

Note: If the `ServerKeyFileName` entry is missing in the **notes.ini** file, add the above line to the **notes.ini** file (where "**server.id**" stands for the appropriate server ID file).

7. Start installation

Make sure that no Notes programs and no shared objects are loaded in memory. To do so, use the `slibclean` command. This command requires root access rights.

Start the **install.sh** shell script with both of the arguments:

- a) Notes program directory
- b) Notes data directory

Example:

```
./install.sh /opt/lotus/notes/latest/ibmpow /home/domino
```

This script provides the actual installation program with the required options.



AIX / SUN: If using a shell other than ksh, please start the installation as follows:

```
/usr/bin/ksh ./install.sh <Notes program directory> <Notes data directory>
```

Linux: If using a shell other than bash, please start the installation as follows:

```
/usr/bin/bash ./install.sh <Notes program directory> <Notes data directory>
```

Beispiel:

```
/usr/bin/ksh ./install.sh /opt/lotus/notes/latest/ibmpow /home/domino
```

Follow the installation instructions on screen.

The files are then copied to your destination directory and the **notes.ini** file is modified.

8. Check notes.ini

The following entries must be present in the **notes.ini** after installation:

- Toolkit_DataDir=grptools
GROUP path, relative to Notes data directory
- Toolkit_ExecDir=<NotesDataPath>/grptools
Absolute path to the GROUP directory
- Toolkit_Admin=GROUP-TOOLS-ADMIN
GROUP administrator. A valid mail address from the name/address book must be specified here. Only **one** entry is possible! This may be a group or an individual.
- Toolkit_Loglevel=6
Global log level for entries in the **log.nsf** Notes log (1 - 9, 1 = little details, 9 = every detail logged).

The log level can be set separately for each job in the Mail database and the DatabaseGrabber database.

Default value: "Loglevel 0 (value from NOTES.INI)".

- `Toolkit_MailIntercept=YES`

If mails are to be processed, set this parameter to *Yes*. For pure database servers, it should be set to *No*.
- `Toolkit_MgrabThreads=5`

Sets number of working threads (2-20) started by MailGrabber, meaning how many mails can be processed simultaneously.
- `Toolkit_DgrabThreads=5`

Sets number of working threads (2-20) started by DatabaseGrabber, meaning how many DatabaseGrabber jobs (not databases) can be processed simultaneously.
- If the iQ.Suite is used on a partitioned server, the entry

`Toolkit_ServerInstance=001`

has to be added **manually**, with servers numbered consecutively. This in particular also applies to Domino servers run in operating system clusters, in which case the numbering must be unambiguous throughout the entire cluster.

Example:

Server1 (**notes.ini**): `ToolKit_ServerInstance=001`

Server2 (**notes.ini**): `ToolKit_ServerInstance=002`
- Make sure the server ID file (`ServerKeyFileName` entry in the **notes.ini** file, e.g.: **server.id**) is present in the Notes data directory.
- `ServerTasks=..., tm_grab, td_grab`

This entry ensures the Grabbers are started automatically.

`tm_grab` = MailGrabber (for products processing e-mails).

`td_grab` = DatabaseGrabber (for products processing databases)
- `extmgr_addins=te_hook`

This entry integrates the hook which identifies new incoming mails and additionally monitors the control databases (MailGrabber DB (**gm_grab.nsf**), DatabaseGrabber DB (**gd_grab.nsf**)).

9. Verify access rights at file level

Owner & group of the copied files must match those of the Notes user. The Notes user must have the following file access rights:

□ <GROUP directory> (rwx):

*.nsf rw

*.dll rwx

res*.txt rw

tk_sun_call rwx (1)

tk_aix_call rwx (1)

tk_390_call rwx (1)

tk_linux_call rwx (1)

toolkit.lic rw

□ <GROUP directory>/infozip (rwx):

unzip rwx

□ Notes program directory (rx):

tm_grab rwx

td_grab rwx

libte_hook.so rwx (1)

libte_hook.a rwx (1)



Owner rights are set automatically during installation.

1. according to operating system

10. Verify database access rights

The server must have Manager rights and document deletion rights. The user type entry has to be *unspecified*.

The GROUP-TOOLS-ADMIN group (also refer to [“Access Rights Configuration Databases” on page 45](#)) must be present in the Domino directory of the server. This must be a **Mail** or **Multi-Purpose** group.

11. Additional points

Operating system patches: No additional patches are currently required.

iQ.Suite is now completely installed! Start your Domino server and the Notes administration client. In order to administer iQ.Suite, you must create the GROUP-TOOLS-ADMIN group and specify its members.

The next step is to set up the iQ.Suite jobs.

5.4.1 Sample Installation

Assumption: You have a partitioned server with four Domino servers and want to install iQ.Suite on three of these four servers.

The Notes program directory is

- /opt/lotus/notes/latest/ibmpow (for AIX),
- /opt/lotus/notes/latest/sunspa (for Sun/Solaris),
- /opt/lotus/notes/latest/linux (for Linux).

The Notes data directories are

- /home/domino1,
- /home/domino2,
- /home/domino3,
- /home/domino4.

The corresponding Unix user names are domino1, domino2, domino3, and domino4. You want to install the program on the first, second, and fourth server (/home/domino1, /home/domino2, /home/domino4).

To do so, proceed as follows:

Install iQ.Suite on the first server.

1. Change to the domino1 user:

```
su - domino1
```

2. Set the `ToolKit_Dir` environment variable.

To do so, add the lines:

```
set ToolKit_Dir=/home/domino1/grptools
```

```
export ToolKit_Dir
```

to the **.profile** file of the first Domino user (i.e. domino1).

3. Change to the root user:

```
su
```

4. Use `slibclean` to ensure the Notes library is not loaded:

```
slibclean
```

5. Set the `ToolKit_Dir` environment variable to a temporary directory (used during installation):

```
set ToolKit_Dir=/tmp
```

```
export ToolKit_Dir
```

6. Start the installation script:

```
./install.sh /opt/lotus/notes/latest/ibmpow /home/domino1.
```



If you want to specify another group in the Domino directory as iQ.Suite administrator (default: GROUP-TOOLS-ADMIN), please change the following line in the installation script:

```
GrpAdm='GROUP-TOOLS-ADMIN'
```

The group must exist in the Domino directory. If it doesn't, please create it after completing the installation. This group must be created in the Domino directory as **multi-purpose** group. Please replace all references to GROUP-TOOLS-ADMIN in this file with the name of the new group.



If you want use a directory other than `grptools` (not recommended!), change the following line in the installation script:

```
GrpFolder='grptools'
```

Please replace all references to the `grptools` directory with the new directory name. Also keep in mind that the **.profile** file of the current Notes user has to be adapted.

Example:

`GrpFolder = goodwork`. Change the following lines (in the **.profile** file):

```
set ToolKit_Dir=/home/dominio1/grptools
export ToolKit_Dir
```

to:

```
set ToolKit_Dir=/home/dominio1/goodwork
export ToolKit_Dir
```

Then, and then only, start the installation script.

7. Change the owner of the `grptools` directory to the first Domino user.

```
chown -R domino1:notes /home/dominio1/grptools
```

8. Add the following line to the **notes.ini** file of the first Domino server:

```
Toolkit_ServerInstance=001
```

(For the second and the fourth server, please replace 001 with 002 and 004 respectively).

Please note that the The **notes.ini** file of the third server does not have to be changed.

9. Check the installation settings on the system.

To do so, refer to the instructions under [“Check notes.ini” on page 20](#), [“Verify access rights at file level” on page 22](#) and [“Verify database access rights” on page 23](#).

10. Repeat all steps above to install iQ.Suite on the second and the fourth server. To do so, first replace `domino1` with `domino2`, then with `domino4`.

11. Start the Domino servers. The installation is now complete. For the correct iQ.Suite configuration, please refer to the Administration Manual.

5.5 Installation Under OS/400 (Version 5.2 Only)

The package includes the following files:

grptools.sav	An AS/400 backup file containing the iQ.Suite data (and executable files)
libascii.htm	An HTML file containing the license terms and the installation instructions for the IBM LIBASCII package. Please read the IBM license terms!
libasc10.sav	An AS/400 backup file containing the LIBASCII package. (In the Installation Guide from IBM, this file is named libasc10.exe .)

5.5.1 Requirements

IBM uses EBCDIC code while iQ.Suite uses ASCII code. Therefore, iQ.Suite for AS/400 requires the

LIBASCII package from IBM for EBCDIC -> ASCII conversion.

However, this package is no longer available and has been replaced with the product named 5799-AAS.

Further information is available under:

<http://www.as400.ibm.com/domino/libascii.htm>

5.5.2 Products

This package contains the following products in an AS/400 version:

- securiQ.Watchdog
- securiQ.Wall
- securiQ.Safe
- securiQ.Trailer
- organiziQ.Clerk
- organiziQ.Smart
- iQ.Action

- iQ.Split
- iQ.Spy
- iQ.Clustering

iQ.Clustering allows to use the entire iQ.Suite for Windows NT/2000 functionality (e.g. securiQ.Crypt). All this requires is a Windows NT workstation with Domino Server installed and iQ.Suite for Windows NT/2000 which uses iQ.Clustering to check the Mail.box on your AS/400. For more detailed information, please refer to [“iQ.Clustering” on page 35](#).

5.5.3 Running the Installation

To install the iQ.Suite software, please observe the following points. This procedure assumes that you have stored the **grouptools.sav** file on your PC workstation under `c:\grouptools.sav`. You will find that file on the product CD or on our download page.

1. Log on to your AS/400 with a user profile which will enable you to use a command line and create a user profile.
2. Create a backup file in a library to which you have access with the `crtsavf` command. You may for instance enter

```
crtsavf file(qgpl/grouptools)
```

in order to create the backup file named **grouptools** in the library named **QGPL**. Please note that there should be no existing backup file with the same name. (In this case, use the `dltf` command to delete the existing backup file or select another name for your backup file.)
3. On the AS/400 command line, enter the command

```
CRTUSRPRF USRPRF(GROUPTOOLS) PASSWORD()
```

in order to create a simple user profile without login capability to your system.
4. Use FTP to create a binary copy of the backup file on your AS/400. In this example, enter the following command in an open MS-DOS Command Prompt:

```
ftp [your AS/400 System name or IP address]
```
5. When prompted to do so, enter your AS/400 user name and your AS/400 password.

6. Once logged in, enter the following commands

binary

put c:\grptools.sav qqpl/grouptools,

in order to enable binary data transfer and to copy the backup file.

7. Enter

bye

to exit the FTP program.



In case data transfer is not possible via FTP, you can use the Operations Navigator to transfer the file to the root file system of the AS/400.

On the AS/400 console, enter the following commands to transfer the data to the backup file created before:

```
CPYFRMSTMF FROMSTMF('/grptools.sav') TOMBR
```

```
('/qsys.lib/qqpl.lib/grouptools.file') MBROPT(*ADD)
```

You may then delete the copy in the root file system.

You can proceed in the same way to transfer the **libasc10.sav** file.



The Operations Navigator may not be available on all systems. A data transfer via FTP, as described above, is the standard method and should be used where possible!

The iQ.Suite backup file is now on your AS/400. In the next step, the data saved in the backup file has to be restored.

8. To do so, enter the following command on the AS/400 command line:

```
rstlib savlib(grouptools) dev(*savf) savf(qqpl/grouptools)
```

The executable files of the iQ.Suite have thus been installed and you now have to install the data files and databases.

9. Before proceeding, however, shut down the Domino server.
10. Then enter the following command on the AS/400 command line to start the installation program:

```
call grouptools/setup
```

You will be prompted for the absolute Integrated File System path of the

data directory of your Domino server for which iQ.Suite is to be installed. This is the directory containing the **notes.ini** file. The data files and databases are then automatically restored and copied to the appropriate directories. The installation program creates symbolic references to the executable files and completes the **notes.ini** file as required.

iQ.Suite is now completely installed! Start your Domino server and the Notes administration client. In order to administer iQ.Suite, you must create the *GROUP-TOOLS-ADMIN* group and specify its members.

The next step is to set up the iQ.Suite jobs. For a detailed description of the job configuration please refer to your Administration Manual.

5.6 Installation in Replicated Environments

5.6.1 General

As of Version 7, the installation routine supports replicated environments under Windows and Unix, i.e. the replication of configuration database.

The installation routine asks whether the installation is to be run in a replicated multi-server environment. If that is the case, the installation routine prompts for the "iQ.Suite Master Server". Enter the server (the default setting is the `ToolKit_MasterServer` entry from the **notes.ini** file). The server specified here is then written to the **notes.ini** file.

The installation routine also prompts for the data directory of the databases to be replicated (`ToolKit_MasterServer_DataDir` in **notes.ini** file).

Rather than installing the databases from the installation directory, the system now creates replicates of the configuration databases from the specified "Master Server".



Any errors occurring during the replication of a database are logged in the installation log file. This log file can be viewed at the end of the installation or opened in the `...\grptools` directory (**tk_inst.log**).



The server must be an existing and known one. In case the database on the "Master Server" cannot be opened (because the server or the database does not exist), the installation is aborted.

The target server (on which the software is to be installed) must have sufficient rights to read the "Master Server" databases. Otherwise, the databases from the installation package will be installed.

5.6.2 Running the Installation

5.6.2.1 Standard Installation

1. Start the installation program for your operating system.
2. In the **Configuration Databases** window, click on the **Install replicated environment** button.
3. In the next window, enter the name of the "master Server" and the data directory of the databases to be replicated.

The installation routine now creates the iQ.Suite databases to be installed as replicates of the server previously specified.

5.6.2.2 Installation on Partitioned Servers

1. On the server from where the databases are to be replicated:
Install iQ.Suite as for non-partitioned servers, see "[Standard Installation](#)".
2. On the server the replicated databases are to be installed on:
 - a) Start the 1st server.
 - b) As for non-partitioned servers, enter the 1st server and the path to the databases. Check for sufficient rights.
 - c) The system will now display a number of messages like the following:
"A read only file, <filename>, was found while attempting to copy files to the destination location."
They are caused by the Grabber opened by the first server when started and by the te_hook in the program path. Confirm each message with **No** = "Do not overwrite". If you answer **Yes**, the installation will be aborted shortly after. It can however be repeated without any problem.
 - d) Complete the installation as under "[Standard Installation](#)".

5.7 Deinstallation

5.7.1 Windows NT/2000

5.7.1.1 Standard Deinstallation

To deinstall the software, go to:

Start → **Control Panel** → **Software** → **Install/Remove**

5.7.1.2 Deinstallation on Partitioned Servers

A deinstallation routine is available for the last server installed only - all other servers have to be uninstalled manually.

5.7.2 Unix

Start the **uninstall.sh** shell script in the command line with the arguments:

1. Notes program directory
2. Notes data directory

Example:

```
./uninstall.sh /opt/lotus/notes/latest/ibmpow /home/domino
```

5.7.3 AS/400

1. Stop the server.
2. Delete the `grptools` directory (using either the Operation Navigator or the `qsh` or the `wrklnk` command).
3. Remove the iQ.Suite links from the Notes data directory: **tm_grab.pgm**, **td_grab.pgm** and **libte_hook.srvpgm**
4. Remove all iQ.Suite-specific entries from the **notes.ini** file:
 - a) Under **ServerTasks**: the entries **tm_grab** and **td_grab**
 - b) Under **EXTMGR_ADDINS**: the entry **libte_hook.srvpgm**. If there are no more entries left, delete the entire line, including the key word.
 - c) All lines with key words beginning with **ToolKit**.
5. Delete the files **grouptools.lib** and **grouptools.sav** (the backup file, by default named **grouptools.sav**, used to restore the **grouptools.lib** file.)

6

Follow-Up Steps

1. Start the server.
2. Install and configure the external programs you want to use, e.g. virus scanners, decompression tools and analysis tools. Check their versions to make sure that the anti-virus tools are compatible with securiQ.
3. Enter your license. To do so, copy the **Toolkit.lic** file to the `grptools` directory.
4. Enter the following database as bookmark on the Desktop: *Entry for iQ.Suite (grptools/nav.nsf)*. This databases controls the mail and database configuration and is located in the `grptools` subdirectory of your data directory of the Domino server.
5. The installation routine modifies the statistics database (**statrep.nsf**). Enable the Statistics Reporter Task after having installed iQ.Suite. Otherwise, you will not receive any statistics logs.
6. Gradually configure and enable the individual jobs. To do so, you have to activate all programs manually. To take full advantage of Watchdog, you must have installed and enabled an anti-virus program. For detailed information on the configuration of jobs, please refer to your Administration Manual.
7. If you don't have assigned database access rights yet: Read "[Access Rights Configuration Databases](#)" on page 45 where assigning rights is described in detail.



When upgrading from an older version, the user rights related to the old databases are preserved. Only the database design is updated.

6.1 Symantec AVF for Domino (Parallel Use) Configuration

As of iQ.Suite 7, Symantec AVF for Domino and iQ.Suite can be used simultaneously. For this purpose, a new Hook (**tk_hook**) was developed and designed to process the documents placed in the Mail.box by the Symantec Task (NTASK). At the same time, the Extension Manager Add-in (**te_hook**) was redesigned to ignore the documents placed in the Mail.box by NTASK. As a result, the documents are always first processed by Symantec AVF and then by iQ.Suite.

To ensure correct interaction with iQ.Suite, please observe the following:

1. In the **notes.ini** file, enter the **tk_hook** under `NSF_HOOKS`:
`NSF_HOOKS= tk_hook`. The order is irrelevant.
2. Use a license file that contains the entry `GRPNAV`. This stands for "GROUP Symantec AVF Assistant".

The only possible processing order is Symantec AVF → GROUP, not vice-versa. In other words, attachments are always first checked for viruses and then processed by iQ.Suite.

This in particular means that, for instance, PGP-encrypted mails are first scanned by Symantec AVF and then decrypted by securiQ.Crypt. For virus scanning after decrypting, you will need securiQ.Watchdog and a virus scanner supported by Watchdog.

Glossary:	
SAV:	Symantec Antivirus
NTASK:	Server add-in task of the SAV for Notes
NNHOOK:	Hook of the SAV for Notes
Extension Manager Add-in	"Hook" entered under <code>EXTMGR_ADDIN=.</code> in the notes.ini file → cf. te_hook
Database Hook:	"Hook" entered under <code>NSF_HOOKS=.</code> in the notes.ini file

7 iQ.Clustering

7.1 General

iQ.Clustering is an iQ.Suite feature that is activated on a Domino server when installed.

iQ.Clustering provides:

1. high availability,
2. fail-safety,
3. load balancing, and
4. distributed computing.

A cluster managed by iQ.Clustering comprises several Domino servers (reasonably not more than 4 to 6) with iQ.Suite installed. iQ.Clustering is an application cluster; it does **not** replace but complements the function of a Domino cluster.



To work correctly, iQ.Clustering requires an identical or replicated configuration on all servers concerned. The network connection between clustered servers must provide sufficiently high data transfer rates, e.g. such as provided by LAN connections.

7.1.1 High-Availability and Fail-Safety

iQ.Clustering can be used to optimize the iQ.Suite system availability according to the requirements of major installations or specific 24/7 applications.

The clustered servers monitor each other, in particular the e-mail traffic in each **Mail.box**, as well as the processing actions taken by iQ.Suite. In the event of an iQ.Suite failure on one computer, the other servers in the iQ.Clustering cluster take over the tasks of the failing server.

7.1.1.1 High-Availability Example

If running a backup computer center for your Domino servers, iQ.Clustering can be used to ensure that the cluster computer in the backup computer center immediately takes over whenever the main server becomes unavailable. This would be a typical scenario for using a Domino cluster in combination with iQ.Clustering.

7.1.1.2 Fail-Safety Example

If running multiple Domino servers, iQ.Clustering can be used to ensure that whenever there is an iQ.Suite failure on one server, the other servers in the cluster take over that server's tasks.

7.1.2 Load Balancing

iQ.Clustering allows to react to dynamic system load requirements by distributing tasks between systems according to their current load. The iQ.Suite system on the less loaded server takes over the task of checking and processing the e-mails of the heavily loaded server and later returns them to the original system.

7.1.2.1 Load Balancing Example

At your main site, multiple Domino servers are operated as Internet gateways. If, for instance, the gateway for incoming e-mails is more heavily loaded than the outgoing mail gateway, the iQ.Clustering load balancing function will shift some of the processing tasks from the more loaded server to the less loaded one.

7.1.3 Distributed Computing

This iQ.Clustering function allows to process e-mails on a separate computer regardless of the e-mail host. In combination with high-availability and load balancing, this ensures highest system safety and ease-of-use in enterprise environments.

iQ.Clustering can thus for instance be used to check e-mails on a remote Domino server (e.g. for viruses) via the network whenever this Domino server is run under an operating system for which iQ.Suite or any required third-party products are not available.



This requires a Domino server and iQ.Suite installed on the separate computer.

7.1.3.1 Distributed Computing Example

iQ.Suite is to be installed on an existing mail host (with Domino server) in a non-Windows environment in order to check e-mail attachments for viruses. The virus scanner to be used is not available on the operating system platform. To solve

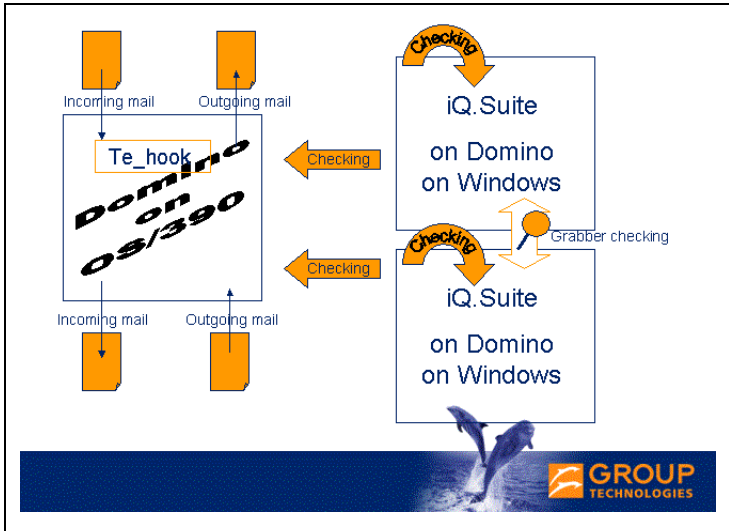
this problem, the virus scanning function can be shifted to a Windows computer. To do so, iQ.Suite and the corresponding function modules (in this case Watchdog) are installed along with the virus scanner on this Windows computer. On the mail host, only the EXTMGR_ADDIN te_hook utility is installed. The e-mail is simply marked for processing by the hook and the MailGrabber installed on the computer running iQ.Suite then processes the e-mail as required.

In addition to virus scanning, iQ.Clustering also allows to run any other module in any environment, as it is always possible to run e-mail checking functions from a platform where the module is available.

7.1.4 Mailbox Checking

- The MailGrabber checks the Mail.box(es) to be monitored for new documents.
- The MailGrabber attempts to reserve any documents found;
→ new status in the **dispatched for <server name>** view.
- The working threads only process documents that have been successfully reserved by the server. This is determined through the `$TKCheckServer` field.
- If a reserved document is not processed within 15 minutes, it is returned to the "general pool".
- If there are any reserved documents when the MailGrabber is shut down or started, the reservation is removed.

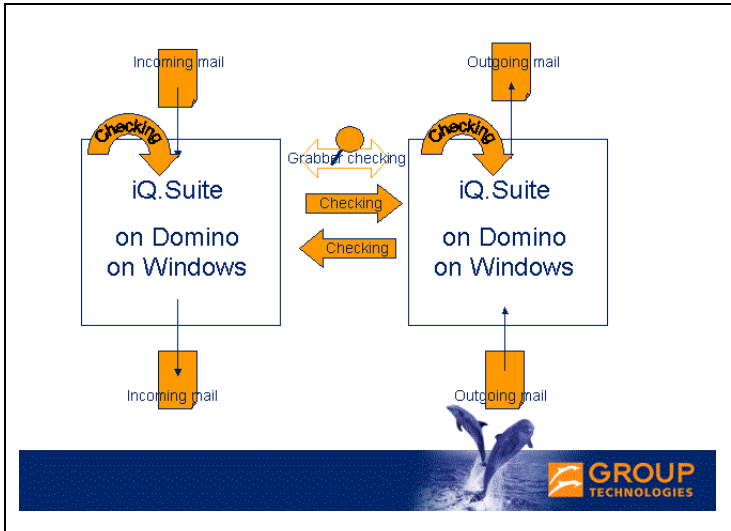
The picture below illustrates the working principle for checking the mailboxes on an OS/390 computer with simultaneous mutual monitoring of the MailGrabbers:



7.1.5 Grabber Checking

- On the servers to be monitored, the MailGrabber checks the Mail.box / Mail1.box for a profile document.
- This profile document contains the last action (with date/time) performed by the Grabber on the monitored server.
- This profile document is written by the Grabber to be monitored (at least once per minute) and it is read and deleted by the monitoring servers (approx. every 5 minutes).
- If no profile document is found, the last status read is considered to be the current status.
- If several Grabbers monitor the same server, there is a risk of false alarms when the write/read cycles interfere with each other.

The picture below illustrates the working principle for mutual monitoring of mailboxes on an Internet gateway by two NT PCs with simultaneous mutual monitoring of the MailGrabbers:



7.1.6 Miscellaneous

- iQ.Clustering requires a separate license.
- It may not be useful to include more than three servers in an iQ Cluster.
- The new "Reserve" and "Process" method is always used, even if checking the own Mail.box only.
- iQ.Clustering requires appropriate access rights to the Mail.box(es)! The servers must have sufficient rights to access each other's mailbox.
- The system time settings on the servers must not differ significantly.

7.2 iQ.Suite Installation for Using iQ.Clustering

7.2.1 Installation Requirements

- Installation requirements for standard installation, refer to ["Installation Requirements" on page 9.](#)
- One of the following operating systems on one computer:
 - Windows NT 4.0 Intel SP3
 - Windows 2000
- Fast network connection
- Virus scanner (for securiQ.Watchdog)
- PGP (for securiQ.Crypt)

7.2.2 Running the Installation - Application Examples

7.2.2.1 Case 1, example:

OS/390 = monitored server, NT = monitoring server

1. Run a normal installation on the monitoring server (NT).
2. On the monitored server (OS/390), copy the appropriate **te_hook.dll** to the Domino program directory.
3. On the monitored server, adjust the notes.ini file as follows:

```
Extmgr_Addins=te_hook and toolkit_MailIntercept=yes
```

4. On the monitoring server, create an **iQ.Clustering** configuration document under **Global Parameters** that contains the following:

```
Server =<monitoring server>
```

```
Server for mailbox checking [= toolkit_WatchServer] =<monitored server>
```

or change the **iQ.Clustering** documents as required for your purposes.

Proceed as follows to install an additional monitoring server:

1. Run a normal iQ.Suite installation on this server.
2. On this monitoring server, create an **iQ.Clustering** configuration document under **Global Parameters** that contains the following:

```
Server =<monitoring server>
```

```
Server for mailbox checking [= toolkit_WatchServer] =<monitored server>
```

The **te_hook** will now stop the e-mails on the monitored server and the MailGrabber on the monitoring server will fetch them in order to process them.



The monitoring servers must replicate the address book of the monitored server!

7.2.2.2 Case 2, example:

Server1 (NT) + Server2 (NT) - mutual monitoring

1. Run a normal installation on both servers (replicated or not).
2. On both servers, create the configuration document under **Global Parameters** (see "[Case 1, example: OS/390 = monitored server, NT = monitoring server](#)") with the following settings:

On server 1:

Server = <Server1>

Server for mailbox checking [= toolkit_WatchServer] = <Server2>

and if the MailGrabber is to be monitored:

Server for Grabber checking [= toolkit_MonitorServer] = <Server2>

On server 2:

Server = <Server2>

Server for mailbox checking [= toolkit_WatchServer] = <Server1>

and if the MailGrabber is to be monitored:

Server for Grabber checking [= toolkit_MonitorServer] = <Server1>

Server 1 will now periodically check the mailbox on server 2 for mails that have not yet been processed by server 2 - and vice versa.

Proceed as follows to install an additional server:

1. Run a normal iQ.Suite installation on this server.
2. On this server 3, create an **iQ.Clustering** configuration document under **Global Parameters** that contains the following:

Server =<Server3>

Server for mailbox checking [= toolkit_WatchServer] = <Server1>

and if the MailGrabber is to be monitored:

Server for Grabber checking [= toolkit_MonitorServer] = <Server1>
3. On server 3, create an **iQ.Clustering** configuration document under **Global Parameters** that contains the following:

Server =<Server3>

Server for mailbox checking [= toolkit_WatchServer] = <Server2>

and if the MailGrabber is to be monitored:

Server for Grabber checking [= toolkit_MonitorServer] = <Server2>
4. On server 2, additionally create an **iQ.Clustering** configuration document under **Global Parameters** that contains the following:

Server =<Server2>

Server for mailbox checking [= toolkit_WatchServer] = <Server3>

and if the MailGrabber is to be monitored:

Server for Grabber checking [= toolkit_MonitorServer] = <Server3>

- On server 1, additionally create an **iQ.Clustering** configuration document under **Global Parameters** that contains the following:

Server =<Server1>

Server for mailbox checking [= toolkit_WatchServer] = <Server3>

and if the MailGrabber is to be monitored:

Server for Grabber checking [= toolkit_MonitorServer] = <Server3>



Again, each server must replicate the address book of the other server!

In case the servers are not mutually monitoring each other, the corresponding configuration documents are not needed!



The jobs on the servers must be the same; the Server field is irrelevant in that context, as it does not relate to which server (mailbox) the mails come from!

7.3 iQ.Clustering Configuration

The configuration of the servers to be checked is carried out via notes.ini parameters or the new global parameters that allow to set up mutual monitoring of mailboxes and Grabbers. If configured as cluster, the servers mutually take over each other's tasks in the event of a server failure.

'iQ.Clustering'
iQ.Suite Configuration iQ.Clustering

Basics | Comments

Basics

Name	[F1]Q.Clustering [J]
Status	<input type="radio"/> Active <input checked="" type="radio"/> Not active
Server	[F1]WP_CO02/SRV/MP/GROUP/De [J]
Server for mailbox checking	[F1]WP_CO01/SRV/MP/GROUP/De [J]
Server for grabber checking	[F1]WP_CO01/SRV/MP/GROUP/De [J]

1. In the **Basics** tab of the configuration document (**Global Parameters** → **iQ.Clustering**), enter the name of your Domino server in the **Server** field. The configuration document applies to the server specified in this field.
2. In the **Server for mailbox checking** field, enter the name of the server whose mailboxes are to be additionally monitored. The own mailboxes are monitored automatically.
3. In the **Server for grabber checking** field, enter the name of the server whose MailGrabber is to be monitored.
4. Repeat this procedure for each server to be monitored.



8 Appendix

8.1 Access Rights Configuration Databases

8.1.1 Basics

As you know, Lotus Notes controls the access to databases by means of Access Control Lists (ACL). These lists are used to assign database access rights to users or user groups. For further information refer to the Lotus Notes/Domino documentation.

8.1.2 Using Predefined Groups

We recommend to use predefined groups to control the access to individual databases:

GROUP-TOOLS-ADMIN and the administrator group specified during installation (if applicable)	Changing configuration documents, database design modifications, and rights management; also refer to notes.ini
GROUP-TOOLS-SRV	Your server(s)
GROUP-TOOLS-USER	Your Notes users (for organiziQ.Clerk only)
GROUP-TOOLS- POWUSER	Your experienced Notes users (for organiziQ.Clerk only)

These groups are already included in the Access Control List with appropriate access rights. All you have to do, is to create the corresponding groups in the Name and Address Book.



During installation, the server hosting the iQ.Suite is entered with manager access rights in all ACLs of the relevant databases.

8.1.3 Using Your Own Groups

Observe the following if you decide to use your own groups:

8.1.3.1 ... for the Server

Servers must have at least editor rights to the iQ.Suite databases and must be included in all database roles.

8.1.3.2 ... for the Administrator/Manager

Administrators should have author or manager rights. Individual databases have additional admin roles to enable a finer structure of the rights. Assign the appropriate administrators to individual roles.

8.1.3.3 ... for the End User

For organiziQ.Clerk, users must have author rights to the delegate database (**g_del.nsf**). User access to any of the other databases is neither necessary nor useful. For a more detailed description refer to [“organiziQ.Clerk and Data Protection” on page 52](#).

8.1.3.4 ... for Administrator Notifications

The recipients of Administrator notifications are set in the **notes.ini** file under `Toolkit_Admin`, the default setting being the group specified during the installation. You may also create a specific group for these notifications, in which case it has to be entered in the **notes.ini** file.



The `%admin%` placeholder in the configuration documents is replaced with the entry under `Toolkit_Admin`.

8.2 Mail.Box Design

To simplify using the MailGrabber, a few changes to the **mail.box** of the server are made during the iQ.Suite installation. These changes do not have any effect on the Lotus Domino server and are primarily for display purposes.

The following design elements are added during the installation:

Element	Name	Purpose
View	MailGrabber\ Mailstatus	Displays the scanning and routing status
Macro	Reprocess Mails	Changes the status of an undeliverable mail so that it is reprocessed by the MailGrabber.
Macro	Release 'undeliverable' Mails	Changes the status of an undeliverable mail so that it is passed on by the router without processing by the MailGrabber.
Macro	Release Mails	Changes the status of any mail so that it is passed on by the router without processing by the MailGrabber.

8.3 Notes Log Database Design

The sequence of operations of each module is logged in the Notes Log database (**log.nsf**) of the server. To display this information, the design of the Notes Log or the design pattern is extended during installation.

The following design elements are added to **log.ntf** and **log.nsf** during the installation:

Element	Name	Purpose
Mask	Toolkit LogPage	Displays the entries
View	Grabber Log\ by Date	Sorts the entries by date
View	Grabber Log\ by Task	Sorts the entries by process

As of iQ.Suite 7, it is possible to use an own database for logging purposes, which has the same functionality as the **log.nsf** database but only contains iQ.Suite-relevant entries. To do so, create a database named **g_log.nsf** on the basis of the **log.nsf** template (supplied in the **grptools** directory) and copy it to a directory of your choice (recommended: **grptools** directory).

Then under the iQ.Suite **Global Parameters** menu, activate the following documents:

1. **Activate New Log Database**
2. **Flags for Log Database**

These documents contain standard settings for the creation of a new log database:

Database: **g_log.nsf**, copied to **grptools** directory
 Flags: 60,30

This causes the following changes in the **notes.ini** file:

1. `"toolkit_logdb=[path to log database]"` (enables the function)
 The path has to be entered as relative path from the **Data** directory!
2. `"toolkit_logdb_flags=[max. seconds],[max. lines]"` (optional)
 Sets the maximum waiting period in seconds or the maximum number of lines in the buffer. Whenever of these values is reached, the external log database is updated. Without `"toolkit_logdb"` setting, this entry is ignored. Both flags support values higher than 1. A "0" value is considered an error and replaced with the standard configuration ("60,30"). It is possible to set one flag only, e.g.:

```
toolkit_logdb_flags=123 (max. 123 seconds), or
toolkit_logdb_flags=,234 (max. 234 lines)
```

If your database has another name or if it is located in another directory, please adjust the path accordingly.

As an alternative, it is also possible to directly enter these parameters in the **notes.ini** file.



In case **Global Parameters** is disabled and no entries are found in the **notes.ini** file, or if the specified database does not exist, the **log.nsf** database is used for logging.

8.4 Entries in notes.ini

The installation program makes the following entries in the **notes.ini** file:

ServerTasks	...,tm_grab, td_grab
EXTMGR_ADDINS	te_hook
Toolkit_DataDir	<Relative path to the Notes data directory>
Toolkit_ExecDir	<Absolute path>
Toolkit_Admin	<Name>
Toolkit_LogLevel	6
Toolkit_MailIntercept	YES
Toolkit_MgrabThreads	<Max. number of threads for MailGrabber>
Toolkit_DgrabThreads	<Max. number of threads for DBGrabber>

For the meaning of each parameter, please refer to the Administration Manual.

8.5 Support for Multiple Mail.Boxes

As of Domino R5, it is possible to define multiple mailboxes to be used by the router.

This means iQ.Suite has to monitor several databases for new messages, and not just one. This is why support for multiple mail.boxes was implemented.

In order for iQ.Suite to work correctly after having changed the number of mailboxes, it must be ensured that only **those** databases are located in the server directory that are also processed by the router.



After having performed the changes, the server has to be restarted!

The following databases must be present if

- one mailbox is used: **mail.box**
- several mailboxes are used: **mail1.box, mail2.box, ...**



Any other mail.boxes must be removed from the data directory!



If you decide to set the number of mail.boxes differently, we recommend changing the server configuration as follows:

- Select the **Configuration** tab.
- Select **Server** and click on **Configurations**. The name of the server will be displayed.
- Double-click on the server name to open the configuration settings for the server.
- Select the **Router/SMTP** tab and enter the number of boxes you wish to use in the **Number of mail.boxes** field.
- Shut down the Domino server.
- Switch to the directory of your **mail.box** file. This will normally be `c:\lotus\domino\data`.
- Delete the **mail.box** file or the **mail1.box, mail2.box**, etc. files so that new ones can be created when the server is restarted.

This ensures that the correct mail.boxes are used.

8.6 List of Files

During the iQ.Suite installation, a number of files are copied to different directories.

8.6.1 grptools Directory

File	Description
?tm_*.dll	MailGrabber working modules
?td_*.dll	DatabaseGrabber working modules
toolkit.lic	License file
de\res*.txt	Message texts (English: en\res*.txt
*.nsf	Help/Configuration database
*.ntf	Templates for configuration databases
test*.*	Test viruses
ntk_attd.dll	Decompression tool for NSFs attached to documents
?tk_*.dll	Interfaces for calling third-party applications
?doscall.exe	NTI/NTA: Enables calling DOS programs and changing database access rights

8.6.2 Lotus Notes Program Directory

File	Description
?te_hook.dll	Extension Manager Add-Ins for database monitoring
libte_hook.a	The same for AIX
libte_hook.so	and for Linux and Sun Solaris
?tm_grab.exe	MailGrabber base module
?td_grab.exe	DatabaseGrabber base module
?t_setup.exe	Installation module

8.7 organiziQ.Clerk and Data Protection

As the advanced redirection document makes it possible to redirect messages without knowledge/consent of the actual addressee, access to this mask should by all means be restricted to individuals in a position of trust (data protection).

For this purpose, the following roles exist in the `g_del.nsf`:

[CREAT-BASIC]	May create basic forwarding
[CREAT-EXTENDED]	May create advanced forwarding
[CREAT-BODYGUARD]	May create redirection
[AUTH-BASIC]	May change other users' basic forwarding
[AUTH-EXTENDED]	May change other users' advanced forwarding
[AUTH-BODYGUARD]	May change other users' redirection
[READ-BASIC]	May read other users' basic forwarding
[READ-EXTENDED]	May read other users' advanced forwarding
[READ-BODYGUARD]	May read other users' redirection

The owners of these roles are allowed to read, create or modify the corresponding documents. For further information on the roles in organiziQ.Clerk please refer to your Administration Manual (versions as of 2003, Release Notes 5.2e).

The relation between these roles and standard ACL groups is shown in the table below:

Group	Function
GROUP-TOOLS-USER	[CREAT-BASIC]
GROUP-TOOLS-POWUSER	[CREAT-BASIC] [CREAT-EXTENDED] [CREAT-BODYGUARD] [AUTH-BASIC] [AUTH-EXTENDED] [AUTH-BODYGUARD] [READ-BASIC] [READ-EXTENDED] [READ-BODYGUARD]
GROUP-TOOLS-ADMIN	[CREAT-BASIC] [CREAT-EXTENDED] [CREAT-BODYGUARD] [AUTH-BASIC] [AUTH-EXTENDED] [AUTH-BODYGUARD] [READ-BASIC] [READ-EXTENDED] [READ-BODYGUARD]



The only difference between the GROUP-TOOLS-POWUSER group and the GROUP-TOOLS-ADMIN group is that power users are defined as authors and administrators as managers.



Be sure to assign these roles to your server and the administrator. Otherwise, the server / administrator will not have access rights to these documents.



Some roles may not be included in the ACL after upgrading from an older version (< R 5.0). In this case, add them to the ACL accordingly. Keep old roles following an update so that existing documents can still be accessed.

 **9**

Notes

