



Documentation

Installation

iQ.Suite 20.2

For IBM Domino

Document Version 1.0

Editor's Note

All rights reserved. This manual and the programs described therein are copyright-protected products of GBS Europa GmbH.

No part of this publication may be reproduced without written permission from GBS Europa GmbH.

All hardware and software names used are registered names and/or trademarks of their respective manufacturer/proprietor.

Copyright © 2017 GBS Europa GmbH, Ottostraße 4,
76227 Karlsruhe, Deutschland

Edition: November 2017

 **Table of Contents**

1	Preface	1
1.1	Hotline.....	1
1.2	Copyright	1
1.3	Warranty	2
1.4	License Terms	2
1.5	Third-Party Copyright Notes	2
1.6	Details on the Manuals	3
2	Quick Start Guide	5
2.1	Preliminary Steps.....	5
2.2	Installation.....	5
2.3	Follow-up Steps	5
3	Installation Requirements	7
3.1	System Requirements	7
3.1.1	For all Operating Systems	7
3.1.2	Requirements for Windows.....	10
3.1.3	Requirements for Linux.....	12
3.1.4	Requirements for IBM AIX	14
3.1.5	Requirements for Oracle Solaris/SUN Solaris	14
3.2	Important Actions and Measures	15
3.2.1	Version Control	15
3.2.2	Rights and Data Backups	16
4	Installation of iQ.Suite	19
4.1	Preliminary Steps.....	19
4.1.1	Check Default Paths	19
4.1.2	Minimizing Domino Server's Downtime During Installation (Optional).....	21
4.1.3	Using External Programs	24
4.1.3.1	Virus Scanner	24
4.1.3.2	Decompressor	25
4.1.3.3	Spam Analyzers	25
4.1.4	Selecting the Language	26
4.2	Installation Routine Under Windows.....	26
4.2.1	Start Setup	26
4.2.2	Select Setup Type.....	27
4.2.3	Set Paths and Directories	27

4.2.4	Set notes.ini Directory and Configuration Databases	27
4.2.5	Install Configuration Databases as Replicas	28
4.2.6	Update/Install New Configuration Databases.....	28
4.2.7	Set Administrator Group for iQ.Suite	28
4.2.8	Set Administrator Group for iQ.Suite WebClient	28
4.2.9	Other Options	29
4.2.10	Specify Proxy Server	29
4.2.11	Set up SASI Analyzer / Update Service	29
4.2.12	Configuring Virus Scanners.....	30
4.2.13	Defining Working Directory for Temporary Files	31
4.2.14	Summary	32
4.2.15	Installation Sequence	33
4.3	Installation Under IBM AIX, Linux and Oracle Solaris/SUN Solaris	34
4.3.1	Before Starting the Installation Script	34
4.3.2	Starting the Installation Script.....	35
4.3.3	Set up SASI Analyzer / Update Service (Linux Only).....	37
4.3.4	Verify File Access Rights.....	38
4.3.5	Verify Database Access Rights	39
4.4	Silent Installation and Silent Uninstallation	40
4.4.1	Silent Installation under Windows	40
4.4.2	Silent Installation under Unix.....	40
4.5	Installation on Replicated Servers.....	41
4.5.1	Installation Under Windows	42
4.5.2	Installation: IBM AIX, Linux and Oracle Solaris/SUN Solaris	43
4.6	Installation on Partitioned Servers	44
4.6.1	Installation Under Windows	44
4.6.2	Installation: IBM AIX, Linux and Oracle Solaris/SUN Solaris	45
4.6.2.1	Same Domino program directory.....	45
4.6.2.2	Sample Installation	46
5	Follow-up Steps	49
5.1	Summary.....	49
5.2	Check notes.ini.....	50
5.3	Optional Features.....	52
6	Optional Features	53
6.1	iQ.Suite WebClient.....	53
6.1.1	System Requirements	54
6.1.2	Installation	55
6.1.3	Configuration	56
6.1.3.1	Website Settings in the Domino Directory	56

6.1.3.2	Configuration in the iQ.Suite	57
6.1.3.3	Restarting the HTTP Task.....	58
6.1.3.4	Login to the iQ.Suite WebClient	59
6.2	iQ.Mastering (Generic Mastering)	60
6.2.1	Technical Background	60
6.2.2	Symantec Mail Security for Domino (Parallel Use).....	62
6.2.3	McAfee Security for Email Servers (Parallel Use: Windows).....	63
6.3	iQ.Clustering	64
6.3.1	Benefits and Fields of Application.....	64
6.3.1.1	High-Availability and Fail-Safety.....	64
6.3.1.2	Load Balancing.....	65
6.3.1.3	Distributed Computing	65
6.3.2	Requirements for iQ.Clustering.....	66
6.3.2.1	Email Checking Sequence	67
6.3.2.2	Grabber Checking	67
6.3.2.3	Installation Requirements	68
6.3.3	Installation Principle	69
6.3.4	iQ.Clustering Configuration.....	71
7	Update	73
7.1	Preparing the Update.....	73
7.2	Update Routine.....	74
7.2.1	Update Routine: Windows	74
7.2.2	Update Routine: IBM AIX, Linux and Oracle Solaris/SUN Solaris	76
7.3	Follow-up Steps	77
7.4	Important Notes on Configuration after an Update	79
7.4.1	Trailer Advanced.....	79
7.4.2	Other Adjustments	79
7.5	Update on Replicated Servers	80
7.5.1	Update: Windows.....	80
7.5.2	Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris	81
7.6	Update on Partitioned Servers	82
7.6.1	Update: Windows.....	82
7.6.2	Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris	82
8	Uninstallation of iQ.Suite	83
8.1	Uninstall: Windows	83
8.2	Uninstall: IBM AIX, Linux and Oracle Solaris/SUN Solaris	84
9	Appendix	85

- 9.1 Access Rights in Configuration Databases85
 - 9.1.1 Using Predefined iQ.Suite Groups85
 - 9.1.2 Using Your Own Groups85
- 9.2 Design Changes for the Installation87
 - 9.2.1 Design Elements: Log Database87
 - 9.2.2 Design Elements: Statrp.nsf88
 - 9.2.3 Design Elements: mail.box89
 - 9.2.4 Support for Multiple mail.boxes90
- 9.3 List of Files and Directories Under Windows91
 - 9.3.1 Log Files91
 - 9.3.2 iQ.Suite Data Directory91
 - 9.3.3 iQ.Suite Program Directory92
 - 9.3.4 Domino program directory92
- 9.4 List of Files and Directories Under Unix93
 - 9.4.1 Log Files93
 - 9.4.2 iQ.Suite Data Directory93
 - 9.4.3 iQ.Suite Program Directory93
 - 9.4.4 Domino Program Directory94
 - 9.4.5 Common iQ.Suite Program Directory94



1 Preface

1.1 Hotline

To give you the best possible support, we need the following information from you in the event of a fault:

-  Product version
-  License number
-  Domino server version including any service pack
-  Operating system and version including any service pack
-  Log Book entries created at log level 8 (for runtime errors)
-  Any RIP files or NSD files
-  Configuration files
-  Log files
-  TECHNICAL_SUPPORT folder (in the installation folder)

The GBS Support Team is available from 8:30 AM to 6:00 PM (time zone: EST).

-  Europe, Asia, other
 -  Tel.: +49 (0)1806 49 01 11
 -  Fax: +49 721 49 01 1922
 -  Email D: hotline@de.gbs.com
-  USA & Canada:
 -  Tel.: +1 877-228-6178
 -  Email: help@gbs.com

1.2 Copyright

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

Copyright 1992-2017 GBS Europa GmbH,
All rights reserved.

1.3 Warranty

GBS assumes no liability, express or implied, for the documentation. This includes quality, design, adherence to commercial standards, 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 up-to-date information, please contact the GBS Sales Department.

1.4 License Terms

The GBS license terms are available on the product CD and the GBS website. Any license agreements from third-party software manufacturers are included with the software product as a PDF file.

1.5 Third-Party Copyright Notes

The package includes third-party products listed in the "Third Party License Agreements" document. This document is available in the program directory. In addition, the following applies:

IBM and AIX are trademarks of International Business Machines (IBM) Corporation. Lotus, Notes and Domino are registered trademarks of IBM Corporation.

Microsoft, MS, Windows and the Windows Logo are registered trademarks of Microsoft Corporation in the United States of America and/or other countries.

Solaris is a registered trademark of Oracle, Avira is a registered trademark of Avira GmbH. McAfee is a registered trademark of Networks Associates, Inc. Any other products mentioned in this document are subject to the copyright provisions of their respective manufacturers. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

The components listed below are also protected by copyright, although not explicitly listed in the "Third Party License Agreements" document:

-  **AntiVir powered by Avira**
Copyright (c) 2006 Avira GmbH
-  The file **dbghelp.dll**
Copyright (c) Microsoft Corporation
-  **Sophos SASI**
Copyright (c) 2006, Sophos Group

1.6 Details on the Manuals

Personal Designations

Our Manuals are addressed equally to both genders. Therefore, we make every effort to use gender-neutral language. Since it is not entirely possible to avoid personal designations, we use the word forms he/she, his/hers or him/her in these cases.

Symbols



Warning.

Refers to critical situations. Please carefully read these messages to minimize the risk of data loss, damage to your system, etc.



Information.

Refers to important but noncritical situations.



Tip.

Provides assistance for a specific issue or describes special workarounds and features.

Freely accessible documentation is available on our website under www.gbs.com.

If you have any suggestions on how we can make further improvements, we would be happy to get your feedback. Send an email to: manual@de.gbs.com



2 Quick Start Guide

The present Quick Start Guide summarizes the installation procedure. We recommend you, to click on the links to the detailed descriptions, since the information described in these chapters may be important for iQ.Suite functionality.

2.1 Preliminary Steps

For a detailed description of the necessary preliminaries please refer to [“Installation Requirements” on page 7.](#)

1. Stop the Domino server.
2. Create a backup of the Domino server.

2.2 Installation

For a detailed description of the installation procedure and licensing information please refer to [“Installation of iQ.Suite” on page 19.](#)

1. Select the setup routine according to your operating system.
2. Run the entire setup.

2.3 Follow-up Steps

For a detailed description of the necessary follow-up steps please refer to [“Follow-up Steps” on page 49.](#)

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 the iQ.Suite Administration Manual.

3 Installation Requirements



This manual describes the features of iQ.Suite for Domino 20.2. At the installation of iQ.Suite > 20.2 these details can vary. Any changes made in subsequent iQ.Suite versions are described in the Release Notes located in the iQ.Suite installation directory.

3.1 System Requirements

3.1.1 For all Operating Systems



Do not use any Domino or Notes versions whose EOS (End-of-Service) has been reached. Using a discontinued version could result in unwanted effects and malfunctions of iQ.Suite. iQ.Suite support ends with the version discontinuation notice by IBM.



If you want to update to iQ.Suite 19.1 or higher and you are using Trailer Advanced in a replicated environment with iQ.Suite servers of Version 17.1.0 to 18.1.4/19.0.2, then update your iQ.Suite servers before replicating the new databases as follows:

17.x -> Update to 17.2.2

18.x -> Update to 18.1.5

19.0.x -> Update to 19.0.3

Otherwise, saving Trailer Advanced Job documents with the new design of 19.1 would cause a crash of the older iQ.Suite servers.

Make sure the following requirements are met:

- IBM Domino server and Notes client as of 8.0.1. Determine the path of your installation and the *notes.ini*.
- One of the following operating systems:
 - Windows Server 2008 / 2008 R2 (for 32-bit and 64-bit systems respectively)
 - Windows Server 2012 / 2012 R2 / 2016
 - AIX 7.1 or 7.2
 - Oracle Solaris 10

- Red Hat Enterprise Linux (RHEL): Version 5, 6 or 7
- SuSE Linux Enterprise Server (SLES): Version 10, 11 or 12

Use the table under "[Version Control](#)" on [page 15](#) to be sure to install the correct iQ.Suite version for your operation system and Domino server

- RAM: Minimum 4 GB are recommended¹.
- iQ.Suite User Portal: To display Trailer documents on the web interface, a Java Runtime as of Version 1.5 is required. The other parts of the User Portal can be used without Java.
- Hard Disk:
 - For iQ.Suite: approx. 1 GB
 - For each virus scanner: additionally 1 GB (approx.)

Also take into account the additional space needed for Notes client/Domino server. The disk space actually required cannot be determined accurately as it depends on the following factors:

- Log level for Grabbers and jobs: size of the iQ.Suite log (*log.nsf* or *g_log.nsf*).
- Size of the `TECHNICAL_SUPPORT` directory in the iQ.Suite program directory.
- Frequency and size of alarm emails: size of the iQ.Suite quarantine (default *g_arch.nsf*).
- Archival frequency when using iQ.Suite Safe and size of archived emails: size of the archival databases.
- Size and storage length of the archival databases and log databases of iQ.Suite Clerk, if using the retroactive forwarding.
- Single logging when using iQ.Suite Budget: size of the iQ.Suite log (default: *g_prot.nsf*). Please note that the size can easily reach 2-3 GB in a relatively short period of time.

1. RAM requirements depend on the number of modules and the external applications used. Additionally approx. 1 GB for each component that performs updates (virus scanner, anti-spam engine).



The setup of the 32-bit Domino server on a 64-bit computer allows to perform the installation in the program directory for 64-bit applications (C:\Program Files\ instead of C:\Program Files(x86)\). This is, however, in contradiction to the operating system conventions. The setup of the 32-bit iQ.Suite on a 64-bit computer does not support installing in the program directory for 64-bit applications (C:\Program Files\), as this would make subsequent updates or an automatic uninstallation impossible. We recommend installing the Domino server in a valid directory (i.e. any directory other than C:\Program Files\) before installing iQ.Suite.



Crypt: For S/MIME, use the new **S/MIME + KeyManager Engine**. The traditional Crypt Engine with *tk_smime.dll* only works on 32-bit versions of Windows, Linux and Solaris. Furthermore, the Crypt Engine does not support all modern cryptographic methods. If you want to switch your configuration to the new Engine, please note that all S/MIME certificates must be managed in iQ.Suite KeyManager. For further information on iQ.Suite KeyManager, please contact the GBS Sales Team.



Crypt: For S/MIME, use the new **S/MIME + KeyManager Engine**. The traditional Crypt Engine with *tk_smime.dll* only works on 32-bit versions of Windows, Linux and Solaris. Furthermore, the Crypt Engine does not support all modern cryptographic methods. If you want to switch your configuration to the new Engine, please note that all S/MIME certificates must be managed in iQ.Suite KeyManager².

Under Windows, please note the additional Runtime requirements for the *tk_smime.dll*. Refer to [“Requirements for Windows” on page 10](#).

For the virus scanner ‘Kaspersky’: This virus scanner has under Linux higher system requirements than the other iQ.Suite components. Required is:

Red Hat Enterprise Linux (RHEL) as of Version 5.6

or

SUSE Linux Enterprise Server (SLES) as of Version 11 SP1

2. For further information on iQ.Suite KeyManager, please contact the GBS Sales Team.

For the virus scanner 'McAfee' on SUSE Linux Enterprise Server (SLES) 12:

This virus scanner requires on this platform the Legacy Module of SLES 12. The support period of this Legacy Module is limited. With the end of support by SUSE, the GROUP Business Software Europa GmbH ends its support of the McAfee virus scanner based on this module.

Please also observe the special requirements related to your operating system, which are described in the sections below.

3.1.2 Requirements for Windows

To install iQ.Suite you need write access to the Windows server Registry. Administrators usually have these rights.

iQ.Suite can be run under Windows on a 32-bit or 64-bit Domino server. Two separate installation packages are available to this end. If not already installed, the required Microsoft Visual C++ Redistributable Packages are installed in the course of the iQ.Suite installation:

- Microsoft Visual C++ 2008 SP1 Redistributable Package (x86)
- Microsoft Visual C++ 2008 SP1 Redistributable Package (x64)
- Microsoft Visual C++ 2013 Redistributable Package (x86)
- Microsoft Visual C++ 2013 Redistributable Package (x64)
- Microsoft Visual C++ 2017 Redistributable (x86) - V14.10.25017
- Microsoft Visual C++ 2017 Redistributable (x64) - V14.10.25017

If you use the traditional Crypt Engine with 'tk_smime.dll', the *Microsoft Visual C++ 2005 SP1 Redistributable Package* must be installed manually. For the installation, execute the file `vcredist_80_sp1_x86.exe` which you can find under `<execdir>\support\vs-runtime`.

When moving the operating system from 32-bit to 64-bit certain iQ.Suite components can not be overridden properly. Thus, uninstall the iQ.Suite on the 32-bit system first and execute an iQ.Suite installation on the 64-bit system afterwards. When importing iQ.Suite configuration, please take into account the following changes:

If the file **nDosCall.exe** is used in the configuration, the resolution of the %ExecDir% path can lead to problems under Windows 64-bit. Instead of %ExecDir% an absolute path can be used as workaround.

3.1.3 Requirements for Linux

The installation under **Linux** requires installation of the software packages which are mentioned below.



Some of the packages listed below must be installed even if a newer version of the package is already installed. This is the case when the newer package use another internal library name, e.g. libstdc++.so.6 instead of libstdc++.so.5. In such a case the newer package receives a new package name as well (not only a new version number). It can be installed on the same system as the older package. The new package does not replace the older one.

For 32-bit Domino 8.5 and 32-bit iQ.Suite (32-bit packages):

Library	RHEL 5	RHEL 6
libpng12.so.0	libpng.i386	libpng.i686
libstdc++.so.5	compat-libstdc++-33.i386	compat-libstdc++-33.i686

Library	SLES 10	SLES 11
libpng12.so.0	libpng-32bit	libpng12-0-32bit
libstdc++.so.5	compat-libstdc++-32bit	libstdc++33-32bit



Do not use the *-32bit packages on a 32-Bit SLES. Instead of that, use the packages without the “-32bit” text. Example: Install *libpng12-0* instead of *libpng12-0-32bit*.

For 32-bit Domino 9 and 32-bit iQ.Suite:

Library	RHEL 6	RHEL 7
libpng12.so.0	libpng.i386	libpng.i686
libstdc++.so.5	compat-libstdc++-33.i386	compat-libstdc++-33.i686

Library	SLES 11	SLES 12
libpng12.so.0	libpng12-0-32bit	libpng12-0-32bit
libstdc++.so.5	libstdc++33-32bit	libstdc++33-32bit



The *libstdc++.so.5* library is only required if the McAfee virus scanner is used.
 The *libstdc++33-32bit* package is contained on SLES 12 in the Legacy Module.

For 64-bit Domino 9 and 64-bit iQ.Suite:

For 64-bit Domino 9 and 64-bit iQ.Suite, several 32-bit and 64-bit packages must be installed:

■ 64-Bit packages:

Library	RHEL 6	RHEL 7
libpng12.so.0	libpng	libpng12

Library	SLES 11	SLES 12
libpng12.so.0	libpng12-0	libpng12-0

■ 32-Bit packages:

Library	RHEL 6	RHEL 7
libc.so.6	glibc.i686	glibc.i686
libgcc_s.so.1	libgcc.i686	libgcc.i686
libstdc++.so.5	compat-libstdc++-33.i686	compat-libstdc++-33.i686
libstdc++.so.6	libstdc++.i686	libstdc++.i686
libz.so.1	zlib.i686	zlib.i686

Library	SLES 11	SLES 12
libc.so.6	glibc-32bit	glibc-32bit
libgcc_s.so.1	libgcc43-32bit	libgcc_s1-32bit
libstdc++.so.5	libstdc++33-32bit	libstdc++33-32bit
libstdc++.so.6	libstdc++43-32bit	libstdc++6-32bit
libz.so.1	zlib-32bit	libz1-32bit



The *libstdc++.so.5* library is only required if the McAfee virus scanner is used. The *libstdc++33-32bit* package is contained on SLES 12 in the Legacy Module.



Use the following command to identify architecture of your installed software package: `rpm -qf "%{Arch}"%{Name}-%{Version}-%{Release}\n' -q <package name>`.

Since the *-32bit packages from SLES are intended for the use on 64-bit SLES systems, the architecture displayed is shown as *x86_64*. However, these packages contain 32-bit library files.

3.1.4 Requirements for IBM AIX

Installation under Domino requires the C Set ++ Runtime as of Version **10.1.0³**. To determine the version installed, use the command **lspp -l xIC.rte**. If a previous version is used, iQ.Suite may not start or some of the DLLs may not be loaded.

3.1.5 Requirements for Oracle Solaris/SUN Solaris

For full iQ.Suite functionality, a **libstdc++-3.3** is required. This is available, for instance, from www.sunfreeware.com in the software package **libgcc-3.3**.

Oracle Solaris 10 requires the C++ Runtime Patch **119963-20**.

3. This software package is provided in the IBM download area.

3.2 Important Actions and Measures

The Domino version of the iQ.Suite package must be the same as for the Domino server. For instance, a Domino 8 iQ.Suite has to be installed on a Domino 8 server.

3.2.1 Version Control

Use the following table to check whether you are about to install the correct iQ.Suite version for your Domino server. Please check related IBM system requirements such as required updates, service packs, etc:

Operating System / Server	Domino 8.5		Domino 9.0	
	32-Bit	64-Bit	32-Bit	64-Bit
Windows Server 2008	as of iQ.Suite 18	as of iQ.Suite 18	-	-
Windows Server 2008 R2	as of iQ.Suite 18			
Windows Server 2012	-	-	as of iQ.Suite 18	as of iQ.Suite 18
Windows Server 2012 R2	-	-	as of iQ.Suite 18	as of iQ.Suite 18
Windows Server 2016	-	-	as of iQ.Suite 20	as of iQ.Suite 20
Red Hat Enterprise Linux 5	as of iQ.Suite 18	-	-	-
Red Hat Enterprise Linux 6	as of iQ.Suite 18	-	as of iQ.Suite 18	as of iQ.Suite 18
Red Hat Enterprise Linux 7	-	-	as of iQ.Suite 18	as of iQ.Suite 18
SuSE Linux Enterprise Server 10	as of iQ.Suite 18	-	-	-

Operating System / Server	Domino 8.5		Domino 9.0	
	32-Bit	64-Bit	32-Bit	64-Bit
SuSE Linux Enterprise Server 11	as of iQ.Suite 18	-	as of iQ.Suite 18	as of iQ.Suite 18
SuSE Linux Enterprise Server 12	-	-	as of iQ.Suite 20	as of iQ.Suite 20
Oracle Solaris 10	as of iQ.Suite 18	-	-	-
IBM AIX 7.1	as of iQ.Suite 18			
IBM AIX 7.2	-	-	as of iQ.Suite 18	as of iQ.Suite 18

3.2.2 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 address book with manager access rights to the iQ.Suite databases. Members of this group will receive all automatic notifications issued by iQ.Suite (default: *IQSUITE-ADMIN*). Refer to ["Access Rights in Configuration Databases" on page 85](#). For further information on roles and access rights please refer to the documentation for your Domino server and Notes client.
4. By default, during the installation process, the Domino databases and templates installed are signed with the ID of the current Domino server. To prevent this, set the following global parameter in the *notes.ini* of the Domino server before installing iQ.Suite:


```
ToolKit_DBG_Setup_Nosign_DBS=1
```
5. Stop the Domino server.

6. Before starting the installation, make a backup of the *log.ntf*, *mailbox.ntf* and *statrp.ntf/statrp5.ntf* files.

Your own templates will be preserved during the installation. iQ.Suite will add the necessary extensions to any existing templates.

4 Installation of iQ.Suite

4.1 Preliminary Steps

Before running the installation, check the settings specified under "[Installation Requirements](#)" on page 7. Otherwise an error-free installation cannot be guaranteed.

Close all unnecessary applications, in particular the Domino server and your Notes client. Otherwise some files may not be installed properly if they are being used by other programs.



In order to check some system requirements, a test virus (Eicar) is installed. Be sure to disable any real-time or on-access scan functions of the virus scanner used for the iQ.Suite working directory.

4.1.1 Check Default Paths

iQ.Suite default paths under Windows

- Domino directory:
`c:\Program Files\IBM\lotus\domino`
- iQ.Suite program directory:
`c:\Program Files\IBM\lotus\domino\iqsuite`
- iQ.Suite data directory:
`c:\Program Files\IBM\lotus\domino\data\iqsuite`
- iQ.Suite working directory: Directory specified in the `ToolKit_ExclusiveTempDir` parameter, for example
`C:\iQTemp\%ServerCommonName%`

If you do not wish to install the databases included in the installation package but your own ones (with the same name), copy these databases to the installation directory before starting the installation. The installation directory also contains the installation file named `setup_iQSuite<Version>.exe`.

iQ.Suite default paths under Unix

■ Domino directory:

Linux: `/opt/lotus/notes/latest/linux`

AIX: `/opt/lotus/notes/latest/ibmpow`

Solaris: `/opt/lotus/notes/latest/sunspa`

■ iQ.Suite program directory:

`/home/domino/iqsuite`

■ iQ.Suite program directory (shared):

`/opt/iQ.Suite-<Version>`

■ iQ.Suite data directory:

`/home/domino/notesdata/iqsuite`

■ iQ.Suite working directory: Directory specified in the `ToolKit_ExclusiveTempDir` parameter, for example

`C:\iQTemp\%ServerCommonName%`

If neither an environment variable nor `ToolKit_TempDir` is set, `/tmp` is used. Check upper/lower case spelling.

If you do not wish to install the databases included in the installation package but your ones (with the same name), copy these databases to the installation directory before starting the installation.



Under **AIX**: If iQ.Suite is not installed in the default path (`/opt`), the `LIBPATH` environment variable has to be manually set to the appropriate directory under `iQ.Suite-<version>/lib` in each server instance. Otherwise the Hook will not be loaded, as the path settings for the required system libraries are not correct. In this case, email processing is aborted with the error message 'TE_Hook is missing'.

4.1.2 Minimizing Domino Server's Downtime During Installation (Optional)

During the iQ.Suite installation, the database templates contained in the setup are signed with the current server or user ID which can be very time-consuming. This section explains how to manually sign the templates before the installation is started.

In general, we recommend to skip this section and let the installation automatically sign the templates. However, if the need arises, manual signing can reduce the Domino server downtime, especially if the signing key has a high security level (for example, 2 048 bit) because the amount of time required for signing increases with the key length.

If you choose to manually sign the templates, the first step is to extract the templates from the iQ.Suite setup package. If the same iQ.Suite version is going to be installed on several servers, extracting and signing the templates need only be performed once.

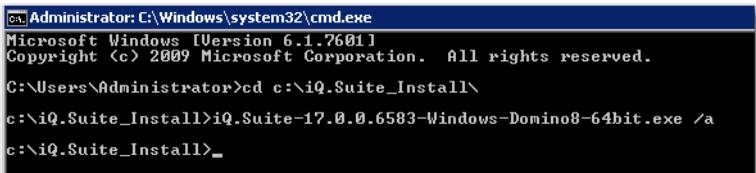
Under Windows

1. Save the setup file (EXE) on your file system:

Example: C:\iQ.Suite_Install\

2. In the Windows prompt, switch to the directory that contains the setup file and use the /a command to start the setup in administrative mode:

```
<setup file> /a
```



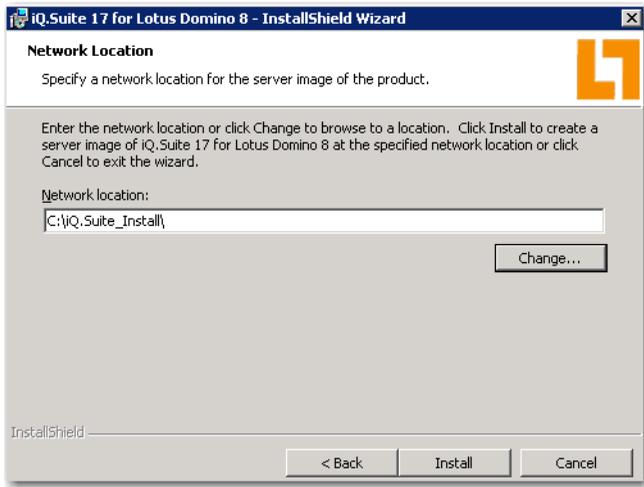
```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

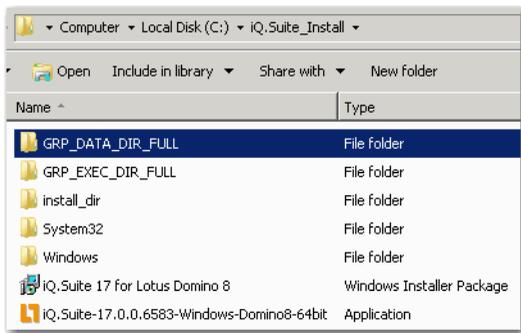
C:\Users\Administrator>cd c:\iQ.Suite_Install\
c:\iQ.Suite_Install>iQ.Suite-17.0.0.6583-Windows-Domino8-64bit.exe /a
c:\iQ.Suite_Install>_
  
```

The InstallShield Wizard opens.

3. In the InstallShield dialog, select a target folder (it can be a temporary folder) in which a so-called server image of the setup package will be created. This server image is merely a collection of files unpacked from the setup package.

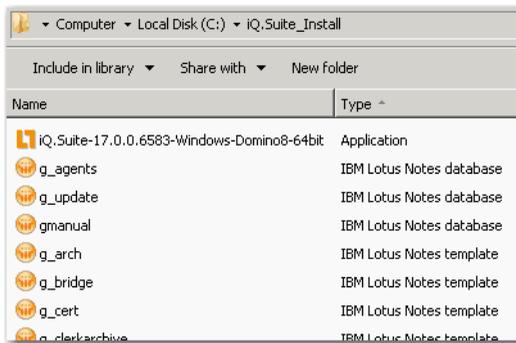


4. Click on INSTALL and FINISH.
5. Open the target folder:



The subdirectory `GRP_DATA_DIR_FULL` contains the iQ.Suite databases (*.nsf) and database templates (*.ntf). The other unpacked files are not needed and should be deleted.

6. Use the Domino Administrator client to sign the databases and database templates.
7. Copy the signed databases and database templates to the same folder that contains the setup package.



8. In the *notes.ini*, set the parameter `ToolKit_DBG_Setup_Nosign_DBS=1` to disable the automatic signing during installation.
9. To additionally reduce installation time, refer to the notes on the global *notes.ini* parameter `ToolKit_SetupNoSafeDbs` in the iQ.Suite Administration Manual.
10. Run the setup as explained in the following sections. The setup program will automatically pick up the database files that are stored in the same folder as the setup package and use them instead of the original files inside the setup package.

Under Unix

1. Save the setup file on your file system, for example:
`/home/dom9_x64/temp/iQ.Suite-<version>-Linux-Domino9-64bit.tar.gz`
2. To extract the database templates from the setup package, in the server console, enter the following command:
`gzip -cd iQ.Suite-<Version>-Linux-Domino9-64bit.tar.gz | tar -xvf -`
 The databases (**.nsf*) and database templates (**.ntf*) are unpacked to the subdirectory `iQ.Suite-<version>/data`. The other files that have been unpacked to `iQ.Suite-<version>` are not needed for manual signing and can be deleted.
3. In the *notes.ini*, set the parameter `ToolKit_DBG_Setup_Nosign_DBS=1` to to disable the automatic signing during installation.

4. To additionally reduce installation time, refer to the notes on the global *notes.ini* parameter `ToolKit_SetupNoSafeDbs` in the iQ.Suite Administration Manual.

5. Follow the usual installation procedure as explained in the following sections, with one exception:

After the setup package has been unpacked, copy the manually signed databases and database templates to the `iQ.Suite-<version>` directory.

The setup program will automatically pick up the database files that are stored in that directory and use them instead of the original files in the `iQ.Suite-<version>/data` subdirectory.

4.1.3 Using External Programs

iQ.Suite is able to use external programs, which have to be installed and licensed separately. Standard configuration documents are provided for some external programs. These documents can be adapted to your specific needs.



If you wish to use external programs not preconfigured in the iQ.Suite, please contact your supplier's Support Team.

4.1.3.1 Virus Scanner

For virus scanning the iQ.Suite supports various third-party virus scanners. The scanners must either be installed separately on the server (External Scan Engines) or the scanner is installed as integrated scanner in the course of the iQ.Suite setup. At the moment, the following integrated scanners are supported¹:

- Avira Scan Engine
- Avira Scan Engine with APC Option
- Kaspersky Scan Engine
- McAfee Scan Engine
- Sophos Scan Engine
- Sophos Scan Engine Sandboxing

1. For further information on these virus scanners, please refer to the separate documents. Download on www.gbs.com.

The iQ.Suite standard configuration contains a pre-set configuration document for each supported virus scanner under WATCHDOG -> UTILITIES -> VIRUS SCANNER. If there is no configuration document available for your virus scanner please contact the GBS Support Team.

For further Information on the virus scanner configuration please refer to the iQ.Suite Administration Manual. If you are using McAfee Groupshield for Domino, also refer to ["iQ.Mastering \(Generic Mastering\)" on page 61](#).

4.1.3.2 Decompressor

iQ.Suite includes an integrated decompressor (unpacker) in form of a DLL (exception: AIX). It is automatically enabled and can be used immediately after installation. If you plan further (external) unpackers, these have to be separately licensed, installed and enabled in the configuration documents.

For further Information on the decompressor please refer to the iQ.Suite Administration Manual.

4.1.3.3 Spam Analyzers

iQ.Suite includes the spam analyzers 'SASI' (Sophos Anti Spam Interface) and 'Kaspersky Anti-Spam'. These spam analyzers are available under Windows and Linux only and can be enabled and used as soon as the installation is complete. The only requirement is a licensed iQ.Suite Wall module and an additional license for the respective spam analyzer.

For the configuration of spam analyzers, please refer to the iQ.Suite Administration Manual.



If you wish to use additional (external) analyzers, these must be licensed, installed and enabled in the configuration documents separately.

Particularities of SASI:

As SASI requires periodic spam pattern updates, you can set whether or not you are to be informed of the success (or failure) of a spam pattern update by the SASI update service. Refer to [“Set up SASI Analyzer / Update Service” on page 29](#) and [“Set up SASI Analyzer / Update Service \(Linux Only\)” on page 37](#).

For further information on SASI, please refer to the separate document (tech-Doc). Download on www.gbs.com.

4.1.4 Selecting the Language

The installation routine can be run in either German or English. Under Windows, the language is selected at the beginning of the installation routine. Under Unix a selection is only required if the language can not be identified from the \$LANG environment variable. For all other operating systems supported, the installation is performed in English.



The installation language setting selected here is independent of the language later used in iQ.Suite for administration purposes. To change the language in the administration console, either use the LANGUAGE button or set the ToolKit_ServerLanguage parameter in the *notes.ini* to the desired value ('en' or 'de').

4.2 Installation Routine Under Windows

4.2.1 Start Setup



Start the setup in a local drive or from a connected network drive. Starting the installation from a UNC path (`\\computer\directory`) is not possible.

1. From the installation package, run the following file:
iQ.Suite-<version>-Windows-Domino<version>-<32/64>bit.exe
2. Select the desired setup language for iQ.Suite installation.
3. For iQ.Suite installation particular Microsoft software components have to be installed. Missing components are installed from the installation package automatically, thus without these components no iQ.Suite setup is possible.

Confirm the installation and licensing messages. For the installation a wizard is started.

4. Confirm the iQ.Suite setup start and agree with the license terms.

4.2.2 Select Setup Type

Select the desired installation setup mode:

■ **Standard** (recommended)

In this mode, only default settings are used and basic information e.g. paths is prompted for. Before iQ.Suite is actually installed, a configuration summary (list of installation settings) selected is displayed. Check all of your entries and then confirm the summary.

■ **Advanced**

This mode provides a number of additional settings and thus allows to change the iQ.Suite default settings. Only select this mode if you need special update configurations or work in partitioned environments.

4.2.3 Set Paths and Directories

(in 'Advanced' mode only)

Enter the path to the Domino server and iQ.Suite executable files.

4.2.4 Set notes.ini Directory and Configuration Databases

Enter the path to the *notes.ini*, in general to the data directory of the Domino server. For partitioned servers you can specify several paths to the *notes.ini* files.

Also enter the subpath to the iQ.Suite configuration databases. In the 'Advanced' mode you can enter special settings for partitioned servers by selecting the 'Installation on partitioned servers' checkbox. For further Information on the installation on partitioned servers please refer to ["Installation on Partitioned Servers" on page 44.](#)

4.2.5 Install Configuration Databases as Replicas

(in 'Advanced' mode only)

If you wish to install the configuration databases as replicas of existing databases, enable here the option **Database installation in replicated environment**. In the dialog displayed next, enter the name of the server and the subdirectory where the databases are located.

The iQ.Suite installation also modifies the design of various standard databases. Refer to "[Design Changes for the Installation](#)" on page 87. To leave the database design unchanged, disable this option.

4.2.6 Update/Install New Configuration Databases

(in 'Advanced' mode only)

If a previous iQ.Suite installation already exists on your computer, you can choose between updating your configuration databases to the new version (update) and running a new installation including the standard database configuration. While a new installation implies that the old databases are deleted, an update provides the possibility to keep the existing configuration for the time being and import the standard configuration at a later stage.

4.2.7 Set Administrator Group for iQ.Suite

(in 'Advanced' mode only)

In the ADMINISTRATION dialog, enter the name of the administrator group, as defined under "[Rights and Data Backups](#)" on page 16. The name of the administrator group is entered in the *notes.ini* in the `ToolKit_Admin` parameter. It is also stored as administrator in the ACL of the iQ.Suite configuration databases.

4.2.8 Set Administrator Group for iQ.Suite WebClient

(only in 'Advanced' mode and only if the 'iQ.Suite WebClient' feature is selected)

In the ADMINISTRATION dialog, an administrator group contained in the Domino address book must be specified. With this, the members of this administrator group will obtain unrestricted administrative access to the WebClient component „Roles and Rights“. Default: `iQSuite-WebAdmin`

During setup, this administrator group will be automatically added to the iQ.Suite configuration's global parameter `WebClient_AdminGroup`.

4.2.9 Other Options

(in 'Advanced' mode only)

The first section of the OTHER OPTIONS dialog provides options to sign databases with the server ID or a user ID. To sign the databases of partitioned servers with different IDs enter the desired user ID in the *notes.ini* of the corresponding partition using the `Toolkit_SetupIDFile` parameter.

The second section provides options to exclude the templates of particular configuration databases from a design update.

4.2.10 Specify Proxy Server

(in 'Advanced' mode only)

During the setup, you can specify a proxy server. This can be particularly useful in iQ.Suite configurations where spam analyzers or virus scanners require periodic spam pattern or virus pattern updates.

If you are using a proxy server, enable the checkbox and enter the proxy settings for IP address, port, user and password. In the **Proxy URL** field you can specify both the name and the IP address of the proxy server.

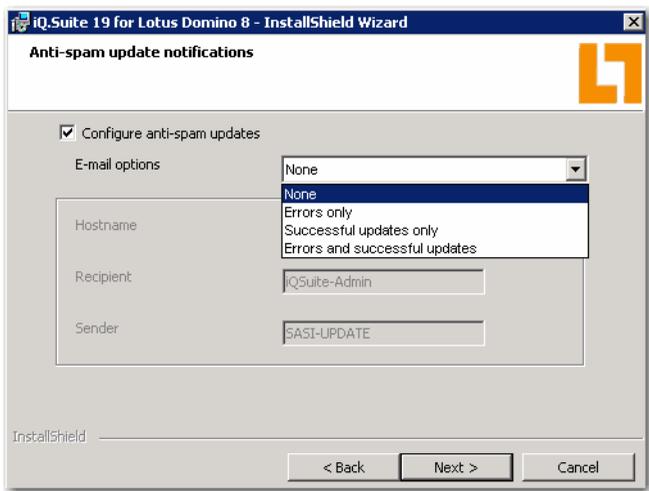
All of the settings can later be changed from the administration console (**Global** menu). For further information please refer to the iQ.Suite Administration Manual.

4.2.11 Set up SASI Analyzer / Update Service

(in 'Advanced' mode only)

The setup packages include a preconfigured SASI version, which can be used as soon as the installation is complete.

To be informed of the success or failure of the SASI update, you can set up automatic notifications. To be informed in both cases, keep the recommended option 'Errors and successful updates' in the **Email options** field. In the **Recipient** field, enter the administrator group that will receive the notifications, e.g. *iQ.Suite-Admin*. The setting in the **Recipient** field is entered as sender address in the notification.



When the iQ.Suite installation is complete, a synchronized download page of the GBS server is used to get the latest updates of all SASI files needed.

4.2.12 Configuring Virus Scanners

(in 'Advanced' mode only)

iQ.Suite supports various virus scanners listed in this dialog. Select the virus scanners that shall be used in the iQ.Suite. If additional settings are necessary, the subsequent dialog will contain further instructions.

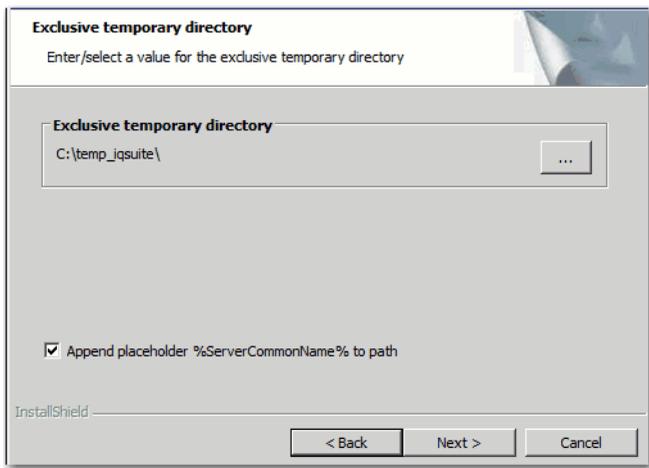
By selecting a virus scanner, the virus scanner document for this scanner is enabled in the iQ.Suite standard configuration.

4.2.13 Defining Working Directory for Temporary Files

Die iQ.Suite requires a working directory for temporary files to be exclusively used by iQ.Suite. Therefore, public temporary directories like %TEMP% are not appropriate.

The path to the working directory mentioned above must be specified during setup in the following cases:

- In the 'Standard' mode:
 - in case of an update installation, if the global parameter ToolKit_ExclusiveTempDir is not set or is disabled.
 - in case of a new installation.
- In the 'Advanced' mode



Default path: C:\temp_iqsuite\%ServerCommonName%

With the 'Append placeholder %ServerCommonName% to path' option enabled, the Common Name part of the short server name will be appended to the specified path². Example: C:\temp_iqsuite\server1

On partitioned servers, iQ.Suite must use a different working directory in each partition. By using the %ServerCommonName% placeholder, a unique directory will be assigned to each instance.

-
2. Siehe Beschreibung des Platzhalters %ServerCommonName% im iQ.Suite-Administrationshandbuch.

During setup, the specified path will be automatically added to the global parameter `ToolKit_ExclusiveTempDir` of the iQ.Suite configuration.

4.2.14 Summary

In the last setup step the components to be installed are summarized. Check these details and correct if required, by navigating with **BACK** on the desired set-up step. Click on **NEXT** and confirm the installation settings to start the iQ.Suite installation.

4.2.15 Installation Sequence

If they do not exist yet, the installation routine first creates the directories specified in the installation dialog. The setup program then copies all files to the corresponding directories, modifies various standard databases (*mail.box(es)*, *log.ntf/log.nsf*, *statrep?.ntf/statrep?.nsf*), changes various entries in the *notes.ini* and creates three log files. Refer to:

- a) [“Check notes.ini” on page 50](#)
- b) [“List of Files and Directories Under Windows” on page 91](#)
- c) [“Design Changes for the Installation” on page 87](#)

4.3 Installation Under IBM AIX, Linux and Oracle Solaris/SUN Solaris

This section describes how to install iQ.Suite under Domino on IBM AIX, Linux and Oracle Solaris/SUN Solaris platforms.

4.3.1 Before Starting the Installation Script

Before starting the installation script, extract the installation package to a directory to which the Domino user has Read and Execute permissions (recommended: the directory `/opt`, mandatory under AIX). The Domino server is started in the context of the Domino user:

1. Log on as user with Write access to the directory, e.g. as `<Root>`.
2. Copy the TAR file to `/opt`.
Example: `iQ.Suite-20.2.0.0.3930-Linux-Domino8-32bit.tar.gz`
3. Call the file with the complete filename of the TAR file using the command **`gzip -cd <tar file> | tar -xvf -`**.
Example:
`gzip -cd iQ.Suite-20.2.0.0.3930-Linux-Domino8-32bit.tar.gz | tar -xvf -`
4. The files are extracted as subdirectory under `/opt`, e.g. to

`/opt/iQ.Suite-20.2.0.0-d8132`.

This directory must not be deleted, not even after a successful installation, as it is used as template for further installations and contains executable iQ.Suite components. For a detailed description of the folder structure within this directory please refer to [“List of Files and Directories Under Unix” on page 93](#).

4.3.2 Starting the Installation Script

1. Make sure that all Domino servers are down and you are logged on as Domino user.

2. Start the installation script with the following command:

```
./install.sh <notes.ini directory>
```

<notes.ini directory> : Directory where the *notes.ini* is located (typically the Domino data directory).

e.g.: /home/domino/notesdata

The parameter can also be omitted when the script is called. In this case, it is prompted for interactively at a later stage.

3. The installation is run in English or German (depending on the value assigned to the environment variable \$LANG). If \$LANG has not been set, the language is selected on screen.
4. The setup is started. You can run the installation with the default values or change the options by setting different values in the dialog, e.g. 'prox' to change the proxy settings:
 - a) **notes.ini directory [ini]**:
Default: /home/domino/notesdata/notes.ini
 - b) **iQ.Suite program directory [exec]**:
Default: /home/domino/iqsuite
 - c) **iQ.Suite Data directory [data]**:
Default: <notesdata directory>/iqsuite
 - d) **Admin name [adm]**:
Name of the administrator in whose user context iQ.Suite is administered.

Default: iQ.Suite-Admin
 - e) **Proxy settings [prox]**:
Default: disabled.

In iQ.Suite configurations where spam analyzers or virus scanners require periodic spam pattern or virus pattern updates, a proxy server can

be very useful. Enter the applicable proxy setting (IP address, port, user and password). You can use both the name and the IP address of the proxy server.

f) **Installation mode:**

Default: Standard installation.

Select the type of installation for the configuration databases:

- ▷ **Standard installation [s]:** The databases provided in the setup package are installed.

The Domino databases are created from the database templates copied to the iQ.Suite data directory. For an update installation, a design refresh of the databases is performed using these templates. Then a program is started that preforms the installation of the databases and sets the necessary *notes.ini* parameters.

- ▷ **Installation in replicated environments [r]:** The installed databases are created as replicas on a server other than the master server.

You will be prompted to specify both the name of the master server and the path to the directory where the databases are located (under the Domino data directory).



If the DAOS function is enabled on a Domino server and Domino 8.5 or 8.5.1 is used, the installation program *tk_setup* could crash when attempting to access the database for the first time. This problem does not occur if the server is running during the installation of the database. Therefore, the server can be started during the setup, before the database installation.



If no values are set for the **WebClient Administrator** and the **exclusive working directory for temporary files**, you will be prompted to specify this information during iQ.Suite installation.

For further information, please refer to [“Set Administrator Group for iQ.Suite WebClient” on page 28](#) and [“Defining Working Directory for Temporary Files” on page 31](#).

5. Select 'j' to confirm the entries and start the installation. Select 'q' to cancel the installation.
6. The files installed in the iQ.Suite program directory represent symbolic links to the corresponding files in the base directory, e.g.
`/opt/iQSuite.../`. Exception: Files that can be modified by the Domino user, e.g. INI files.
7. All Domino databases (templates) are copied to the iQ.Suite data directory.



In certain system environments, it can happen that the *tk_setup* program freezes during the iQ.Suite installation when attempting to generate databases. In such a case, you can set the *notes.ini* parameter `Toolkit_DBG_Setup_Continue=1` to prevent a rollback and resume the installation. Please note that this could result in unpredictable error situations. Please contact our Support Team before modifying the *notes.ini*.

Starting the MailGrabber manually

The MailGrabber can be started manually using the following command:

load /opt/iQ.Suite-<version number>/tm_grab. This requires certain start scripts to be available in the Domino program directory. Use the *link_grabber.sh* to set the links accordingly:

1. Log on as <Root> or as user with Read and Execute permissions to the Domino program directory.
2. Start the shell script and specify the path to the Domino program directory:
`./link_grabber.sh <Domino program directory>`

4.3.3 Set up SASI Analyzer / Update Service (Linux Only)

The setup packages include a preconfigured SASI version, which can be used as soon as the installation is complete.

To efficiently use the SASI analyzer for spam protection, the spam patterns are updated periodically by the update service. To be informed of the success or failure of the SASI update, you can set up automatic notifications. To be informed in both cases, keep the recommended option 'Errors and successful updates' in the

Email options field. In the **Recipient** field, enter the administrator group that will receive the notifications, e.g. *iQ.Suite-Admin*. The setting in the **Recipient** field is entered as sender address in the notification.

When the iQ.Suite installation is complete, a synchronized download page of the GBS server is used to get the latest updates of all SASI files needed.

4.3.4 Verify File Access Rights

For all files in the shared iQ.Suite program directory (`/opt/iQ.Suite <version>`) `root` should be entered as user. The Domino user only requires Read and Execution rights to the files in this directory.

The owners and the group of the files copied to the iQ.Suite data directory (e.g. `/home/domino/notesdata/iqsuite`) must match those of the Domino user. The Domino user requires the following rights to the files:

- `<iQ.Suite directory> (rwx):`

```
*.nsf rw
*.dll rwx
res*.txt rw
toolkit.lic rw
```

- Under AIX only: `<iQ.Suite directory>/infozip (rwx):`

```
unzip rwx
```

4.3.5 Verify Database Access Rights

1. The server must have manager rights and the permission to delete documents.
2. The user type must be set to "unspecified".
3. The *IQSUITE-ADMIN* group (also refer to ["Access Rights in Configuration Databases" on page 85](#)) must be available in the Domino data directory of the server. This must be a **Mail** or **Multi-purpose** group.

The iQ.Suite installation is now complete. Start your Domino server and the Notes client. In order to administrate iQ.Suite, you need to create the *IQSUITE-ADMIN* group and specify its members. The next step is to set up the iQ.Suite jobs.

4.4 Silent Installation and Silent Uninstallation

The Silent Installation refers to an installation routine without user interaction at command line level. Typically, a silent Installation is used if you wish to install iQ.Suite on several servers and 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.

4.4.1 Silent Installation under Windows

Under Windows, Silent Installation and Silent Uninstallation is performed by using batch files that are included together with an appropriate documentation in the *Silent_Installation.zip* file. Download on www.gbs.com.

4.4.2 Silent Installation under Unix

Under Unix, the silent installation is performed by recording a previous installation. Please note that a silent uninstallation is not available so far.



As of iQ.Suite 14.1 the content structure of the control file used for silent installations is changed. To execute a silent installation from iQ.Suite Version < 14.1 to a Version \geq 14.1, the existing control file *iqsuite_silent_rec_dat* has to be supplemented manually before executing a silent installation. At the first entry position add the entry *silent* followed by a line break. With this changed control file future silent installations are executed. As an alternative, perform a standard update installation to a Version \geq 14.1, once. By this, a new control file that is used for future silent installations is created automatically.

To perform a silent installation proceed as follows:

1. Open a command line program.
2. Record the desired installation sequence using the following command:
`./install.sh rec`

3. During the installation, all dialog entries are stored in the *iqsuite_silent_rec_dat* file in the home directory (\$HOME) of the Domino user.
4. To run additional installations with the parameters recorded, simply call the following command:

```
./install.sh <$HOME/iqsuite_silent_rec_dat
```

4.5 Installation on Replicated Servers

The installation routine supports replicated environments under Windows and Unix. In a replicated environment, the installation program automatically creates replicas of the installed iQ.Suite configuration databases.

Requirements

The following requirements must be met before the installation is started:

-  All replicated servers have access/read rights to the databases of the server from where replication is performed (master server). Normally, this will be the server where the first iQ.Suite installation (standard) was run.
-  A network connection is available between both servers.
-  All servers involved have been started. Otherwise no replicas can be created.

During the installation, the setup program checks whether the installation is performed in a replicating multi-server environment (under Windows in the [Set up SASI Analyzer / Update Service](#) dialog). If that is the case, both the master server and the iQ.Suite data directory of the databases to be replicated are prompted for. The setup program does not install the databases from the installation directory, but creates replicas of the configuration databases on the master server specified. Then specify the server, which will be entered in the *notes.ini*.



If the replication of a database fails, this is logged in the installation log file (*iqsuite<Version>_setup_data.log*). This file can be viewed at the end of the installation or in later in the iQ.Suite data directory.



If the database on the master server cannot be opened (because either the server or the database does not exist), the installation is cancelled.

4.5.1 Installation Under Windows

For a non-partitioned installation proceed as follows:

1. Perform the preliminary steps needed to prepare the installation. Refer to [“Preliminary Steps” on page 19.](#)
2. Install iQ.Suite on the first Domino server (master server). You can run the installation in either ‘Standard’ or ‘Advanced’ mode. If you select the ‘Advanced’ mode, **do not** enter any settings for replicated environments.
3. If the installation is successful, restart the master server. For further Information on the installation please refer to [“Installation Routine Under Windows” on page 26.](#)
4. Make sure all replicating servers have access rights to the databases of the master server (from where replication takes place).
5. Make sure the master server has been started.
6. Install iQ.Suite on the first replicating server:
 - a) Select the installation mode ‘Advanced’.
 - b) In the CONFIGURATION DATABASES dialog click on the INSTALL REPLICATED ENVIRONMENT button.
 - c) In the next dialog, specify the name of the master server as well as the iQ.Suite data directory of the databases to be replicated. The installation process creates the databases of the iQ.Suite to be installed as replicas of the databases of the server specified.
 - d) Also refer to Sections [4.2.7](#) through [4.2.12 from Seite 28.](#)
7. To avoid replication conflicts with specific configuration documents, refresh the following views from the Notes client menu (ACTIONS -> ADMIN -> REFRESH SELECTED DOCS):
 - CRYPT -> MAIL JOBS
 - CRYPT -> SMIME CERTIFICATES -> PRIVATE CERTIFICATES
 - CRYPT -> UTILITIES -> ENGINES
8. After the replication of the configuration databases, iQ.Suite can be installed on further servers.
9. When complete, restart all servers involved.

10. Proceed as described under [“Follow-up Steps” on page 49](#).

4.5.2 Installation: IBM AIX, Linux and Oracle Solaris/SUN Solaris

For a non-partitioned installation or an installation with **different** Domino program directories, proceed as follows:

1. Perform the preliminary steps needed to prepare the installation. Refer to [“Preliminary Steps” on page 19](#).
2. Install iQ.Suite on the first Domino server (master server). You can run the installation in either ‘Standard’ or ‘Advanced’ mode. If you select the ‘Advanced’ mode, **do not** enter any settings for replicated environments.
3. If the installation is successful, restart the master server. For further Information on the installation please refer to [“Installation Under IBM AIX, Linux and Oracle Solaris/SUN Solaris” on page 34](#).
4. Make sure all replicating servers have access rights to the databases of the master server (from where replication takes place).
5. Install iQ.Suite on the first replicating server:
 - a) During the installation, select the ‘Advanced’ mode and the ‘Install replicated environment’ option.
 - b) You will be prompted to specify the master server and the corresponding iQ.Suite installation directory (iqsuite), e.g. *myServer/myOrganization, iqsuite*.
6. When complete, restart the server.
7. Repeat this procedure for all replicated servers involved.
8. Proceed as described under [“Follow-up Steps” on page 49](#).

4.6 Installation on Partitioned Servers

In most cases, databases on a partitioned server will be replicated. But a replicated environment is not necessarily required for an installation on partitioned servers.

The installation in replicated environments automatically creates replicas of the existing iQ.Suite configuration databases. These replicas can only be created if a running master server is specified at the time of installation. However, for the installation on a partitioned server, all servers have to be stopped on all partitions, as the basic iQ.Suite program files are written to the Domino program directory (which exists only once on a partitioned server). The files in this program directory must not be accessed during the installation.

iQ.Suite can be installed on up to 15 partitioned servers.

If the message 'The server is not reachable <server name>' appears although the server <server name> is available and running, check that the server name is unique and has been specified in canonical form.

4.6.1 Installation Under Windows

To install iQ.Suite in a partitioned environment, proceed as described under ["Installation Under Windows" on page 42](#). However, also do the following:

1. Before installing iQ.Suite on a partitioned server, make sure the first server (master server) is stopped.
2. For the installation on the replicating servers select the 'Advanced' mode.
3. Enable the 'Installation on partitioned servers' option.
4. Select one of the following options:
 - a) **Install databases without replication**
 - b) **Install databases as replicas**
 - c) **Install databases as replicas of databases located on another server:** Again, the databases are replicas of each other.



On a partitioned server, the same iQ.Suite version has to be installed on all partitions.

4.6.2 Installation: IBM AIX, Linux and Oracle Solaris/SUN Solaris

4.6.2.1 Same Domino program directory

To install iQ.Suite in a partitioned environment or for an installation with the **same** Domino program directory, proceed as described under ["Installation Under Windows" on page 42](#). However, additionally do the following:

1. Before installing iQ.Suite on a partitioned server, make sure the first server (master server) is stopped.
2. Select the replication mode 'Installation in replicated environments'.
3. You will be prompted to specify the master server and the corresponding iQ.Suite installation directory (iqsuite), e.g. *myServer/myOrganization, iqsuite*.
4. Then you will be prompted to start both Domino servers (the master server and the server where the installation takes place).
5. Confirm that the installation is to be continued.



On a partitioned server, the same iQ.Suite version has to be installed on all partitions.

If you wish to install an **additional server**, proceed as follows:

1. First stop all Domino servers.
2. Install iQ.Suite on the next (third) Domino server and select the replication mode 'Installation in replicated environments'.
3. You will be prompted to start the master server and the Domino server where the installation takes place.
4. Confirm that the installation is to be continued.
5. After installation is complete on all servers, start the servers that have not been started yet.

4.6.2.2 Sample Installation

Assumption: You have a partitioned server with four Domino servers.

Directory	Path
iQ.Suite data directory	/home/domino1/notesdata/iqsuite /home/domino2/notesdata/iqsuite /home/domino3/notesdata/iqsuite /home/domino4/notesdata/iqsuite
Unix user names	domino1, domino2, domino3, domino4
Domino program directory	Linux: /opt/lotus/notes/latest/linux Solaris: /opt/lotus/notes/latest/sunspa AIX: /opt/lotus/notes/latest/ibmpow
Domino data directories	/home/domino1/notesdata /home/domino2/notesdata /home/domino3/notesdata /home/domino4/notesdata
iQ.Suite program directory:	lotus/domino/iQSuite
iQ.Suite program directory (shared)	/opt/iQSuite-<version>

You want to install the program on the first, second and fourth server. To do so, proceed as follows:

1. Log on as domino1: **su domino1**
2. Install iQ.Suite on the first server by starting the installation script:
/opt/iQ.Suite-<version>/install.sh /home/domino1/notesdata



If you want to use another group in the Domino data directory as administrator for iQ.Suite (default: *IQSUITE-ADMIN*), you can specify so within the installation dialog.

The group must exist in the Domino address book (*names.nsf*). If it does not, please create the group after the installation. The group has to be created as **multi-purpose** group.

3. Check the installation settings on the system. To do so, please refer to the following instructions:
 - a) ["Check notes.ini" on page 50](#)
 - b) ["Verify File Access Rights" on page 38](#)
 - c) ["Verify Database Access Rights" on page 39](#)
4. Repeat all steps from Step 2 to install iQ.Suite on the second, third and the fourth server.
5. Start the Domino servers. The installation is now complete.

For the correct iQ.Suite configuration please refer to the iQ.Suite Administration Manual.



5 Follow-up Steps

5.1 Summary

1. Check the *notes.ini*. Refer to [“Check notes.ini” on page 50](#).
2. Start the Domino server.
3. Install and configure the external programs you want to use, e.g. virus scanners, decompression tools (unpackers) and analysis tools. Check their versions to make sure that the antivirus tools are compatible with iQ.Suite. The configuration of each of these programs is described in the corresponding **Comments** tab under UTILITIES -> VIRUS SCANNER.
4. Enter your license. To do so, copy the *Toolkit.lic* file to the iQ.Suite program directory¹.
5. Enter the following database as bookmark on the Desktop: *Entry for iQ.Suite (<iQ.Suite data directory>/nav.nsf)*. This database controls the mail and database configuration and is located on your Domino server in the iQ.Suite data directory.
6. 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.
7. Make sure the *g_trailer_advanced.nsf* database is available and can be opened. This is necessary even if iQ.Suite Trailer is not used.
8. If iQ.Suite is installed on multiple servers and you want to display statistics from all servers in the Cockpit of iQ.Suite WebClient, then all data of the statistics databases (*g_statistics.nsf*) from all iQ.Suite servers must be replicated to the WebClient server.
9. The iQ.Suite databases and templates are created in the ODS 48 format, by default. If you set the `Create_R85_Database=1` parameter in the *notes.ini* the databases *gmanual.nsf* und *g_update.nsf* are converted to the ODS 51 format. New created databases are created in the target format defined in the *notes.ini*.

1. Refer to [“Preliminary Steps” on page 19](#).

10. Gradually configure and enable the individual jobs. To take full advantage of iQ.Suite Watchdog, you must have installed and enabled an antivirus program. For further information on the configuration of jobs please refer to the iQ.Suite Administration Manual.
11. If you don't have assigned database access rights yet, please refer to ["Access Rights in Configuration Databases" on page 85](#) for further information on assigning rights.

5.2 Check notes.ini

Check that the following entry exists: `ServerKeyFileName=server.id`

Note: If the `ServerKeyFileName` entry is missing in the `notes.ini`, add the above line to the `notes.ini`. Make sure the server ID file (`server.id`) exists in the Notes data directory.

After the installation, the following entries must exist in the `notes.ini`:

■ `extmgr_addins`

Under Windows: `extmgr_addins=te_hook`

Under Unix: `extmgr_addins=<iQ.Suite program directory (shared)>/domino/libte_hook.so`

This entry ensures the integration of the Hook, which identifies new incoming emails and also monitors the iQ.Suite configuration databases in the iQ.Suite data directory.

■ `ServerTasks`

Under Windows: `ServerTasks=..., tm_grab, td_grab`

Under Unix: `ServerTasks=..., <iQ.Suite program directory (shared)>/tm_grab,<iQ.Suite program directory (shared)>td_grab`

This entry ensures the automatic start of the Grabbers.

`tm_grab` = MailGrabber (process emails).

`td_grab` = DatabaseGrabber (process databases)

- Under Unix only: `ToolKit_SharedExecDir=<iQ.Suite program directory (shared)>`
- `ToolKit_DataDir=<iQ.Suite directory>`
iQ.Suite data directory, relative to the Domino data directory
- `ToolKit_ExecDir=../<iQ.Suite directory>`
Absolute path to the iQ.Suite directory
- `ToolKit_Admin=IQSUITE-ADMIN` (or any other value specified during the installation)
iQ.Suite administrator. A valid email address from the name and 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 Domino log (*log.nsf*)
(1 - 9, 1 = few details, 9 = every detail logged).

The log level can be set separately for each job in the Mail and Database-Grabber databases.

Default: Log level 0 (value from *notes.ini*).
- `ToolKit_MailIntercept=YES`
If emails are to be processed, set this parameter to 'Yes'. For pure database servers, it should be set to 'No'.
- `ToolKit_MgrabThreads=5/ToolKit_DgrabThreads=5`
Sets number of worker threads simultaneously started and processed by the MailGrabber or DatabaseGrabber. Where required, adjust the number of worker threads according to your system environment. Please note that an excessive number of concurrent threads may lead to performance problems. We recommend to increase the value gradually while monitoring the server load and performance.

Under **Unix**: Check that, in the *notes.ini*, the line break code is consistent: CR LF ; LF ; CR (*CR: carriage return; LF: line feed*). If not encoded consistently, line breaks can cause problems when reading the file. Inconsistencies can occur, for instance, when the *notes.ini* is exchanged between different operating systems.

5.3 Optional Features

Optionally, you have the possibility to use iQ.Mastering and iQ.Clustering. Refer to [“iQ.Mastering \(Generic Mastering\)” on page 61](#) or [“iQ.Clustering” on page 67](#).

For a web-based access to some iQ.Suite components, you can use iQ.Suite WebClient. Refer to [“Installation of iQ.Suite WebClient” on page 81](#).



6 Optional Features

6.1 iQ.Suite WebClient

For a web-based access to some iQ.Suite components, you can use iQ.Suite WebClient (short 'WebClient').

iQ.Suite WebClient is available as a separate feature in the iQ.Suite Setup. The WebClient requires a separate license. For further information, please contact the GBS Sales Team.

iQ.Suite WebClient consists of the following modules:

 **Quarantines:**

- Administrator Quarantine / User Quarantine: Access emails in regular quarantines.
- Reviewer Quarantine: Access emails in Review quarantines.

The displayed quarantined emails and the possible actions on quarantined emails depend on the user rights.

For emails in quarantines, the user must have the role [Admin], [Deliver] or [Resend]; for the emails in Review databases, a reviewer role is required.

By default, file attachments can be downloaded from emails of the Administrator Quarantine and of the Review Quarantine.

-  **User Lists:** Display the own Blacklist/Whitelist entries. Entries can be added and existing entries can be deleted.
-  **Cockpit:** In the Cockpit, statistics can be viewed in Statistic Widgets, e.g.:
 - Number of processed emails per job
 - Number of emails per quarantine
 - Found viruses
-  **Trailer:** Trailer documents, images, file attachments and Notes Data Sources can be created, processed or deleted.

- **Trailer Preview:** Before sending her email, the user can view how her email would look like after processing by the Trailer jobs. The trailer valid for the respective recipient is displayed in the email preview.
- **DLP:** View the collected data and calculated Baselines for the DLP Anomaly Detection.
- **Roles & Rights:** To set access rights to quarantine databases and White-lists/Blacklists, use the procedure that applies for the iQ.Suite User Portal. To allow access to the Review database, the DLP Anomaly databases and the Trailer Advanced database, access rights must be set as well. For further information on the rights/roles concept, please refer to the iQ.Suite Administration Manual¹.

6.1.1 System Requirements

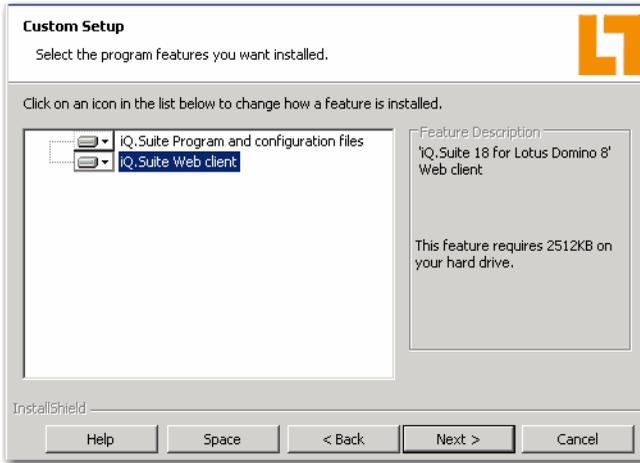
- IBM Domino Server as of Version 9.0
- IBM Domino Server 8.5.3: If this Domino version is used, the UpgradePack 1 has to be installed in addition: *w32n_upgradepack.exe* or *w64n_upgradepack.exe*. For detailed information on the installation, refer to [IBM-Website](#).
- To avoid an 'OutOfMemory' crash, the parameter `HTTPJVMMaxHeapSize` in the *notes.ini* must have a value $\geq 1024M$. `1024M` is the default value on Domino Server ≥ 9 . After an **update from Domino 8.x to 9.x**, the value on Domino 8.x (default: `64M`) must be increased to `1024M`.
- Supported web browsers:
 - Google Chrome
 - Mozilla Firefox
 - Microsoft Edge
 - Internet Explorer

We support the latest version of each mentioned web browser.

1. Refer to section "Rights/Roles Concept in "iQ.Suite User Portal", "iQ.Suite DLP" and "Using iQ.Suite WebClient for Trailer Utilities".

6.1.2 Installation

Run the iQ.Suite Setup and select in the Setup dialog the 'iQ.Suite WebClient' feature:



During the installation, the JAR files required by iQ.Suite WebClient are automatically created in the following path:

```
<Domino-Data-Verzeichnis>/domino/workspace/applications/  
eclipse/plugins/
```



In case of an update installation, already existing plug-ins are deleted from this directory. This directory should always contain only the plug-ins corresponding to the iQ.Suite Version.

6.1.3 Configuration

Perform the steps described in the following chapters step by step.

6.1.3.1 Website Settings in the Domino Directory

Enabling the Domino Access Service

The Domino Server must be configured in such way that the Domino Data Service is supported². To do so, enable the Domino Access Service

de.group.das.service:



■ **Method 1:** If you are using an Internet Site document, proceed as follows:

1. Open the desired 'Internet Site' document (type: Web) for the server:
DOMINO DIRECTORY -> CONFIGURATION -> WEB -> INTERNET SITES -> <SITE>.
2. In the **Configurations** tab under DOMINO ACCESS SERVICES -> FIELD: ENABLED SERVICES, enter the service **de.group.das.service**.
3. Save the document.

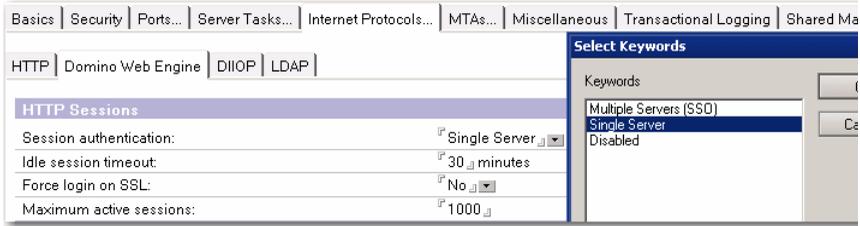
■ **Method 2:** If you are not using an Internet Site document, proceed as follows:

1. Open the server document:
DOMINO DIRECTORY -> CONFIGURATION -> WEB -> WEB CONFIGURATIONS -> <SERVER>.
2. In the server document under INTERNET PROTOCOLS, open the **Domino Web Engine** tab.
3. Under DOMINO ACCESS SERVICES -> FIELD: ENABLED SERVICES, enter the service **de.group.das.service**.

2. For detailed information on the Domino Data Service, refer to the [IBM documentation](#).

Enabling Session Authentication

In the **Domino Web Engine** tab under HTTP SESSIONS, enable the session authentication (**Session Authentication** field). With this setting, WebClient users need to login only once per session. If this option is disabled, the login won't work.



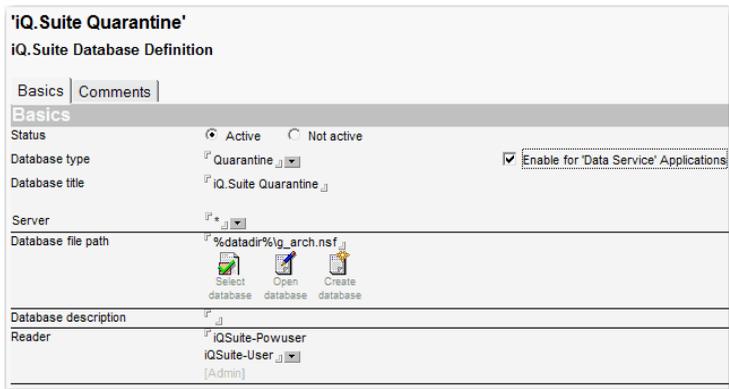
4. Save the document.

6.1.3.2 Configuration in the iQ.Suite

Database Definition

For the quarantined emails, the DLP Review emails and the data of the DLP Anomaly Detection to be displayed in the WebClient, open the iQ.Suite administration console and enable the option **Enable for 'Data Service' Applications** in the respective database definition: GLOBAL -> DATABASE DEFINITIONS -> <DATABASE DEFINITION> (e.g. *g_review.nsf*).

Example with the Quarantine database:



The field **Reader** controls the users' access rights to the emails or data of the respective database (e.g. to the quarantined emails). All persons listed in this field can view the emails or data of the respective database in the WebClient.

For further information on the configuration of a database definition, please refer to the iQ.Suite Administration Manual.

DEFAULT - Create index folders in quarantine

We recommend you to use the iQ.Suite Action Database Job **DEFAULT - Create index folders in quarantine**. Use this job to create index directories in the quarantine database in order to allow accessing the quarantined emails faster.

For further information on this job and its configuration, please refer to the iQ.Suite Administration Manual.

6.1.3.3 Restarting the HTTP Task

For the changed configuration to be used, if necessary, stop the HTTP task and restart it.

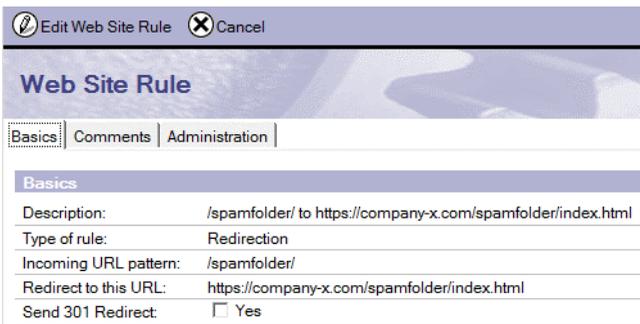
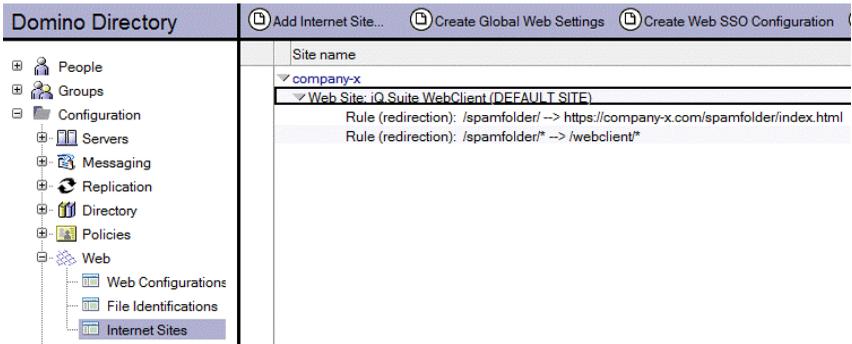
6.1.3.4 Login to the iQ.Suite WebClient

Once the configuration has been loaded successfully, the users entered in the Domino Directory can login to the WebClient with their username and Internet password.

URL to the iQ.Suite WebClient: *http(s)://<hostname>/webclient/index.html*

If you want the WebClient being accessible through another URL (e.g. *https://<hostname>/spamfolder/index.html*), configure corresponding website redirection rules:

CONFIGURATION -> WEB -> INTERNET SITES -> <INTERNET SITE> -> MENU BUTTON:
 EDIT WEB SITE -> CREATE RULE:



In the **Type of rule** field, select 'Redirection'.

For further information on creating a website rule, please refer to the documentation of IBM Domino.

6.2 iQ.Mastering (Generic Mastering)

6.2.1 Technical Background

iQ.Mastering allows to use third-party products (e.g. for spam protection) along with iQ.Suite. Besides 'Symantec Mail Security for Domino (Windows)' and 'McAfee Security for Email Servers', a wide range of additional products can be combined with iQ.Suite.

To this end, iQ.Suite uses the **tk_hook**, a utility that processes documents placed into the mail.box by the third-party product. As a general rule, the documents are first processed by the third-party product and then by iQ.Suite.



The server tasks of the third-party product have to be started through the `ServerTask` parameter in the `notes.ini`. Starting a third-party product using a program document is not possible.



Please make sure the iQ.Suite Grabber tasks are ignored by the third-party product.

The only possible processing order is third-party product -> iQ.Suite, not vice-versa. In other words, attachments are first checked for viruses and then processed by iQ.Suite. More specifically, this means that PGP-encrypted emails are first scanned by the third-party product and then decrypted by iQ.Suite Crypt. To perform a virus scan after decrypting, it is recommended to use iQ.Suite Watchdog along with a virus scanner supported by Watchdog.



iQ.Mastering requires a separate license and cannot be run along with iQ.Clustering. Any changes made to the third-party product may result in the existing installation becoming inoperable.

Procedure

To configure iQ.Mastering after having installed iQ.Suite, adjust the following parameters in the `notes.ini`:

Under Windows:

- NSF_HOOKS=... , tk_hook
- EXTMGR_ADDINS=... , te_hook

Under Unix:

- NSF_HOOKS=<Path to tk_hook>
- EXTMGR_ADDINS=<Path to te_hook>

Under Windows and Unix:

- ToolKit_Mastering_Tasks=<server task of third-party product>

Enter the name of the tasks used by the third-party product for email processing. Multiple entries have to be separated by comma (,). task names are not case-sensitive.

As a general rule, enter the hooks **after** the hooks of the third-party product.

Sample configuration for TrendMicro Scanmail

- NSF_HOOKS=tk_hook
- EXTMGR_ADDINS=**SMDext**, te_hook
- ToolKit_Mastering_Tasks=**SMDreal**
- Adjust TrendMicro to ignore tm_grab. The following entry is set in the notes.ini: SMDSkipTaskList=... , TM_GRAB

At tg_hook Windows (Runtime 2008 is required):

- EXTMGR_ADDINS=tg_hook, SMDext, te_hook
- ToolKit_Secure=ATTDMP, COMPACT, DESIGN, FIXUP, REPORT, STAT-LOG, UPDALL

At tg_hook Unix:

- EXTMGR_ADDINS=<iqsuite-install-path>/domino/libtg_hook.so, SMDext, <iqsuite-install-path>/domino/libte_hook.so
- ToolKit_Secure=ATTDMP, COMPACT, DESIGN, FIXUP, REPORT, STAT-LOG, UPDALL

Sample configuration for Kaspersky Anti-Virus 2014

- NSF_HOOKS=nKavMailHook, tk_hook
- EXTMGR_ADDINS=te_hook

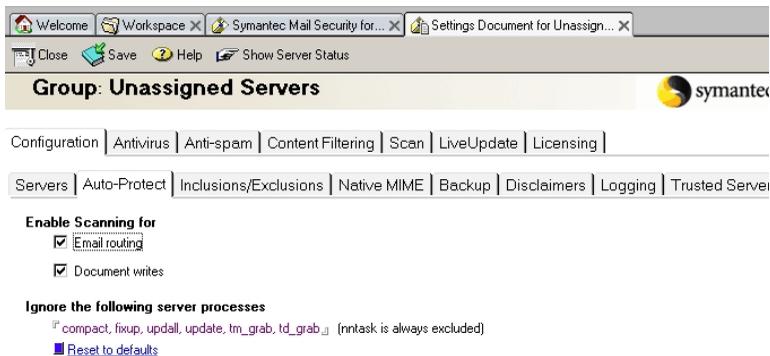
■ ToolKit_Mastering_Tasks=KavMailMonitor, KavDbScanner

6.2.2 Symantec Mail Security for Domino (Parallel Use)

'Symantec Mail Security for Domino (Windows)' can be used simultaneously with iQ.Suite.

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

1. In the *notes.ini*, add the following parameters:
 - Windows (new creation): NSF_HOOKS= tk_hook
 - Sun Solaris: NSF_HOOKS= tk_savhook, tk_hook
 - Linux, AIX: NSF_HOOKS= savhook, tk_hook
2. Use a license file that contains the entry GRPNAV.
3. In the Symantec configuration in the **Auto-Protect** tab, enter the two Grabber tasks under **Ignore the following server processes**:



Glossary	
SAV	Symantec Anti virus
NTASK	Server add-in task of SAV for Domino
NNHOOK	Hook of SAV for Domino
ExtensionmanagerAddin	"Hook" entered under EXTMGR_ADDIN= in the <i>notes.ini</i> → see te_hook
Database Hook	"Hook" entered under NSF_HOOKS= in the <i>notes.ini</i>

6.2.3 McAfee Security for Email Servers (Parallel Use: Windows)

Under Windows, 'McAfee Security for Email Servers' can be used simultaneously with iQ.Suite.

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

1. In the *notes.ini*, add the following parameter:
`NSF_HOOKS= tk_hook`
2. Check the entry `ExtMgr_Addins`:
 - For Version 5.2.1: `ExtMgr_Addins=GSDem, te_hook`
 - For Version 5.3: `ExtMgr_Addins=McAfeeEm, te_hook`
3. Under **Exclude specified applications** in the McAfee Groupshield **Server settings**, insert `NTM_GRAB` and `NTD_GRAB`.
4. Use a license file that contains the entry `GRPGSD`.

Glossary	
GSD	McAfee Groupshield
GSDConfig, GSDOAScan, GSDOD-Scan, GSDUpdate, GSDReport	Server add-in tasks of GSD for Domino
GSDem	Hook of GSD for Domino
ExtensionmanagerAddin	"Hook" entered under <code>EXTMGR_ADDIN=.</code> in the <i>notes.ini</i> → see te_hook
Database Hook	"Hook" entered under <code>NSF_HOOKS=</code> in the <i>notes.ini</i>

6.3 iQ.Clustering

6.3.1 Benefits and Fields of Application

iQ.Clustering is an iQ.Suite feature that is enabled on a Domino server after having been installed and licensed.

iQ.Clustering provides:

- High availability
- Fail-safety
- Load Balancing
- Distributed Computing

All of these features are described in detail in this chapter.

A cluster managed by iQ.Clustering may comprise 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 a replicated configuration on all servers involved. The network connection between clustered servers must provide sufficiently high data transfer rates, e.g. such as provided by LAN connections.



If running [iQ.Mastering \(Generic Mastering\)](#), iQ.Clustering is not possible!

6.3.1.1 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 applications.

The servers involved under iQ.Clustering monitor each other, in particular the email traffic in each mail.box, as well as the processing actions taken by iQ.Suite. Should iQ.Suite be unavailable on one server (e.g. for maintenance reasons), the other servers in the iQ.Suite cluster take over the tasks of that server.

High-availability example

If running a backup data center for your Domino servers, iQ.Clustering can be used to ensure that the cluster computer in the backup data 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.

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.

6.3.1.2 Load Balancing

iQ.Clustering allows to react to dynamic system load requirements by distributing tasks between systems according to their current load. The iQ.Clustering system on the less loaded server checks and processes the emails on the heavily loaded server.

Load balancing example

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

6.3.1.3 Distributed Computing

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

It is thus possible, for instance, to check emails on a remote Domino server (e.g. for viruses) via the network whenever this Domino server is running on an operating system for which iQ.Suite or any required third-party products (e.g. virus scanners or PGP) are not available. *te_hook* and/or *te_mailhook* must be available for the operating system in question.



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

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 email 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 email is simply marked for processing by the Hook and the MailGrabber installed on the computer running iQ.Suite then processes the email as required.

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

6.3.2 Requirements for iQ.Clustering

To use iQ.Clustering most efficiently and with all functions, observe the following:

- iQ.Clustering requires a separate license.
- Under normal circumstances, two servers will be sufficient to cover standard tasks (fail-safety and load balancing).
- The new "Reserve" and "Process" method is always used, even if checking the own mail.box only.
- Appropriate access rights to the mail.box(es). The servers need Manager rights (including deletion) to access each other's mail.box.
- The system time settings on the servers must not differ significantly.

6.3.2.1 Email Checking Sequence

The description below explains the working principle:

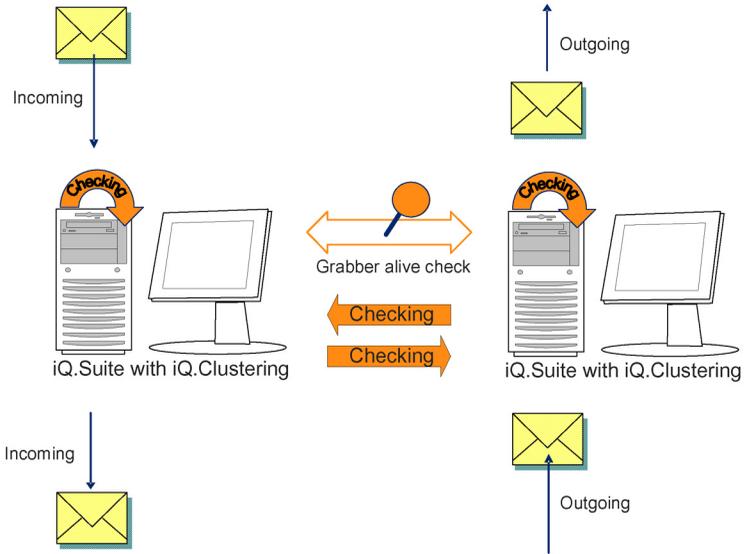
1. The MailGrabber checks the mail.box(es) to be monitored for new documents.
2. The MailGrabber attempts to reserve any documents found -> new status in the *dispatched for <server name> view*.
3. The working threads only process documents that have been successfully reserved by the server (`$TKCheckServer` field).
4. If a reserved document is not processed within 15 minutes, it is reset.
5. If there are any reserved documents when the MailGrabber is stopped or started, the reservation is removed.

6.3.2.2 Grabber Checking

The description below explains the working principle:

1. On the servers to be monitored, the MailGrabber checks the mail.box / mail1.box for a profile document.
2. This profile document contains the last action (with date/time) performed by the Grabber on the monitored server.
3. 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).
4. With no profile document found, the last status read is the current status.
5. If several Grabbers monitor the same server, there is a risk of false alarms when the cycles happen to interfere with each other.

The figure below illustrates the working principle for mutual monitoring of mailboxes on an Internet gateway by two Windows PCs. The MailGrabbers monitor each other:



6.3.2.3 Installation Requirements

The basic installation requirements for iQ.Clustering are described under [“System Requirements” on page 7](#).

In addition, the following requirements must be met:

- A fast network connection is available.
- A virus scanner is available (for iQ.Suite Watchdog).

6.3.3 Installation Principle

Example: This example features two Windows 2008 servers mutually monitoring each other. To perform the installation, proceed as follows:

1. Run a standard installation on both servers (both Windows 2008), whether replicated or not.
2. On both servers, create the configuration documents under IQ.SUITE -> GLOBAL -> GLOBAL PARAMETERS (see example above) with the following settings:

 **On Server 1:**

Server = <server 1>

Server for email checking [=ToolKit_WatchServer] = <server 2>

If MailGrabber is to be monitored:

Server for Grabber checking [=ToolKit_MonitorServer] =<server 2>

 **On Server 2:**

Server = <server 2>

Server for email checking [=ToolKit_WatchServer] = <server 1>

If MailGrabber is to be monitored:

Server for Grabber checking [=ToolKit_MonitorServer] =<server 1>

Server 1 will now periodically check the mail.box on server 2 for emails that have not yet been processed by server 2 – and vice versa.

To install an additional server 3, proceed as follows:

1. Run a standard iQ.Suite installation on that server.
2. On **Server 3**, under IQ.SUITE -> GLOBAL -> GLOBAL PARAMETERS, create a second iQ.Clustering configuration document with the following settings:

 **On Server 3:**

Server =<server 3>

Server for email checking [=ToolKit_WatchServer] = <server 1>

If MailGrabber is to be monitored:

Server for Grabber checking [=ToolKit_MonitorServer] =<server 1>

3. On **Server 3**, under GLOBAL PARAMETERS, create a second iQ.Clustering configuration document with the following settings:

On Server 3:

Server =<server 3>

Server for email checking [=Toolkit_WatchServer] = <server 2>

If MailGrabber is to be monitored:

Server for Grabber checking [=Toolkit_MonitorServer] =<server 2>

4. On **Server 2**, under GLOBAL PARAMETERS, create a further iQ.Clustering configuration document with the following settings:

On Server 2:

Server =<server 2>

Server for email checking [=Toolkit_WatchServer] = <server 3>

If MailGrabber is to be monitored:

Server for Grabber checking [=Toolkit_MonitorServer] =<server 3>

5. On **Server 1**, under GLOBAL PARAMETERS, create a further iQ.Clustering configuration document with the following settings:

On Server 1:

Server =<server 1> Server for email checking

[=Toolkit_WatchServer] = <server 3>

If MailGrabber is to be monitored:

Server for Grabber checking [=Toolkit_MonitorServer] =<server 3>



Both the iQ.Suite Quarantine and the iQ.Suite configuration should be replicated. If the grabbers are not supposed to mutually monitor each other, the iQ.Clustering configuration documents (Toolkit_MonitorServer) are not needed.



With mutual Grabber monitoring, enter an asterisk (*) in the the job configuration documents in MISC TAB -> SERVER FIELD.

Reason: The Server field in the job configuration documents relates to the execution of a job by a Grabber and not to the processing of emails/documents on a server. This means, for instance, that Job A on Server X also processes the emails in the mail.box(es) on Server Y, but the same job on Server Y no emails at all because only Server X is specified in the Job A configuration document (replicated configuration). Therefore, the Grabber on Server Y will not start this job at all, since the job is not valid for Server Y.

6.3.4 iQ.Clustering Configuration

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

1. Open the configuration document for iQ.Clustering from the standard configuration: GLOBAL -> GLOBAL PARAMETERS -> iQ.CLUSTERING.

Do not enter an asterisk (*) in any of the following fields:

Basics	Comments
Basics	
Name	iQ.Clustering
Status	<input type="radio"/> Aktiv <input checked="" type="radio"/> Nicht aktiv
Server	WVP_CO02/SRV/WVP/GROUP/De
Server für E-Mail-Prüfung	WVP_CO01/SRV/WVP/GROUP/De
Server für Grabber-Prüfung	WVP_CO01/SRV/WVP/GROUP/De

- **Server:** Enter the name of your Domino servers. This is the server for which this iQ.Clustering configuration applies.
 - **Server for mailbox checking:** Enter the name of the server whose mail.boxes are to be additionally monitored. The own mail.boxes are monitored automatically.
 - **Server for grabber checking:** Enter the name of the server whose Mail-Grabber is to be monitored.
2. Repeat this procedure for each server to be monitored.

3. Configure iQ.Suite as desired. When configuring mail jobs in a context of monitored server operation, please also set the following fields in the **Misc** tab:

- **Server exceptions:** This field is used to set that a job does not apply to specific servers. This allows to exclude specific servers with iQ.Suite installed and replicas of the databases. Enter the servers to be excluded from the job in this field, each one on a separate line.
- **Monitored server:** This field is used for iQ.Clustering-specific purposes. Use this field to set that a job applies to specific documents on specific monitored servers only. This allows to run a job on a specific server although the iQ.Suite cluster includes a server that monitors several servers. Enter the servers on which this job is to be run in this field. For each entry, use a separate line. This setting facilitates the assignment between specific jobs and clients for computing center operation.



Please note that any notification emails generated within iQ.Clustering are not to be checked again by a member server of the iQ.Suite cluster. To exclude processing by another server in the job configuration, use the *IsModuleNotificationMail* rule in the **Basics** tab. This will prevent both servers from generating notification emails and sending them back and forth (risk of overloading the mail.box).

7 Update



All descriptions referring to iQ.Suite updates are valid for iQ.Suite upgrades as well.

7.1 Preparing the Update

Before starting the update installation, observe the following:

- The update requires a valid license for the new iQ.Suite version. Please contact our License Service for details.
- Be sure to read the Release Notes file, which may contain important additional information.
- Log on to your system as administrator.
- Stop the Domino server.
- By default, during the installation process, the Domino databases and templates installed are signed with the ID of the current Domino server. To prevent this, set the following global parameter in the *notes.ini* of the Domino server before installing iQ.Suite: `ToolKit_DBG_Setup_Nosign_DBS=1`
- Close all unnecessary applications, in particular iQ.Suite, the Domino server and your Notes client. Otherwise, some files may not be installed properly if they are being used by other programs.
- Create a backup of the iQ.Suite program directory (under Unix: e.g. `/home/domino/notesdata/iqsuite`). Make sure this backup is located outside of the Domino data directory (`/home/domino/notesdata`).
- If your virus scanners support 'Realtime' or 'On-Access-Scan', disable these features for the iQ.Suite data directory.
- By default, when opening the iQ.Suite Entry database (*nav.nsf*), the IMPORT STANDARD CONFIGURATION dialog is displayed¹. To suppress this, set the following parameter in the *notes.ini* before updating iQ.Suite:
`ToolKit_DBG_Setup_Suppress_Importdialog=1`.

1. For further information on importing the standard configuration, please refer to the iQ.Suite Administration Manual.

- If using external programs, please read the section [“Using External Programs” on page 24](#) before starting the setup.



The update will renew the database design. The user rights of the old databases are preserved.

7.2 Update Routine

7.2.1 Update Routine: Windows

1. Prepare the update. Refer to [“Preparing the Update” on page 73](#).

2. Run the following installation package file:

iQ.Suite-<version>-Windows-Domino<version>-<32/64>bit.exe

Start the setup in a local drive or a connected network drive. Starting the installation from a UNC path (`\\computer\directory`) is not possible.

3. Agree with the license terms.

4. Select the desired installation setup mode:

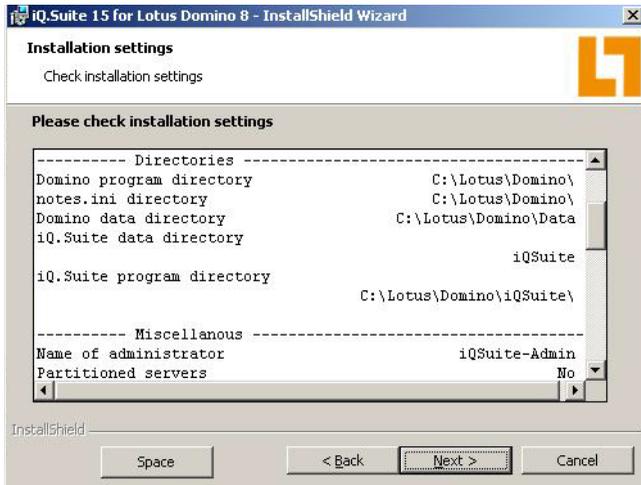
- a) 'Standard' (recommended)

In this mode, the current iQ.Suite settings (e.g. paths, administrator email address, etc.) are preset and not checked during the update.

- b) 'Advanced'

In this mode, the current iQ.Suite settings are also preset, but checked individually. You can select, if current configuration databases are to be updated or if the iQ.Suite is to be installed new by using the databases of the iQ.Suite standard configuration. Select this mode for special update settings. The settings are the same as for the initial installation. Refer to [“Installation Routine Under Windows” on page 26](#).

5. In the final summary, check and confirm the settings to be used for the update.



a) Settings correct:

▷ Confirm with NEXT -> INSTALL to start the update.

b) Settings incorrect:

▷ Click on BACK.

▷ Select the 'Advanced' mode to correct the settings as required. The update is started.

6. Restart your system.

7. Proceed as described under ["Follow-up Steps" on page 77](#).

If working in a replicated or partitioned environment, please refer to ["Update on Replicated Servers" on page 80](#) or ["Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris" on page 82](#).

7.2.2 Update Routine: IBM AIX, Linux and Oracle Solaris/SUN Solaris

1. Prepare the update. Refer to [“Preparing the Update” on page 73](#).
2. Log on as Domino user and install the desired iQ.Suite version. Installation can not be performed as <Root>. Refer to [“Installation Under IBM AIX, Linux and Oracle Solaris/SUN Solaris” on page 34](#).
3. Proceed as described under [“Follow-up Steps” on page 77](#).



If you are using the iQ.Suite Bridge module, you may have to make a few manual adjustments.

Example: A Bridge job is configured to use the %DataDirABS%\bridge directory. The %DataDirABS% variable refers to the (original) Domino data directory /home/domino/notesdata/grptools.

As described above, the /home/domino/notesdata/grptools/bridge directory was moved to the iQ.Suite program directory /home/domino/iqsuite/bridge, rather than to the iQ.Suite data directory /home/domino/notesdata/iqsuite/bridge.

In such a situation, either move the subdirectory ../bridge to the iQ.Suite data directory, or replace the variable %DataDirABS% with %ExecDir% in the configuration.



If you are using the *ntk_hook*, enter this in the *notes.ini* with the complete path.

If working in a replicated or partitioned environment, please refer to [“Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris” on page 81](#) or [“Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris” on page 82](#).

7.3 Follow-up Steps

After having completed the update setup, proceed as follows:

- For using the SAVAPI3 engine, a number of configuration settings need to be adjusted following an iQ.Suite update:

- Under Windows: If you have an adjusted update configuration, replace the following entries under `<execdir>\savapi\update\` in the files `avupdate-savapi-mirror.conf` and `avupdate-savapi-update.conf` after the update:

`product-file=/idx/savapi3lib-win32-en.idx` with

`product-file=/idx/savapilib-win32-en.idx` and

`update-modules-list=VDF,ENGINE` with

`update-modules-list=VDF,AVE2,SAVAPI3.`

Otherwise match the following files:

`<execdir>\savapi\update\avupdate-savapi-update.conf` with

`<execdir>\savapi\update\avupdate-savapi-update.conf.new` and

`<execdir>\savapi\update\avupdate-savapi-mirror.conf` with

`<execdir>\savapi\update\avupdate-savapi-update.conf.new.`

- Under Unix: If you have an adjusted update configuration, replace the following entry under `<execdir>/savapi/update/avupdate-scanner.conf` after the update:

`product-file=/idx/savapi3lib-linux_glibc22-en.idx` with

`product-file=/idx/savapilib-linux_glibc22-en.idx.`

Otherwise match the file

`<execdir>/savapi/update/avupdate-scanner.conf` with

`<execdir>/savapi/update/avupdate-scanner.conf.new.`



If you use the 'Avira Update Manager', select in the program the 'Avira Savapi Library' product.

- Check whether all iQ.Suite jobs are executed as configured.

- Under Windows only: If, during the update, you have specified separate directories for data (NSF files) and programs, you may have to adjust the existing configuration accordingly.
- As of Q.Suite Version 18.1, you should no longer use the Eclipse administration console (Widget). The modules iQ.Suite Convert and iQ.Suite Trailer can now be entirely administrated in the Notes Client. Refer to [“Important Notes on Configuration after an Update” on page 79](#).
- Check any existing proxy server settings.
- Replace any existing domain rules with address rules.
- Make sure the iQ.Suite jobs are linked to the associated rule through the Notes ID. Otherwise, they are linked through the rule name and displayed in the standard configuration in green font.
- An existing *tk_unpak.dll* file will be replaced with *tk_unpack2.dll* by the update.
- If updating to an iQ.Suite Version ≥ 13.2 , you should adjust the S/MIME Engine documents used accordingly:
 - In the **Settings** tab, insert the parameter `%STANDARD_SMIME_PARAMETERS%` in all fields from 'Sign with company certificate' to 'Verify signature'. Please note that the parameter must be included **before** any additional parameters.
 - Remove all duplicate parameters. For further Informationen on S/MIME parameters please refer to the description for the S/MIME engine in the Online Help.
 - To overwrite a default value of the parameter, insert the desired parameter with different values **after** `%STANDARD_SMIME_PARAMETERS%`.
Exception: The parameters `--certificates` and `--recipients` cannot be overwritten.

Please note that, depending on the S/MIME mode selected in the Crypt job, the `%STANDARD_SMIME_PARAMETERS%` parameter will be expanded in a different way. For further Information please refer to the Online Help.

7.4 Important Notes on Configuration after an Update

7.4.1 Trailer Advanced

After a successful update to **iQ.Suite ≥ 18.1**, the Trailer images and attachments, which were administrated in the Eclipse administration console (Widget) until iQ.Suite 18.0, are now available in the Notes administration console.



After you have updated successfully, remove the Widget to avoid inconsistencies. **As of iQ.Suite 18.1, edit all Trailer documents only in the Notes Client!**

After the update, the Trailer images and attachments created in the Widget need to be reassigned to categories in the Notes administration console. This is necessary because the old assignments could not be transferred.

After the update, the first time you access documents under TRAILER -> UTILITIES or PDFCRYPT -> UTILITIES, a warning is displayed:



This warning is displayed once per day when a document of the Utilities is accessed the first time.

7.4.2 Other Adjustments



Please read in the Release Notes the section “Important Notes on Configuration” carefully. After an update, refreshing documents can be necessary.

7.5 Update on Replicated Servers

Basically, the iQ.Suite update process in a replicated environment is the same as for a normal iQ.Suite update. Refer to [“Update Routine” on page 74](#) or [“Update Routine: IBM AIX, Linux and Oracle Solaris/SUN Solaris” on page 76](#).

7.5.1 Update: Windows

1. Prepare the update. Refer to [“Preparing the Update” on page 73](#).
2. Make sure all replicated servers have access rights to the databases of the master server. Typically, this will be the server where the first iQ.Suite installation (standard) was performed.
3. Perform an update on the first server. Select the same mode as for the initial installation. Please note that in ‘Standard’ mode, your existing configuration of the replicated environment will be preserved.
4. The Domino servers need not to be stopped during the update.
5. To avoid replication conflicts, we recommend to first install iQ.Suite on a server and update all documents in the following views (Notes client menu under ACTIONS -> ADMIN -> REFRESH SELECTED DOCS):
 - MAIL JOBS
 - S/MIME CERTIFICATES -> LOCAL DATABASE -> PERSONAL CERTIFICATES
 - UTILITIES -> ENGINES

Once the configuration databases (*g_wdog.nsf*, *gm_grab.nsf*, *g_cert.nsf*) have been replicated, iQ.Suite can be installed on further servers.
6. Before updating the replicated servers, make sure the first server (already updated) has been started.
7. Then perform an update on all other Domino servers, again using the same mode as for the initial installation.
8. Check the summary of your settings and proceed with the update.
9. When complete, restart all servers involved.
10. Proceed as described under [“Follow-up Steps” on page 77](#).

7.5.2 Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris

Note: The program files and iQ.Suite databases can be stored in different directories.

1. Prepare the update. Refer to [“Preparing the Update” on page 73](#).
2. Log on as Domino user to the master server and install the desired iQ.Suite version. Installation must not be performed as <Root>. Refer to [“Installation Under IBM AIX, Linux and Oracle Solaris/SUN Solaris” on page 34](#). Select the ‘Standard’ mode if you wish to preserve the existing configurations of the replicated environment. The Domino servers involved need not be stopped during the update.
3. If the `/home/domino/notesdata/grptools` directory still contains files, use the installation dialog to move them to the new directories.
4. After having completed the update, make sure the master server is started and then run the update installation on the replicated server:
 - a) Make sure the replicated server has access rights to the databases of the master server.
 - b) Select ‘Standard’ mode.
 - c) Check the summary of your settings.
5. When complete, restart the server.
6. Proceed in the same way for all other servers involved.
7. Proceed as described under [“Follow-up Steps” on page 77](#).

7.6 Update on Partitioned Servers



On a partitioned server, you need to install the same iQ.Suite version on all partitions.

7.6.1 Update: Windows

If you plan to replicate the databases on a partitioned server, perform an update on all servers involved.

Basically, the iQ.Suite update process in a partitioned environment is the same as for a replicated environment. Refer to [“Update on Replicated Servers” on page 80](#). Exceptions:

- **Before** starting the update of the **master server**, be sure to stop all partitioned servers (“slaves”) involved.
- **After** having updated the **master server**, start the first partitioned server.
- Stop the master server and perform the update.

7.6.2 Update: IBM AIX, Linux and Oracle Solaris/SUN Solaris

Basically, the iQ.Suite update process in a partitioned environment is the same as for a replicated environment. Refer to [“Update on Replicated Servers” on page 80](#). Exceptions:

- **Before** starting the update of the **master server**, be sure to stop all partitioned servers (“slaves”) involved.
- **After** having updated the **master server**, stop the master server and perform the update on all partitioned servers.
- **After** having updated the **partitioned servers**, restart all partitioned servers as well as the master server.

8 Uninstallation of iQ.Suite



Uninstallation of the iQ.Suite does not remove the iQ.Suite Widgets from the Notes client (Eclipse client). For further information on removing widgets, please refer to the IBM documentations.

8.1 Uninstall: Windows

To uninstall iQ.Suite under Windows, proceed as follows:

1. Under START -> CONTROL PANEL-> SOFTWARE select the iQ.Suite program and click on INSTALL/REMOVE.
2. Follow the instructions displayed. Then use the **Refresh Design** command to reset the productive databases *log.nsf* and *mail.box* to their original state.
3. Where required, delete the iQ.Suite databases and database templates in the iQ.Suite data directory, as they may not have been removed by the uninstall program.

If iQ.Suite is uninstalled, the log entries are written to the *iqsuite<version>_setup_script.log* file.



In order to delete all iQ.Suite related data and directories after iQ.Suite uninstallation, select the CHANGE button instead of INSTALL/REMOVE under START -> CONTROL PANEL-> SOFTWARE. With this, a deletion option can be enabled at the end of the uninstallation. The same option is available, when you use the setup file *iQ.Suite-<Version number>-<Platform>-<Server>-<32/64>bit.exe* for iQ.Suite uninstallation.

8.2 Uninstall: IBM AIX, Linux and Oracle Solaris/SUN Solaris

To uninstall iQ.Suite under Unix, proceed as follows:

1. Stop the Domino servers.
2. Log on as Domino user and navigate to the iQ.Suite program directory (shared).

Example: **cd /opt/iQ.Suite-<version>**

3. Start the *uninstall.sh* shell script from the command line with the argument 'Domino data directory'.

Example: **./uninstall.sh /home/domino/notesdata**

4. If it is the last partition with an iQ.Suite installation, you can delete the iQ.Suite program directory (shared).

9 Appendix

9.1 Access Rights in Configuration Databases

Domino controls the access to databases by means of ACLs. These lists are used to assign database access rights to users or user groups. For further Information please refer to the IBM documentations.

9.1.1 Using Predefined iQ.Suite Groups

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

IQSUITE-ADMIN	iQ.Suite administrator or the administrator group specified during the installation. Rights: Change configuration documents, database design modifications and rights management; also refer to the <i>notes.ini</i> .
IQSUITE-SRV	Server group
IQSUITE-USER	Standard users
IQSUITE-POWUSER	Experienced users

These groups are already included in the ACL with appropriate access rights. All you have to do is to create the corresponding groups in the address book.

During the installation, the server where iQ.Suite has been installed, is entered in all relevant database ACLs with Manager access rights.

For further Information on the roles for the User Portal please refer to the iQ.Suite Administration Manual, chapter "iQ.Suite User Portal".

9.1.2 Using Your Own Groups

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

Server

Servers must have at least Editor rights to the iQ.Suite databases and must be included in all database roles. For iQ.Clustering the servers need Manager rights to the mail.box(es).

Administrator/Manager

Administrators should have Author or Manager rights. Individual databases have additional Admin roles to allow for more granular rights.

End user

To make efficient use of the iQ.Suite User Portal, the users need appropriate rights to the user database (*g_user.nsf*).

As the iQ.Suite User Portal takes the views from different databases, the rights have to be assigned individually for each database and must match the roles assigned in the *g_user.nsf* database. For a list of roles please refer to the iQ.Suite Administration Manual, chapter "iQ.Suite User Portal".

Administrator notifications

The recipients of administrator notifications are set in the *notes.ini* 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*.



The `%ADMIN%` variable in the configuration documents is replaced with the entry under `Toolkit_Admin`.

9.2 Design Changes for the Installation

9.2.1 Design Elements: Log Database

By default, the sequence of operations of each module is logged (default) in the Notes log database (*g_log.nsf*) of the server. To be able to use this database, the `ToolKit_LogDB` parameter in the *notes.ini* is automatically set to the path of the log database.



If not set, the *log.nsf* Domino database is used for logging. We recommend to use the *g_log.nsf* supplied for logging and not to change this parameter.

To visualize this information, the design of the Domino Log or the design template is extended during the installation. The following *g_log.ntf* design elements are added to the *g_log.nsf* during installation:

Element	Name	Purpose
Screen	ToolKit LogPage	Displays the entries
View	Grabber Logby Date	Sorts the entries by date
View	Grabber Logby Task	Sorts the entries by process
Frame-set	Entry	Required for own database only.
View	Grabber Log\ Error by Date	As before, but for documents with ErrCount > 0 only
Agent	(Export Grabber Log)	File dialog for export to Excel spreadsheets
Agent	(Server)	Used in Frameset <i>Entry</i> for server change

In iQ.Suite, you can also create a new **Flags for Log Database** document for the buffer delay: GLOBAL -> GLOBAL PARAMETERS -> NEW: GENERAL GLOBAL PARAMETER.

Alternatively, you can also set this parameter directly in the *notes.ini* through the `Toolkit_LogDB_Flags=[max. seconds], [max. lines]` entry. Set the maximum delay in seconds or the maximum number of lines in the buffer. Whenever one of these values is reached, the external log database is updated. Without the `Toolkit_LogDB` setting, this entry is ignored. Both flags support values higher than '1'. A '0' value is considered as an error and replaced with the default configuration '60,30'.

It is also possible to set one flag only, e.g.:

```
Toolkit_LogDB_Flags=123 (max. 123 seconds) or
```

```
Toolkit_LogDB_Flags=, 234 (max. 234 lines)
```

9.2.2 Design Elements: Statrp.nsf

During the iQ.Suite installation, a number of *Statrp5.ntf* design elements are added to your *Statrp.nsf*. These changes do not have any effect on the Domino server and are primarily for display purposes.

The following design elements are added during installation:

Element	Name	Purpose
Screen (Form)	GROUP Tools Report (GTSTAT)	Displays the mail statistics as well as the elements of the two subforms.
Subform	GROUP Tools Statistics (Mail)	Elements written by the MailGrabber.
Subform	GROUP Tools Statistics (Database)	Elements written by the DatabaseGrabber.
View	1. Statistics Reports \ 99. Grabber	Collection of elements created during the installation of iQ.Suite.

9.2.3 Design Elements: mail.box

For the MailGrabber's use, a few changes to the mail.box and the corresponding template (*mailbox.ntf*) of the server are made during the iQ.Suite installation.

These changes do not have any effect on the Domino server and are primarily for display purposes.

The following design elements are added during installation:

Element	Name	Purpose
View	MailGrabber\ Mail Status	Displays the scanning and routing status.
Frame-set	Entry	Required for own database only.
Macro	Reprocess Mails	Changes the status of an undeliverable email so that it is processed again by the MailGrabber.
Macro	Release "Undeliverable" Mails	Changes the status of an undeliverable email so that it is delivered by the router without further processing by the MailGrabber.
Macro	Release Mails	Changes the status of any email so that it is delivered by the router without further processing by the MailGrabber.
Screen	TkMemo	Displays the email and additional status information; no storage option.

9.2.4 Support for Multiple mail.boxes

It is possible to define multiple mail.boxes to be used by the router.

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

For iQ.Suite to work correctly after having changed the number of mail.boxes, it must be ensured that only those mail.boxes are located in the server directory that are processed by the router.



Restart the server after having completed the changes. The following mail.boxes may exist when

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

Any other mail.boxes must be deleted from the Domino data directory.



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

1. Click on CONFIGURATION TAB -> SERVER -> CONFIGURATIONS to display the name of the server.
2. Double-click on the server name to open the configuration settings for the server.
3. In the **Router/SMTP** tab enter the number of boxes you wish to use in the **Number of mail.boxes** field.
4. Stop the Domino server.
5. Switch to the directory of your *mail.box* file.
Default: C:\lotus\domino\data
6. 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.

9.3 List of Files and Directories Under Windows

During the iQ.Suite installation, various files are copied to different directories:

9.3.1 Log Files

The different LOG files created are used to store detailed information on the installation. All files are located in the %TEMP% directory.

These files are:

- *iqsuite<version>_setup_installer.log*
(or, for silent installation, the specified Installer log file)
- *iqsuite<version>_setup_data.log*
- *iqsuite<version>_setup_script.log*

9.3.2 iQ.Suite Data Directory

For instance under

C:\Program Files\IBM\Lotus\Domino\data\iQSuite

File	Description
<i>*.nsf</i>	Help / configuration database, e.g. <i>C:\Program Files\IBM\Lotus\Domino\data\iQSuite\g_wdog.nsf</i>
<i>*.ntf</i>	Templates for configuration databases, e.g. <i>C:\Program Files\IBM\Lotus\Domino\data\iQSuite\g_wdog.ntf</i>

9.3.3 iQ.Suite Program Directory

For instance under C:\Program Files\IBM\Lotus\Domino\iQSuite

File	Description
<i>toolkit.lic</i>	iQ.Suite license file
<i>de\res*.txt</i> <i>en\res*.txt</i>	Messages
<i>ntk_*.dll</i> <i>tk_*.dll</i>	Interfaces used to call third-party components
<i>soap.ntk_*.dll</i> <i>soap.tk_*.dll</i>	Sandbox interface to call third-party components
<i>soap.ntk_*.dll.defaults.ini</i> <i>soap.ntk_*.dll.ini</i>	Configuration files for sandboxes

The iQ.Suite program directory contains subdirectories with further third-party components, the log directory `TECHNICAL_SUPPORT` and program interfaces.

9.3.4 Domino program directory

For instance under C:\Program Files\IBM\Lotus\Domino

File	Description
<i>nte_hook.dll</i> <i>ntk_hook.dll</i>	Extension Manager add-ins for database monitoring NSF Hooks for iQ.Mastering
<i>ntm_grab.exe</i>	MailGrabber base module
<i>ntd_grab.exe</i>	DatabaseGrabber base module
<i>nt_setup.exe</i>	Installation module

9.4 List of Files and Directories Under Unix

9.4.1 Log Files

During the installation, the *iqsuite<version number>_install.log* file is created in the iQ.Suite program directory of the Domino user.

9.4.2 iQ.Suite Data Directory

For instance under `/home/domino/notesdata/iqsuite/`

File	Description
<i>*.nsf</i>	Help / configuration database, e.g. <i>/home/domino/notesdata/iqsuite/g_wdog.nsf</i>
<i>*.ntf</i>	Templates for configuration databases, <i>/home/domino/notesdata/iqsuite/g_wdog.ntf</i>

9.4.3 iQ.Suite Program Directory

For instance under `/home/domino/iqsuite/`

File	Description
<i>toolkit.lic</i>	iQ.Suite license file
<i>devres*.txt</i> <i>envres*.txt</i>	Messages
<i>tk_*.dll</i>	Interfaces used to call third-party components
<i>soap.tk_*.dll</i>	Sandbox interface for third-party components
<i>soap.tk_*.dll.defaults.ini</i> <i>soap.tk_*.dll.ini</i>	Configuration files for sandboxes

The iQ.Suite program directory contains subdirectories with further third-party components, the log directory `TECHNICAL_SUPPORT` and program interfaces.

9.4.4 Domino Program Directory

For instance under `/opt/lotus8/lotus/notes/80000/linux`

No iQ.Suite files have to be copied to this directory. Optionally, you can use the `link_grabber.sh` script to store the `tm_grab` and `td_grab` scripts in this directory. Refer to [“Starting the Installation Script” on page 35](#).

9.4.5 Common iQ.Suite Program Directory

As a rule, the installation under Unix requires a common iQ.Suite program directory (share). In partitioned environments all Domino partitions can use the same iQ.Suite program directory.



All Domino users require Read rights to this common program directory, but Write rights should not be granted.

After having copied and unpacked the TAR file, the files are extracted as subdirectory under `/opt`. The subdirectory is structured as follows:

iQ.Suite-<iQ.Suite version>-d<Domino version><platform letter: l (Linux)/ s (Solaris)/ x (AIX)><bit architecture: 32/64>

This directory contains the following components:

- Shell scripts for installation and uninstallation
- Start-up scripts for the Grabber
- `domino` subdirectory
 - Contains files directly referenced from the `notes.ini` or started by start-up scripts (Hooks and Grabbers)
- `bin` subdirectory (basically corresponds to the previously used directory `grptools/bin`)
 - Contains permanent files, which need to be set in `PATH` or `LD_LIBRARY_PATH/ LIBPATH`
- `lib` subdirectory
 - Contains the libraries required by the Hooks
- `data` subdirectory

- Contains the template for `ToolKit_DataDir` (iQ.Suite data directories)
- Contains NSF and NTF files previously stored in the `grptools` directory
- `exec` subdirectory
 - Contains the template for `ToolKit_ExecDir` (iQ.Suite program directory)
 - Contains most of the components of the former `grptools` directory. Exception: NSF and NTF files, Grabbers and the files in the `bin` directory.
 - Most of the files in the iQ.Suite program directories are installed as symbolic links to this directory.

File	Description
<i>libte_hook.a</i> <i>libte_hook.so</i>	Extension Manager add-ins for database monitoring for AIX for Linux and Solaris
<i>libtk_hook.a</i> <i>libtk_hook.so</i>	NSF Hooks for iQ.Mastering for AIX for Linux and Solaris
<i>libtk_shared.so</i> <i>libtk_shared.a</i>	Library shared by Extension Manager add-ins, NSF Hooks and Grabbers
<i>tm_grab</i>	'MailGrabber' base module
<i>td_grab</i>	'DatabaseGrabber' base module