

KerioMailServer⁶™

Administrator's Guide

Kerio Technologies

© 1997-2006 Kerio Technologies. All rights reserved.

Release Date: January 19, 2006

This guide provides detailed description on *Kerio MailServer*, version 6.1.3. Any additional modifications and up-dates reserved. Detailed description on the *Kerio WebMail* user interface is provided in a standalone document called *Kerio MailServer 6.1, Kerio WebMail*.

For current product version, check <http://www.kerio.com/kms>.

Contents

1	Quick Checklist	10
2	Introduction	13
2.1	Kerio MailServer 6.1	13
3	Installation	18
3.1	System requirements	18
3.2	Conflicting software	19
3.3	Installation	19
3.4	Configuration Wizard	26
3.5	Upgrade and Uninstallation	31
4	Product Registration and Licensing	33
4.1	Product registration at the website	33
4.2	Registration with the administration console	33
4.3	License information and import of the license key	38
4.4	Licensing policy	41
5	Kerio MailServer Components	42
5.1	Kerio MailServer Monitor	42
6	Kerio MailServer Administration	45
6.1	Administration Window	45
6.2	View Settings	48
7	Services	50
7.1	Service Parameter Settings	51
7.2	Important Notes	54
8	Domains	56
8.1	Definition of Domains	56
8.2	General	58
8.3	Aliases	60
8.4	Footers	61
8.5	Forwarding	61
8.6	Setting of Directory Services	63
8.7	Advanced	68

8.8	Webmail Logo	70
9	Internet Connection	71
9.1	Internet Connection	71
9.2	Sending High Priority Messages	73
10	Scheduling	74
10.1	Setting Up the Scheduler	74
10.2	Optimal Scheduling	76
11	SSL certificate	77
11.1	Kerio MailServer Certificate	77
12	Kerio WebMail parameters	82
12.1	Skins	82
12.2	Logo	82
12.3	Language	83
13	Tools	85
13.1	IP Address Groups	85
13.2	Time Intervals	86
13.3	Setting Remote Administration	89
14	User accounts	91
14.1	Administrator account	92
14.2	Creating a user account	92
14.3	Editing User Account	104
14.4	Editing multiple users	105
14.5	Removing user accounts	106
14.6	Search for:	107
14.7	Restoring deleted items	107
14.8	Statistics	107
14.9	Import Users	108
14.10	Publish users in address book	112
14.11	User Account Templates	113
15	User Groups	116
15.1	Creating a User Group	116

16	Sending and Receiving Mail	121
16.1	Mail Delivery over the Internet	121
16.2	Relay server hostname	124
16.3	Aliases	131
16.4	remote POP3 mailboxes	134
16.5	Receiving Email Using ETRN Command	140
16.6	Advanced Options	141
17	Antispam	155
17.1	Spam Rating tab	155
17.2	Blacklists tab	159
17.3	Email policy records check	162
17.4	Action	165
17.5	Spam repellent	167
18	Antivirus Control of Email And Attachment Filtering	169
18.1	Integrated McAfee Anti-Virus	170
18.2	Choosing a Module for an Antivirus Program	171
18.3	Server responses to detection of a virus or a forbidden attachment	172
18.4	Supported antivirus programs	173
18.5	Filtering Email Attachments	174
19	Email backup	177
19.1	Archiving	177
19.2	Backup of user folders	180
20	LDAP server	187
20.1	LDAP server configuration	187
20.2	Configuring Email Clients	187
21	Mailing lists	192
21.1	User Classification	192
21.2	Creating a Mailing List	193
21.3	Posting rules	197
21.4	Moderators and Members	199
21.5	Mailing list archiving	200
21.6	Server Reports	201
21.7	How to use Mailing Lists	201

22	Status Information	204
22.1	Messages in queue	204
22.2	Message queue processing	206
22.3	Active Connections	208
22.4	Traffic Charts	210
22.5	Statistics	212
23	Logs	214
23.1	Log settings	214
23.2	Config	217
23.3	Mail	218
23.4	Security	221
23.5	Warning	223
23.6	Error	223
23.7	Spam	223
23.8	Debug	225
23.9	Performance Monitor (under Windows)	228
24	Kerio MailServer Environment	229
24.1	Configuring Email Clients	229
24.2	Web browsers	231
24.3	Firewall	232
25	Deployment Examples	234
25.1	Leased Line	234
25.2	Dial-up Line + Domain Mailbox	236
25.3	Dial-up Line + ETRN	237
25.4	A company with a filial	239
25.5	Setting up the backup mail server	243
26	Troubleshooting in Kerio MailServer	246
26.1	Reindexing mail folders	246
26.2	Configuration Backup and Transfer	248
27	KMS Web Administration	250
27.1	Web browsers	250
27.2	Setting access rights to the web interface	251
27.3	Settings that enable web administration	251
27.4	Users logged in	252
27.5	Page header	252
27.6	Welcome page	253
27.7	User accounts	254

27.8	User groups	261
27.9	Aliases	267
28	Kerio Active Directory Extensions	270
28.1	Installation of Active Directory Extensions	271
28.2	Active Directory	272
28.3	User Account Definition	272
28.4	Group Definition	275
29	Kerio Open Directory Extensions	276
29.1	Kerio Open Directory Extensions installation	276
29.2	Apple Open Directory	277
29.3	User accounts mapping in Kerio MailServer	277
29.4	Authentication using the apple.map configuration file	277
30	Kerberos Authentication	280
30.1	Kerio MailServer on Windows	281
30.2	Kerio MailServer on Linux	284
30.3	Kerio MailServer on Mac OS	288
30.4	Starting Open Directory and Kerberos authentication settings	298
31	Kerio Outlook Connector	301
31.1	Upgrade the Kerio Outlook Connector	302
31.2	Installation and configuration without the migration tool	302
31.3	Installation and profile creation using the migration tool	312
31.4	Installation and configuration of MS Outlook 2000	313
31.5	Spam/Not Spam buttons displaying problems	314
31.6	Private events	314
31.7	Messages signed in MS Outlook	314
31.8	Kerio Outlook Connector and Kerio Synchronization Plug-in	315
31.9	Sharing and Mapping in MS Outlook	316
31.10	Public and archive folders	319
31.11	Rules for incoming messages	320
31.12	Spam filter	327
31.13	Searching contacts via the MAPI interface	330
31.14	Error in settings of contact folders used as address books	331
31.15	Contacts forwarding	332
31.16	User login data	333
31.17	Usage of the Free/Busy server	333

32	Kerio Synchronization Plug-in	336
32.1	Installation	338
32.2	Synchronization	338
33	MS Entourage support	343
33.1	Initial settings	344
33.2	Connection to the LDAP server	357
33.3	Usage of the Free/Busy server	359
33.4	Delegating folders and their connection in MS Entourage 2004	360
33.5	Secure communication of Kerio MailServer with MS Entourage	366
34	Apple iCal Support	374
34.1	Setting Apple iCal in Mac OS X 10.3	374
34.2	Setting Apple iCal in Mac OS X 10.4	378
35	Apple Address Book Support	382
35.1	Apple Address Book for Mac OS X 10.2 (Jaguar)	382
35.2	Apple Address Book for Mac OS X 10.3 (Panther) and 10.4 (Tiger)	383
36	Support for Apple Mail 10.4	388
36.1	Exchange account in Apple Mail	389
36.2	IMAP account in Apple Mail	389
37	Kerio Exchange Migration Tool	390
37.1	About Kerio Outlook Connector	392
37.2	Kerio Exchange Migration Tool Installation	392
37.3	Migration requirements	393
37.4	Recommendations	394
37.5	Migration with full support for UNICODE	395
37.6	Migration Wizard	397
37.7	Kerio Outlook Connector automatic installation	406
37.8	Creating profiles at user computers	408
37.9	Log	409
38	Technical support	413
38.1	Contacts	413
A	Used open-source libraries	415

Glossary of terms	416
Index	420

Chapter 1

Quick Checklist

This chapter gives you a basic step-by-step guide to quickly set up *Kerio MailServer* so that it can function as a mail server for your company immediately. All that you need is basic knowledge of TCP/IP and of the principles of Internet mail protocols, and some information from your ISP: the type of connection and the way email is delivered for your domain.

If you are unsure about any element of *Kerio MailServer*, simply look up an appropriate chapter in the manual. If you do not know how and/or where email is delivered for your domain, please contact your ISP.

1. Install *Kerio MailServer* and make the required settings using the configuration wizard (create the primary domain as well as username and password for the user Admin). Log into the *Kerio Administration Console* program.

By default, *Kerio MailServer* is installed to the following directories:

- *Mac OS X*
`/usr/local/kerio/mailserver`
- *Linux*
`/opt/kerio/mailserver`
- *MS Windows*
`C:\Program Files\Kerio\MailServer`

2. In *Configuration/Services*, set up the services you are planning to use. If you would like to run a web server on the same machine, for example, stop the *HTTP / Secure HTTP* service, change its port or reserve one IP address for the service's default port. For more details refer to chapter [7.1](#).
3. Create local domains (*Configuration/Domains*). The primary domain must be created first (configuration guide). After you create other domains, you can set any of them as primary. If you are not sure as to which domain should be primary, choose the domain that contains the most users. Do not forget to fill in the DNS name of the SMTP server. For more information see chapter [8](#).

-
4. Create user accounts for individual domains (*Domain Settings/Users*). Account names should correspond with the users' primary email addresses. We do not recommend using special characters for name definitions. You can also import users from external sources. See chapter 14 for more details.
 5. If necessary, create groups (to create group addresses, for instance) (*Domain Settings/Groups*) and assign users to them. For more information refer to chapter 15.
 6. Define aliases for users and user groups if necessary (*Domain Settings/Aliases*). More details can be found in chapter 16.3.
 7. In *Configuration/Internet Connection*, set the type of Internet connection: *Online* for leased line, cable modems and ADSLs and *Offline* for any kind of dial-up connection. For more information go to chapter 9.
 8. If the modem is installed on the same computer as *Kerio MailServer*, choose the correct RAS line. Again, see chapter 9 for more information.
 9. If the Internet connection type is *Offline*, set Scheduling (*Configuration/Scheduling*). If the type is *Online*, only set scheduling if you would like to retrieve email from remote POP3 accounts or receive email using ETRN command. More information can be found in chapter 10.
 10. If you would like to retrieve email from remote POP3 accounts or domain accounts, create corresponding accounts in *Configuration/POP3 Download*. If email from these accounts is to be sorted into local accounts, also define the sorting rules. Refer to chapter 16.4.
 11. If email for certain domains should be received from a secondary server using ETRN command, define corresponding accounts in *Configuration/ETRN Download*. See chapter 16.5 for details.
 12. Set up antivirus control in *Configuration/Antivirus*. Choose a plug-in module for the antivirus program that you have installed. Choose the action that should be performed in case an infected attachment is found. You can also choose to filter certain types of attachments (e.g. executables). Refer to chapter 18 for more information.
 13. If *Kerio MailServer* is running behind a firewall, map an appropriate ports. See chapter 24.3 for more information.
 14. If the SMTP server is accessible from the Internet, set up Anti-spam protection (*Configuration/Spam Filter*), to prevent misuse of the mail server for sending spam email. You can also protect yourself from receiving such email from other servers. For more information, see chapter 17.

15. Set up email backup/archiving of mail folders and configuration files if necessary. See chapter [19.2](#) for details.
16. Create a certificate for the mail server for secure communication, or ask a commercial certification authority to do this. For more information, see chapter [11](#).

Chapter 2

Introduction

2.1 Kerio MailServer 6.1

Kerio MailServer 6.1 is designed as a “secure mail server accessible from anywhere”. Here is a brief list of its main functions and features.

Relay server hostname

A full-featured SMTP server which enables to use multiple independent local domains, to create virtual addresses (aliases), to receive email via ETRN, etc. Outgoing email can be sent either directly to target domains (according to MX records in DNS) or via a parent SMTP server (e.g. the ISP’s SMTP server).

POP3 Server

POP3 (Post Office Protocol version 3) is an Internet protocol that allows a POP3 client to download mail from a server. It is suitable for clients who don’t have a permanent connection to the Internet.

Unlike Internet Message Access Protocol (IMAP), POP3 does not allow users to manipulate messages at the server. Mail is simply downloaded to the client where messages are managed locally. POP3 provides access only to a user’s *INBOX*; it does not support access to public folders.

IMAP server

IMAP4 (Internet Message Access Protocol version 4) is an Internet messaging protocol that enables a client to access email on a server rather than downloading it to the user’s computer. This architecture allows the user to access his/her mail from multiple locations (messages downloaded to a local computer would not be available from other locations).

It is possible under certain conditions to access the email account using both IMAP and POP3 protocols.

NNTP server

(Network News Transfer Protocol) is a protocol used to transfer news messages and display public folders for users. A NNTP server stores archives of all newsgroup posts.

Web Interface (Kerio WebMail)

The built-in HTTP server allows remote access to the user account. It allows reading and writing of email messages, events and tasks, folder management and modifications of personal settings. No email client software needs to be installed and no settings are needed. All the user needs is a web browser. For information about *Kerio WebMail*, refer to separate user manual.

WAPmail

Allows access to email using a cellular telephone. For more information about settings and using of *Kerio WebMail*, see the *Kerio WebMail* user manual.

Personal and Public Contact Lists

In *Kerio MailServer 6.1* you can manage private and public contact lists (users' data, such as email addresses). Users can access their mail and contact lists via any supported email client or *Kerio WebMail* interface. *Kerio MailServer* also supports for *Free/Busy* server — a special type of public calendar where free/busy time of all users can be viewed.

Personal and Shared Calendar, Tasks

In *Kerio MailServer 6.0*, users can store the private and public calendar and tasks on the server. This information is managed using the *Kerio WebMail* interface and the *MS Outlook* application with *Kerio Outlook Connector* (see chapter 31).

LDAP server

The secure LDAP service allows remote clients to search public and private contacts. Most email client programs support this feature of LDAP.

Administration of user accounts, groups and aliases via web interface

Kerio MailServer version 6.1 and higher supports user administration via web interface. This way, clients of ISPs can access user mailbox, groups and aliases settings from within their domains.

Collecting mail from remote accounts

The mail server can automatically retrieve email from one or more accounts located at external servers (e.g. domain account at the ISP) and deliver this mail to local accounts or sort it according to defined rules.

Secure communication channels

All *Kerio MailServer* services offer standard non-secure connections and SSL-encrypted secured connections. It is also possible to send messages via a secured connection, provided that the destination server supports this feature.

Antivirus control

All incoming mail can be checked for viruses. Several actions can be taken if a virus is detected: the infected attachment can be removed, the mail can be sent back to the sender, a notification can be sent, the message can be sent to the system

administrator, etc. Antivirus control is performed by an external antivirus program (such as AVG, NOD32, etc.). In addition, certain types of attachments can be filtered (by file extension — e.g. exe, com, vbs, etc. or by MIME type — e.g. application/x-msdownload) regardless of whether or not they are infected by a virus.

Anti-spam protection

The mail server can be protected from spam email misuse. Messages can be detected and filtered by the *SpamEliminator* antispam filter, Bayesian filter, SMTP spam-server databases, checking “e-mail policy” records and/or by your own spam rules which can be set in the *SpamEliminator* section.

Archiving

Kerio MailServer can make backup copies of all email (or just sent email) either locally or to a remote server.

User folders and configuration files backup

Kerio MailServer can create backups of user folders (the store directory) as well as mailserver configuration files in predefined time intervals.

Filtering and notification

Each user can define a range of actions to be performed after a message is received (moving a message to a specific folder, filtering, cellular phone notification, automated reply...). Actions can be applied to all messages or selectively by the sender’s or recipient’s address, subject, etc.

Scheduler

The server administrator has absolute control over whether messages are to be sent immediately or at given times or time intervals. This makes it possible to minimize connection costs (with dial-up lines).

Mailing lists

Any number of mailing lists can be created within each local domain. List members can be defined by the server administrator, approved by a moderator or they can be added automatically through email. Each list can have one or more moderators who control user participation, message deliveries, etc.

In *Kerio MailServer*, parameters for mailing list archiving can be set.

Active Directory and Open Directory support

Kerio MailServer provides full support for *Microsoft Active Directory* as well as *Apple Open Directory*. It is not necessary to import user accounts into the internal database. To add or remove user account/group use the *Active Directory* or *Open Directory* system tool.

Kerio Outlook Connector

Kerio Outlook Connector is an extension to *MS Outlook* that uses an open MAPI interface. It is used for communication between *Kerio MailServer* and *MS Outlook*. It enables storing of various folder types (such as email messages, contacts, calendars and tasks) at the server. It is also possible to share and map folders, as well as set up message sorting rules.

IMAP and POP3 account synchronization in MS Outlook

Kerio Synchronization Plug-in is an add-on to *MS Outlook* that provides basic groupware features using IMAP and POP3 accounts. *Kerio Synchronization Plug-in* is available also in offline mode, providing the possibility to connect to *Kerio MailServer* and synchronize changed data.

Account migration from MS Exchange to Kerio MailServer

Kerio MailServer provides for easy migration of user accounts from *MS Exchange* to *Kerio MailServer*.

MS Entourage Support

Kerio MailServer provides support for *Microsoft Entourage* email client. It allows saving email folders, contact and calendars on the server. This support also enables to work with the *Kerio MailServer's Free/Busy* server .

For communication with *MS Entourage*, *Kerio MailServer* uses the WebDAV protocol. Therefore, the HTTP server must be running at the server.

Support for groupware features in Apple Mail 10.4

Since version 6.1.2, *Kerio MailServer* support some groupware features in *Apple Mail 10.4*.

Apple iCal Support

Kerio MailServer version 6.1 and higher provides support for the *Apple iCal* application. Users can subscribe and publish calendars in the *Kerio MailServer*.

Apple Address Book Support

The *Apple Address Book* application support allows users to search the LDAP database used by *Kerio MailServer*. In *Apple Address Book* version *Apple Mac OS X 10.3*, users can also synchronize contacts.

BlackBerry support

Kerio MailServer enables wireless access to email by using the *BlackBerry Internet Service*. For detailed information, refer to the knowledge base article at *Kerio Technologies* website (<http://support.kerio.com/>).

Active Sync support

Support for *MS Active Sync* enables to synchronize email, calendars and tasks in *MS Outlook* and *MS Windows* on a PDA device. Synchronization will be performed

between a desktop application and a mobile device (only if *MS Active Sync* is installed).

Warning: To ensure that the synchronization is performed also at the server's side, *MS Outlook* must be extended by the *Kerio Outlook Connector* or the *Kerio Synchronization Plug-in*.

Chapter 3

Installation

3.1 System requirements

The minimum hardware configuration recommended for *Kerio MailServer*:

- CPU Intel Pentium II or compatible; 300 MHz
- 128 MB RAM
- 50 MB of disk space for installation
- Disk space for user mailboxes (depends on the number of users)
- For maximum protection of the installed product (particularly its configuration files), it is recommended to use the *NTFS* file system.

Recommended hardware configuration of the computer where *Kerio MailServer* will be running:

For 100 active users

- Processor: 1.5 GHz
- 512 MB RAM
- The size of disk space depends on the volume of data in user mailboxes

For 500 active users

- Processor: 2.5 GHz
- 1.5 GB RAM
- The disks are arranged in RAID 0+1 or RAID 5, the size of disk space depends again on the volume of data in user mailboxes.

Notes:

1. An active user is a user that uses the *Kerio MailServer* services multiple times a day (e.g. mail services, calendar, tasks, etc.).
2. These recommendations apply only in case the computer is used only as a mailserver (*Kerio MailServer*, antivirus, anti-spam).

3.2 Conflicting software

Kerio MailServer runs on the application layer and there are not any known low-level conflicts with other software, operating system components or device drivers (except the antivirus that is used to open files). If a received email message includes an infected attachment, the mail server stores it into a temporary file on the disc. Antivirus might damage the disc or the system. To prevent your computer from such failure, deny your antivirus to the file (or the disc) where *Kerio MailServer* data is kept (refer to chapter 18).

A possible conflict is a port clash (if all services are running in *Kerio MailServer*, these TCP ports are used: 25, 80, 110, 119, 143, 443, 465, 563, 993, and 995). It is therefore not recommended that users run other mail, LDAP or web server software on the same computer. If this is necessary, the system administrator must ascertain that there will be no port clashes. For example, if *Kerio MailServer* is running on a computer together with a web server, we recommend changing the *HTTP* service port or disabling the service and only enabling its secured version — *Secure HTTP*. Another alternative is to reserve one or more IP addresses for ports at which *Kerio MailServer* services are listening. For detailed information on services and port settings, see chapter 7.

If *Kerio MailServer* is run on a firewall or on a secured local network behind a firewall, the firewall will affect the mail server's behavior to a certain extent (e.g. accessibility of some or all services). When configuring the firewall take into consideration which services should be accessible from the Internet or the local network and enable communication on appropriate ports (see above or chapters 7 and 24.3 for more detail).

3.3 Installation

It is recommended that older versions of *Kerio MailServer* 5 should upgrade to *Kerio MailServer* 5.7.10 (<http://download.kerio.com/archive>) before upgrading to *Kerio MailServer* 6.x.

Kerio MailServer can be installed on one of these operating systems:

Microsoft Windows

The product can be installed under the following operating system versions:

- Windows 2000 (SP4)
- Windows XP
- Windows 2003

When the installation program is started, a wizard is run where basic parameters can be set as well as some settings from *WinRoute Pro 4.x* can be imported. For details about this wizard, refer to chapter 3.4.

Note: If you use *WinRoute Pro 4.x* and you want to import the settings, stop the *WinRoute Engine* service before starting the *Kerio MailServer* installation (all the settings will be saved to the system registry).

Warning: Don't perform *Kerio WinRoute* uninstallation — all the settings would be lost!

By default, *Kerio MailServer* is installed to

C:\Program Files\Kerio\MailServer

This setting can be changed during the installation process if necessary.

The first step during the installation is a language selection. It is relevant only to the installation program.

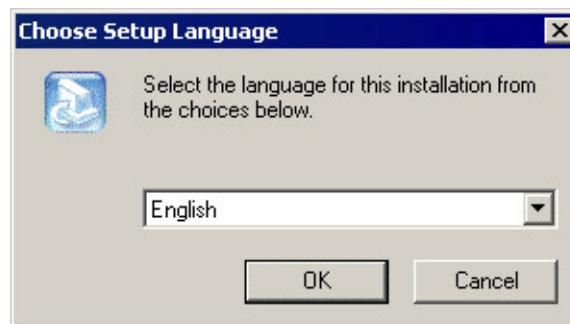


Figure 3.1 Installation — language selection

The next step is a selection of an installation type. The following types are available:

- *Typical* — complete installation
- *Minimal* — minimal installation

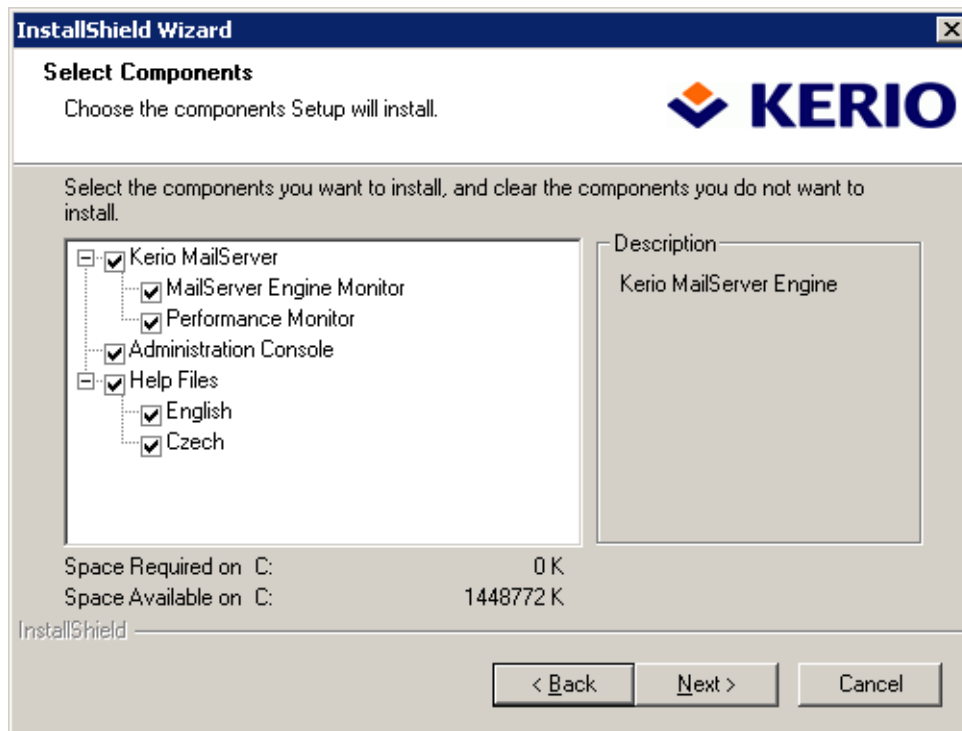


Figure 3.2 Installation — custom install

- *Custom* — selection of *Kerio MailServer* components which will be installed as well as of a language of the *Kerio MailServer*'s help. If you enable both *English* and *Czech*, the help will be displayed in the language version which is set in the *Kerio Administration Console*. If the language in the *Kerio Administration Console* is changed, the language in the help is switched automatically.

Note: If you upgrade the current installation, notice that all selected components will be installed or updated whereas all non-selected components will not be installed or uninstalled (if they are already installed). Therefore, all components which should be preserved must be selected.

After this step, the installation continues (i.e. files are copied to a hard drive and all necessary system settings are performed). Then the wizard for the basic server parameters settings is run.

After installation process is completed successfully, the configuration wizard will be started. Insert primary domain name and password for administration (see chapter 3.4).

Kerio MailServer Engine, which is the mail server's core, running as a service, will be started immediately after the installation is complete. This implies that a utility called *Kerio MailServer Monitor* will also be run, by which you can view the *Engine* status, stop

or start the mail server and perform other tasks. *Kerio MailServer Monitor* is displayed as an icon in the SysTray.

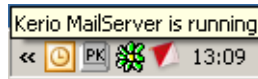


Figure 3.3 Kerio MailServer Monitor

Linux

Kerio MailServer supports the following version of the operating system:

- *Red Hat 9.0*
- *Red Hat Enterprise Linux 3*
- *Fedora Core 1-4*
- *SuSE Linux* since 9.0

Kerio MailServer is distributed in two *RedHat Package Manager* packages — the server and the administration console.

The installation must be performed by a user with root rights. *Kerio MailServer Engine* is installed to `/opt/kerio/mailserver` and the *Kerio Administration Console* to `opt/kerio/admin`.

New installation

Start installation using this command:

```
# rpm -i <installation_package_name>
```

Example:

```
# rpm -i kerio-mailserver-6.1.3-linux.i386.rpm
```

In case of the recent versions of the distributions, problems with package dependencies might occur. If you cannot install *Kerio MailServer*, download and install the `compat-libstdc++` package.

It is recommended to read carefully the `LINUX-README` file immediately upon the installation. The file can be found in

```
/opt/kerio/mailserver/doc
```

When the installation is completed successfully, run the configuration wizard to set the domain and the administrator's account:

```
/opt/kerio/mailserver
```

```
./cfgwizard
```

Warning: The *Kerio MailServer Engine* must be stopped while the configuration wizard is running.

Starting and stopping the server

Once all settings are finished successfully in the configuration wizard, *Kerio MailServer* is ready to be started.

Within the installation, the `keriomailserver` script is created in the `/etc/init.d` directory which provides automatic startup of the daemon (i.e. *MailServer Engine*) upon a reboot of the operating system. This script can also be used to start or stop the daemon manually, using the following commands:

```
/etc/init.d/keriomailserver start
/etc/init.d/keriomailserver stop
```

Administration

The *Kerio Administration Console* can be run by the `kerioadmin` command. The *X-Window* graphical interface is required.

Note: Kerio MailServer must be running on the root account.

Mac OS X

The product supports for the following operating systems:

- Mac OS X 10.3 Panther
- Mac OS X 10.4 Tiger

Kerio MailServer is distributed in the installation package

`kerio-mailserver-6.1.3-mac.dmg`

When it is started, the file is opened as a disk and the executable installation file is offered.

Installation requires a valid username and password. Only authorized users (members of the *Admins* group) are allowed to install applications under the system.

If you confirm the licensing policy you will be allowed to select an installation type. The *Easy Install* type is already predefined. Within the *Custom Install* type you can select individual components that you would like to install (*Kerio Administration Console*, *Kerio MailServer Engine* and *Administrator's Guide* are available). To uninstall the application, choose the last option.

Select an installation type (the *Easy Install* option will install all available components) and wait until the installation process is finished. Complete version of *Kerio MailServer* will be installed (*Kerio Administration Console*, *Kerio MailServer Engine* and *Administrator's Guide*).

By default, *Kerio MailServer* is installed under `/usr/local/kerio/mailserver`.



Figure 3.4 User authentication



Figure 3.5 Installation — custom install

After installation process is completed successfully, the configuration wizard will be started. Insert primary domain name and password for administration (see chapter 3.4). Click *OK* to open the *Kerio MailServer* folder which includes the Administration Console executable file, the administrator's guide (Administrator's Guide) in *PDF*, *Kerio MailServer Monitor* (see chapter 5.1) and *Configuration Wizard* (refer to chapter 3.4).



Figure 3.6 Kerio MailServer folder

Kerio MailServer will be run automatically after the operating system is booted. However, in order to stop or restart the service, it is necessary to run *Kerio MailServer Monitor* (located in the *Kerio MailServer* folder). Username which must belong to the Admins group and password is required for stopping or running of the service. Once authenticated, clicking *Stop* or *Start* is sufficient.

You can also stop, start or restart the *MailServer* through *Terminal* or a SSH client with the following commands with root access:

Stopping the Kerio MailServer Engine

```
SystemStarter stop KerioMailServer
```

Starting the Kerio MailServer Engine

```
SystemStarter start KerioMailServer
```

Restarting the Kerio MailServer Engine

```
SystemStarter restart KerioMailServer
```

3.4 Configuration Wizard

The installation program for Windows and MacOS X operating systems automatically runs a wizard that helps to set the basic parameters for *Kerio MailServer*. This wizard can be invoked anytime later by running `cfgWizard.exe` (Prior to running the wizard, the *Kerio MailServer* service must be stopped). After running the wizard, existing configuration files will be deleted.

The wizard can be also run on Linux. When a corresponding RPM package is installed, user will be informed that the wizard is available. This information is also provided by the daemon if it detects that the wizard has not been used yet. To run the wizard use the following command:

```
/opt/kerio/mailserver  
./cfgwizard
```

Warning: *Kerio MailServer* must be stopped while settings are changed in the configuration wizard.

Note: The configuration wizard for all operating systems is available in English version only.

Primary Domain

To create user accounts (or groups) in *Kerio MailServer*, at least one local domain must be created. The first local domain created is the primary domain. Unlike in the other local domains, users can login by their usernames (In the other domains, it is necessary to use the full email address. For detailed information on domains, see chapter 8.

First, insert name of your primary domain. If you want *Kerio MailServer* to manage multiple domains, select the one that will be used for administration account definition as the primary domain (typically the domain of your company).

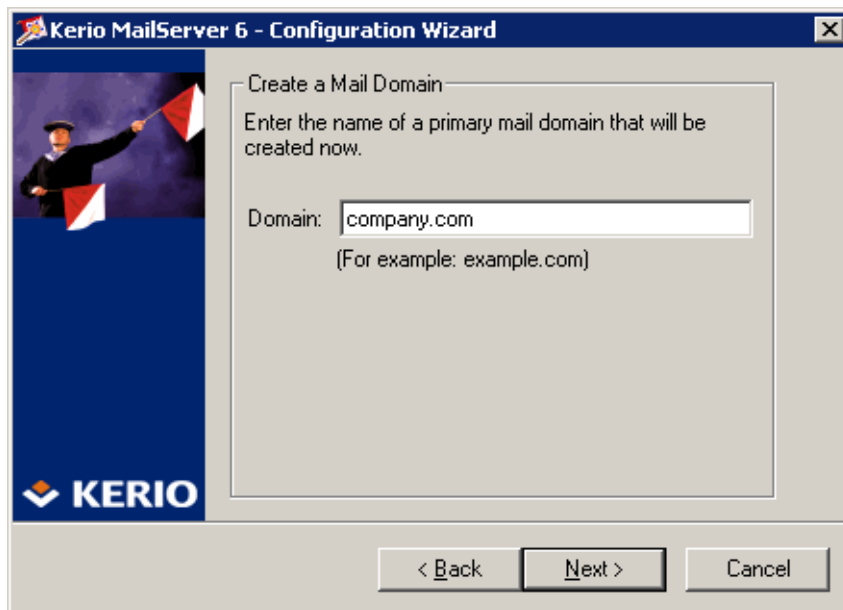


Figure 3.7 Configuration Wizard — creation of the primary domain

Administrator Password Settings

Administrator password is a very important aspect of your server security. Blank password is not accepted. For security reasons passwords should consist at least of six characters.

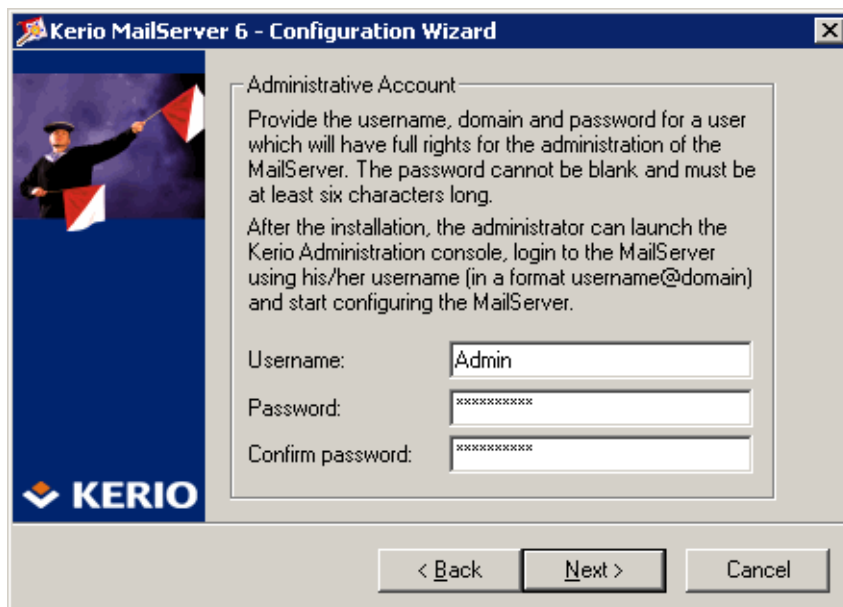


Figure 3.8 Configuration Wizard — user account creation

Password and its confirmation must be entered in the dialog for account settings. The administrator's username (Admin is used as default) can be edited in the *Username* text field.

Store Directory Selection

Kerio MailServer stores a relatively large amount of data (email messages, information about user folders, records, etc.). The administrator can require to store data to another disk (e.g. another disk partition, RAID etc.). The store directory can be changed anytime later through the *Kerio Administration Console* (see chapter 16.6), then it is necessary to move files located in this directory. Prior to this potentially very time-consuming operation, the *Kerio MailServer Engine* must be stopped. Therefore, it is recommended to select an appropriate folder during the installation — using the configuration wizard.



Figure 3.9 Configuration Wizard — folder selection

The *Change* button opens the standard system dialog for folder selection.

The last step of the initial configuration

The last dialog provides information about writing of the primary domain in the configuration files:

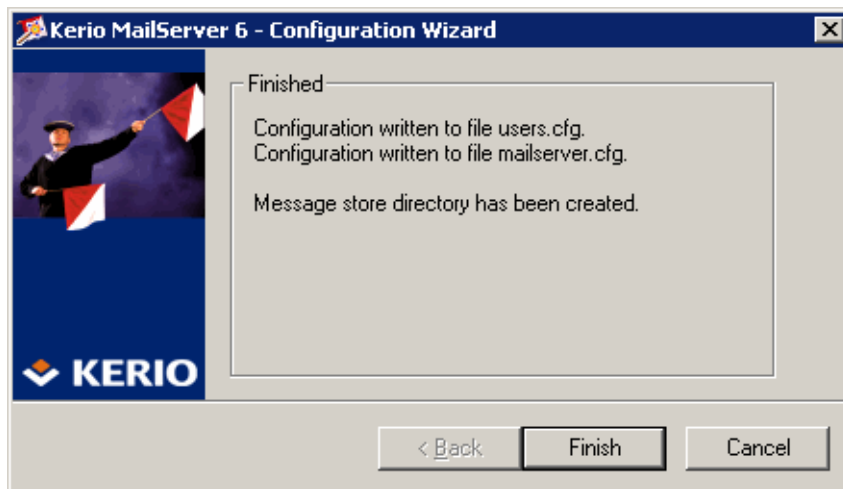


Figure 3.10 Information about successful completion of the primary domain configuration

users.cfg

The `users.cfg` file is an XML file that includes information about user account, groups and aliases.

Administration name and password was written in this file by the configuration wizard.

mailserver.cfg

`mailserver.cfg` is an XML file containing any other parameters of *Kerio MailServer*, such as configuration parameters of domains, back-ups, antispam filter, antivirus, etc.

In this file, the local primary domain just created as well as the location of the message store was written.

Importing Settings from WinRoute

If the configuration wizard detects a *WinRoute Pro 4.x* installation, then it asks the user if he wants to perform an import of settings from this application. To import the settings, make sure that the *WinRoute Engine* service is stopped (so the latest changes are saved to the system registry). The following settings will be imported after the *Next* button is clicked:

- user accounts (*users*)
- user groups (*groups*)
- aliases
- remote POP3 mailboxes

- sorting rules
- IP address groups

The following dialog window shows the results of import (number of imported user accounts, groups, aliases, etc.).



Figure 3.11 Configuration Wizard — import from WinRoute

Other *Kerio MailServer* parameters must be set manually.

Note: Local domains and their settings are not imported from WinRoute. Imported accounts, groups and aliases don't belong to any domain; they are automatically inserted into the primary local domain.

Protection of the installed product

In order to ensure the maximum protection of the mailserver, it is necessary to disallow unauthorized access to the application files (in particular to the configuration files). If the *NTFS* file system is used, the system resets the access rights to the directory where *Kerio MailServer* is installed (including all subdirectories — even if the path has changed) upon each startup: the read and write access is allowed only for members of the *Administrators* group and the local system account (*SYSTEM*); no one else is allowed to access the system files.

Warning: If the *FAT32* file system is used, it is not possible to protect *Kerio MailServer* in the above way. Thus, we strongly recommend to install *Kerio MailServer* only on *NTFS* discs.

3.5 Upgrade and Uninstallation

Windows Operating Systems

To upgrade this product the *Kerio Administration Console* must first be closed. The other components (*Kerio MailServer Engine* and *Kerio MailServer Monitor*) will be automatically closed by *Kerio MailServer* installation program. The installation program will detect the directory where the older version is installed and replace appropriate files with new ones automatically. All settings and all stored messages will be available in the new version. We recommend not changing the installation directory!

Stop the *Kerio Administration Console* before you start an uninstallation. *Kerio MailServer* can be uninstalled by using Uninstall from the Start menu using the *Add/Remove Programs* in the *Control Panels*.

Linux Operating System

Upgrade

To upgrade, use the following command:

```
# rpm -U <installation_package_name>
```

Example:

```
# rpm -U kerio-mailserver-6.1.3-linux.i386.rpm
```

Uninstallation

To uninstall *Kerio MailServer*, use the following commands:

```
# rpm -e <package_name>
```

This means:

```
# rpm -e kerio-mailserver (for the standard version of Kerio MailServer)
```

```
# rpm -e kerio-mailserver-admin (for Kerio Administration Console)
```

Note: During the uninstallation process, only the files that have been included in the former installation package and that have not been edited will be removed. Configuration, messages in the mailboxes, etc. will be retained. Such files may be deleted manually or kept for further installations.

Mac OS X

Upgrade

To upgrade this product the *Kerio Administration Console* must first be closed. The other components (*Kerio MailServer Engine* and *Kerio MailServer Monitor*) will be automatically closed by *Kerio MailServer* installation program. The installation program will detect the directory where the older version is installed and replace appropriate files with new ones automatically. All settings and all stored messages

will be available in the new version. We recommend not changing the installation directory!

Uninstallation

Stop the *Kerio Administration Console* before you start an uninstallation. You can also use the installation program to uninstall this product.

Chapter 4

Product Registration and Licensing

Once purchased, *Kerio MailServer* must be registered. Registration may be performed in the *Kerio MailServer's* administration console (see chapter 4.2) or at *Kerio Technologies* website (refer to chapter 4.1).

If *Kerio MailServer* is not registered, it behaves like a trial version. The trial version of *Kerio MailServer* is not limited in functionality, it only expires after a certain period of time. After 30 days from the installation, *Kerio MailServer Engine* is disabled.

This means that the trial version differs from the registered version only in time of functionality. Under such conditions, each customer can test the product in the regular environment. It is not necessary to reinstall or reconfigure *Kerio MailServer* after registration.

4.1 Product registration at the website

Web registration can be performed at the *Kerio Technologies* website (<http://www.kerio.com>), in the *Support* → *License registration* menu. This registration method is useful especially when *Kerio MailServer* cannot access the Internet.

Against the registration, you will receive a license key (the `license.key` file including the corresponding certificate) which must be imported to *Kerio MailServer*. For detailed information on the import of the license key, refer to chapter 4.3.

Note: The trial version of *Kerio MailServer* cannot be registered via the website.

4.2 Registration with the administration console

In *Kerio Administration Console*, the product can be registered at the main page of *Kerio MailServer* (see figure 4.7). *Kerio MailServer* main page is opened upon each startup of the *Kerio Administration Console*. It can be also displayed by clicking on *Kerio MailServer* in the sections list provided in the tree (see chapter 6.1).

Warning: If *Kerio MailServer* is protected by a firewall, it is necessary to allow outgoing HTTPS traffic for *Kerio MailServer* at port 443. Unless HTTPS traffic is allowed, *Kerio MailServer* cannot use the port to connect to the *Kerio Technologies* registration server.

When installed, the product can be registered as trial or as a full version:

Why should I register the trial version?

The trial version is intended to introduce product's features and configuration. Once you register the trial version, you will be provided free *Kerio Technologies* technical support during the entire trial period (up to 30 days).

Upon the installation, a dialog offering registration of the trial version is displayed (see figure 4.1). The trial version can be registered at the product's main page (see figure 4.7). Just click the *Trial* link at the page to register the product using a registration wizard.

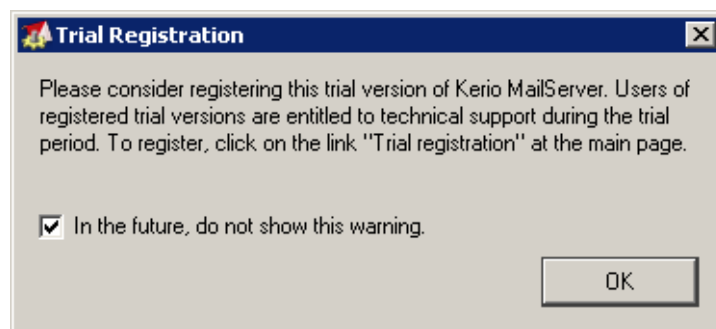


Figure 4.1 Registration of the trial version

It is recommended to increase attention especially at step five where a special identification code called *Trial ID* is generated. This ID is later required when contacting the technical support. Once the product is registered successfully, the code is displayed at the main page accompanied by additional license information.

Note: If you intend to reinstall *Kerio MailServer* or to move it to another working station in the registered trial period, it is recommended to back-up the `mailserver.cfg` configuration file first (besides another information, your trial ID is included in this file).

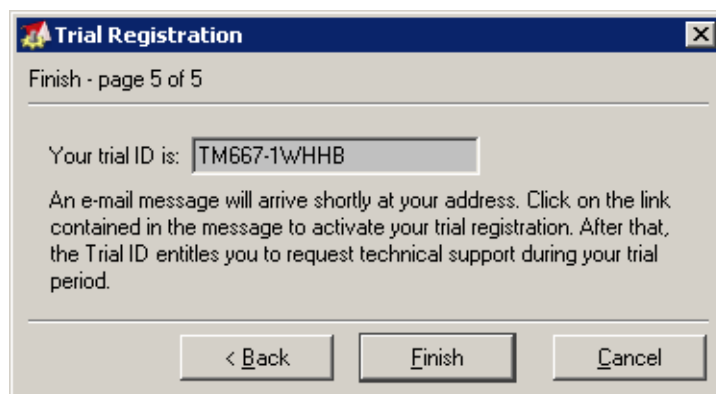


Figure 4.2 Trial ID

If the registration is completed successfully, a confirmation message will be sent to your email address provided.

Registration of full version

To run the process of full version registration, click on the *Register product* link provided at the main page of the administration console(see figure 4.7).

Step One — Base Product

In step one, enter the license number you acquired upon purchasing the product (*License number*).

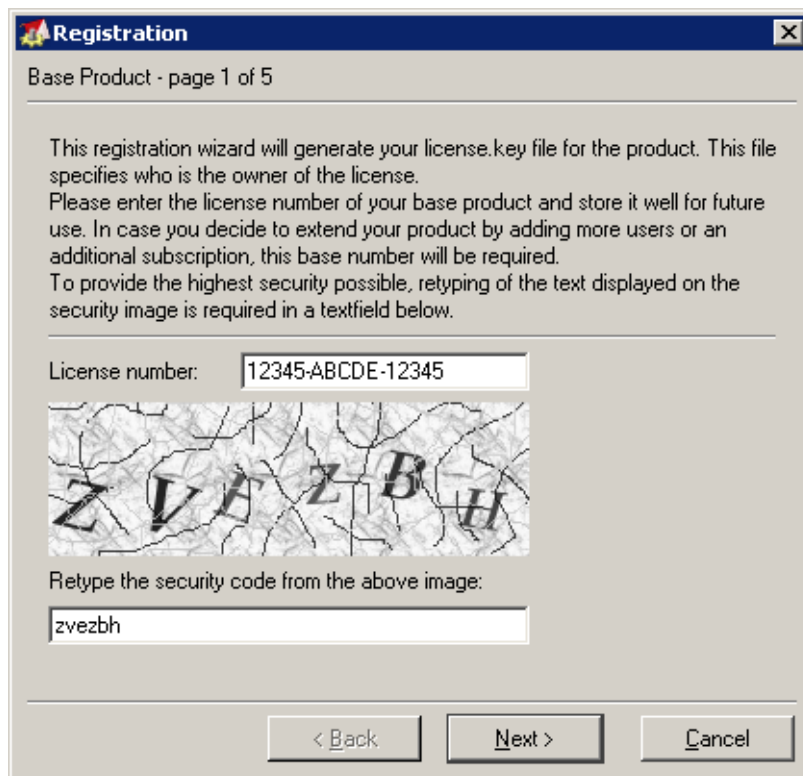


Figure 4.3 License number

License number

Enter your license number for the product.

Security code

Copy the security code provided in the picture. The code is a part of the protection against license number generators.

The code is not case-sensitive.

Click *Next* to make *Kerio MailServer* establish connection to the registration server and check validity of the number entered. If the number is invalid, the registration cannot be completed.

Step Two — Subscriptions

In this dialog you can specify add-ons and/or subscriptions numbers. If you have purchased only the base license so far (usually when registering the product for the first time), skip this step.

Subscription and add-on licensing policies are described in detail at the *Kerio Technologies* webpage — <http://www.kerio.com/subscription.html>.

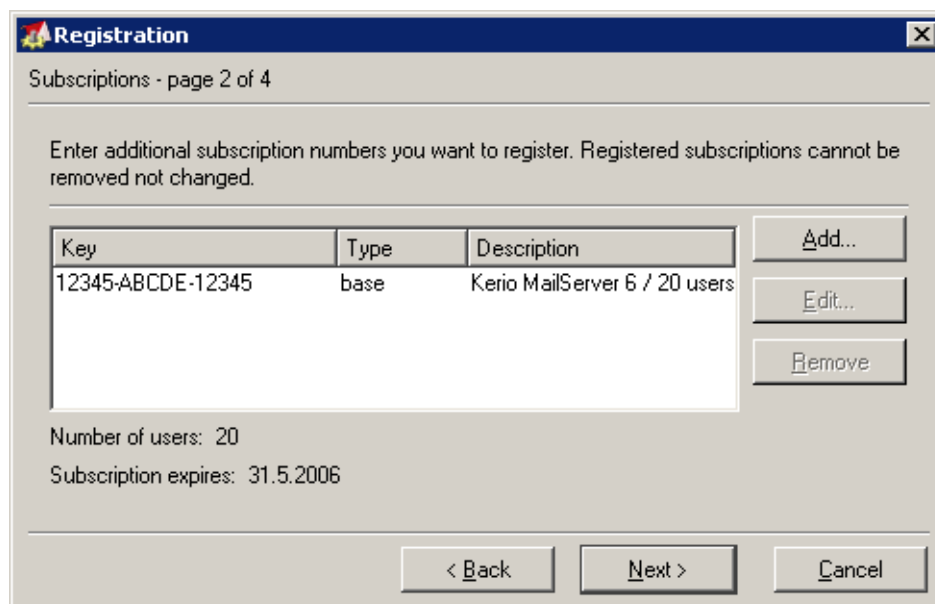


Figure 4.4 Subscriptions and add-ons numbers

You can add one or more license numbers acquired upon purchasing a subscription or an add-on license. Numbers provided in the list can also be edited or removed. To register all numbers specified, click *Next*.

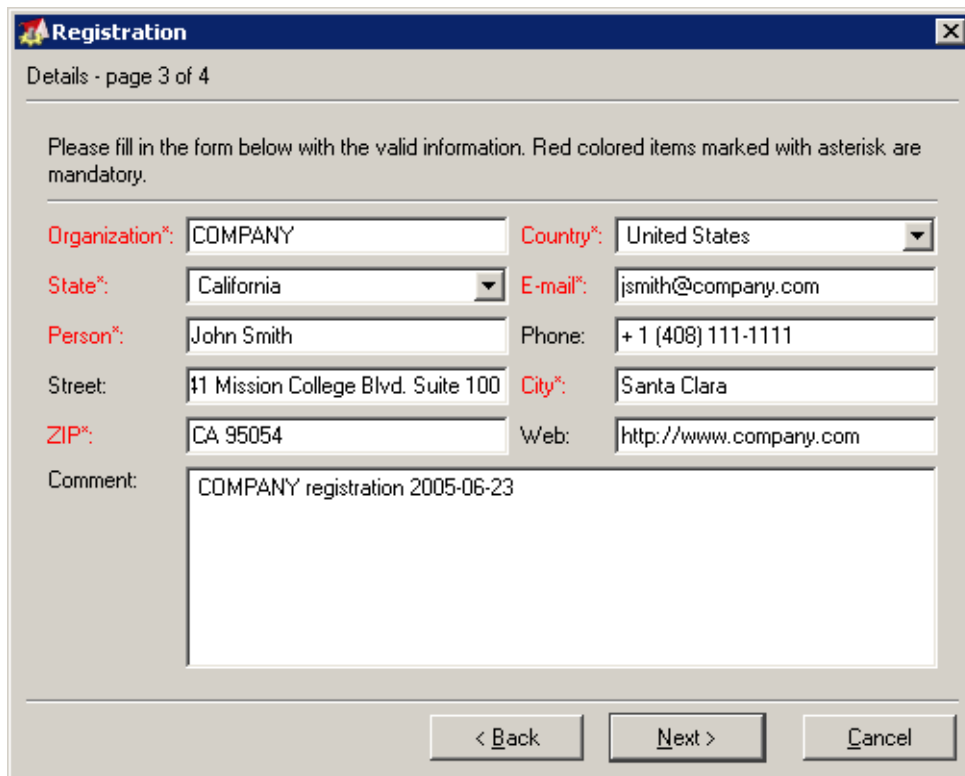
Step Three — Details

At this page, registration information identifying the company (organization) to which the product is registered is required.

The red entries marked with an asterisk are required, the other ones are optional.

Step Four — Summary

In the last dialog, the data specified in the wizard is summarized. Information of expiration date is provided (the latest date when the product can be updated for free).



The image shows a 'Registration' window with a title bar and a close button. Below the title bar, it says 'Details - page 3 of 4'. A message reads: 'Please fill in the form below with the valid information. Red colored items marked with asterisk are mandatory.' The form contains several fields: 'Organization*' (COMPANY), 'Country*' (United States), 'State*' (California), 'E-mail*' (jsmith@company.com), 'Person*' (John Smith), 'Phone' (+ 1 (408) 111-1111), 'Street' (11 Mission College Blvd. Suite 100), 'City*' (Santa Clara), 'ZIP*' (CA 95054), and 'Web' (http://www.company.com). A 'Comment' field contains the text 'COMPANY registration 2005-06-23'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Organization*	COMPANY	Country*	United States	
State*	California	E-mail*	jsmith@company.com	
Person*	John Smith	Phone:	+ 1 (408) 111-1111	
Street:	11 Mission College Blvd. Suite 100		City*	Santa Clara
ZIP*	CA 95054	Web:	http://www.company.com	
Comment:	COMPANY registration 2005-06-23			

Figure 4.5 Registration form

Kerio MailServer connects to the registration server, checks whether the data inserted is correct and downloads automatically the license key (digital certificate).

Click *Finish* to close the wizard.

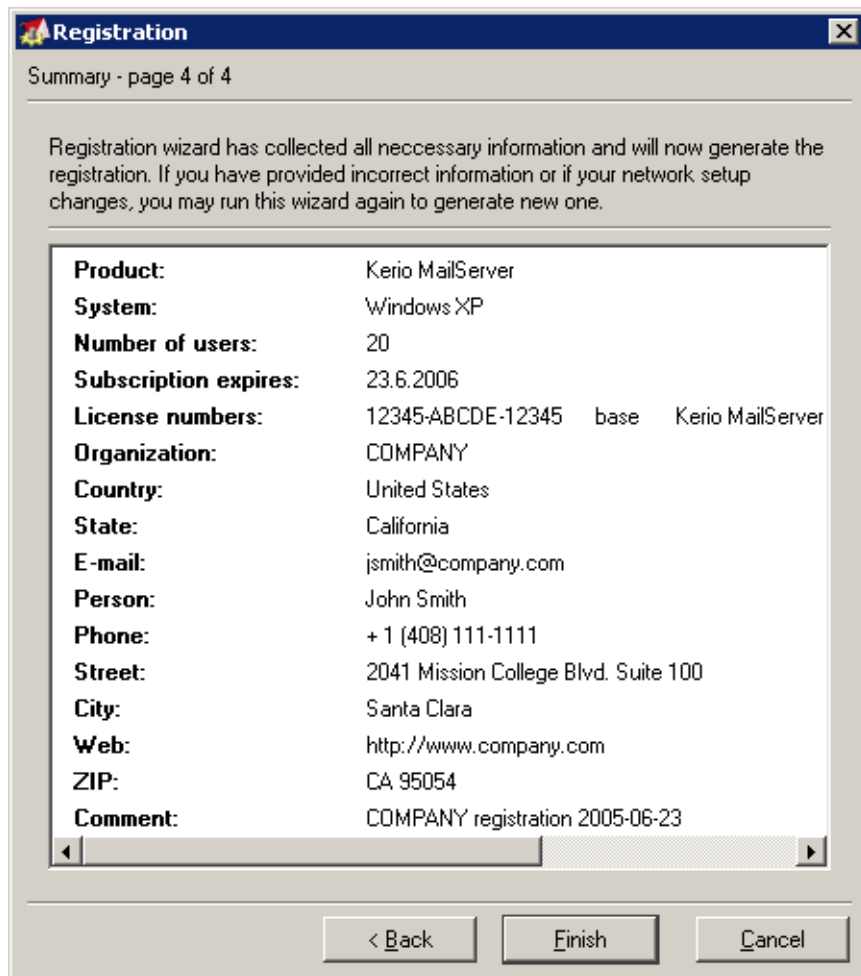


Figure 4.6 Registration data summary

4.3 License information and import of the license key

License information is provided at the main page of *Kerio MailServer*. *Kerio MailServer* main page is opened upon each startup of the *Kerio Administration Console*. It can be also displayed by clicking on *Kerio MailServer* in the sections list provided in the tree (see chapter 6.1).

To run a full version of *Kerio MailServer*, so called license key is required. A license key is a special file that must be imported to the product. Three methods can be applied to obtain the key (depending on the type of the product's registration and on the fact whether the product was registered in time):

- The license key is imported automatically during the product's registration in the administration console (see chapter 4.2)



Figure 4.7 Viewing license information

- *Import via the context menu* — click the right mouse button at the main page (see figure 4.7) to open the context menu and select the *Install license* option (see figure 4.8). A standard file-opening dialog is displayed where the license key can be browsed and imported. If the import is successful, information about the new license is provided at the main page.

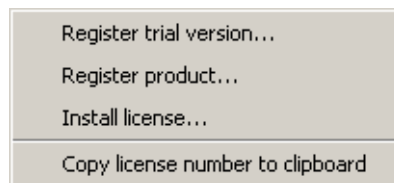


Figure 4.8 The main page's context menu

If the new license increases number of licensed users, the *Kerio MailServer Engine* must be restarted upon the successful installation.

- *Adding the license key file in the license directory manually* — it is possible to copy the `license.key` file manually to the `license` subdirectory under the directory where *Kerio MailServer* is installed.

If the file must be imported manually, it is necessary to stop the *Kerio MailServer Engine* before the import process is started.

Product

Product name (*Kerio MailServer*).

Copyright

Copyright of the product.

Homepage

Kerio Technologies homepage.

Operational system

Operating system on which the application is running.

License ID

License number of the product.

Subscription expiration date

The latest date when the product can be updated for free.

Product expiration date

The date when the product expires and stops functioning (only for trial versions and special licenses).

Number of users

Number of licensed users. Number of locally created users is provided in brackets. Users mapped from the directory service are not included in this number.

Users tracked since server start

Number of users connected since the last restart of *Kerio MailServer*. The number includes all local users, all mailing lists (one mailing list for one license) as well as all users mapped from the directory service connected to their *Kerio MailServer* accounts.

Company

Name of the company (or a person) to which the product is registered.

If the *New version available...* link is displayed in the introductory window when the console is started, it means that *Kerio Technologies* released a new version of the product. Click on the link to open a web page the new product version can be downloaded from. New versions are saved in

`Kerio/MailServer/store/tmp`

4.4 Licensing policy

Number of users is counted by email accounts and mailing lists created in the *Kerio MailServer* or imported from the domain. Number of domains and aliases is not limited.

If users are mapped from the LDAP database of the directory service, all users having been connected to *Kerio MailServer* since the last startup of the server are considered as licenses. Users not having been connected to their *Kerio MailServer* mailboxes are not included in the total number of users (licenses).

Subscription

Subscription and add-on licensing policies are described in detail at the *Kerio Technologies* webpage — <http://www.kerio.com/subscription.html>.

Chapter 5

Kerio MailServer Components

Kerio MailServer consists of the following components:

Kerio MailServer Engine

is the core of the program that provides all services and functions. It runs as a background application (as a service on Windows 2000 or XP, or as a daemon on UNIX-like systems).

Kerio MailServer Monitor

allows viewing and modification of the *Engine's* status (stopped/running) and setting of start-up preferences (i.e. whether *Engine* and *Monitor* should be run automatically at system start-up). It also provides easy access to the *Administration Console*. Details can be found in chapter 5.1.

Note: *Kerio MailServer Monitor* is an application completely independent of the *Kerio MailServer Engine*. The *Engine* can be running even if there is no icon in the System Tray on Windows or in the Dock in Mac OS X.

Kerio Administration Console

is a universal program designed for local or remote administration of Kerio Technologies products. To connect to a certain application a module containing a specific interface for this application is needed. During *Kerio MailServer* installation the *Administration Console* is installed together with the appropriate plugin. *Kerio Administration Console* and its usage are described in detail in chapter 6.

Performance Monitor

This component allows for real time system performance monitoring of KMS components. For more details, see chapter 23.9. This module is available under *MS Windows* operating systems only.

5.1 Kerio MailServer Monitor

Kerio MailServer Monitor is a utility used to control and monitor the *MailServer Engine* status. This component is available only under *Windows* and *Mac OS*.

Windows Operating Systems

In *Windows*, *Kerio MailServer Monitor* is displayed as an icon in the System Notification Area.

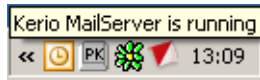


Figure 5.1 Kerio MailServer Monitor

If the mailservice is stopped, a red mark appears over the icon. Starting or stopping the service can take several seconds. During this time the icon is grey and inactive.

On *Windows*, left double-clicking on this icon runs the *Kerio Administration Console* (described later). Right-clicking on this icon displays the following menu.

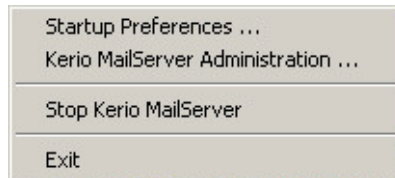


Figure 5.2 Kerio MailServer Monitor — menu

Start-up Preferences

- options for running *Kerio MailServer* and *Kerio MailServer Monitor* automatically at system start-up. Both options are enabled by default.

Kerio MailServer Administration

- this option runs the *Kerio Administration Console* program (this can also be achieved by double-clicking the *Kerio MailServer Monitor* icon).

Start/Stop Kerio MailServer

- start or stop the *MailServer Engine* (*Start* or *Stop* is displayed according to the *Engine* status).

Exit

- exits the *Kerio MailServer Monitor*. This option does not stop the *MailServer Engine*. The user is informed about this fact by a warning window.

Mac OS X

Under *Mac OS X*, *Kerio MailServer Monitor* is displayed in a special window. Unlike the version for *Windows*, this dialog only enables to run or stop *Kerio MailServer Engine*.



Figure 5.3 Kerio MailServer Monitor

You can also stop, start or restart the *Kerio MailServer Monitor* through *Terminal* or a SSH client with the following commands with root access:

Stopping the Kerio MailServer Engine

```
SystemStarter stop KerioMailServer
```

Starting the Kerio MailServer Engine

```
SystemStarter start KerioMailServer
```

Restarting the Kerio MailServer Engine

```
SystemStarter restart KerioMailServer
```

Linux

Installation packages for Linux do not include *Kerio MailServer Monitor*. *Kerio MailServer Engine* can be started by the following command:

```
/etc/rc.d/init.d/keriomailserver [start | stop]
```

Chapter 6

Kerio MailServer Administration

Kerio Administration Console is a general purpose application for administration of *Kerio Technologies* software products. It enables local (i.e. from the computer where *Kerio MailServer Engine* is running), as well as remote administration (from any other computer). The communication between *Kerio Administration Console* and *Kerio MailServer Engine* is encrypted, which prevents it from being tapped and misused.

Note: *Kerio MailServer* administration does not depend on the platform. Server running on Linux can be administered by *Kerio Administration Console* running on Windows and vice versa.

The *Kerio Administration Console* is installed together with the *Kerio MailServer* application (on Windows and Linux, *Kerio Administration Console* can be installed separately — e.g. for remote administration of *Kerio MailServer*). Its use is described in detail in a separate *Kerio Administration Console — Help* manual.

Further chapters of this manual describe the individual sections of the *Kerio MailServer* administration window, which is opened upon a successful login to the *Kerio MailServer Engine*.

6.1 Administration Window

After the user has been successfully logged in to the *Kerio MailServer Engine* by the *Kerio Administration Console*, the main window of the *Kerio MailServer* administration plugin is displayed (further called the “administration window”). This window is divided into two parts:

- The left column contains the list of sections in the form of a tree view. The individual sections of the tree can be expanded and collapsed for easier navigation. *Kerio Administration Console* remembers the current tree settings and uses them upon the next login.
- In the right part of the window, the contents of the section selected in the left column is displayed (or a list of sections in the selected group).

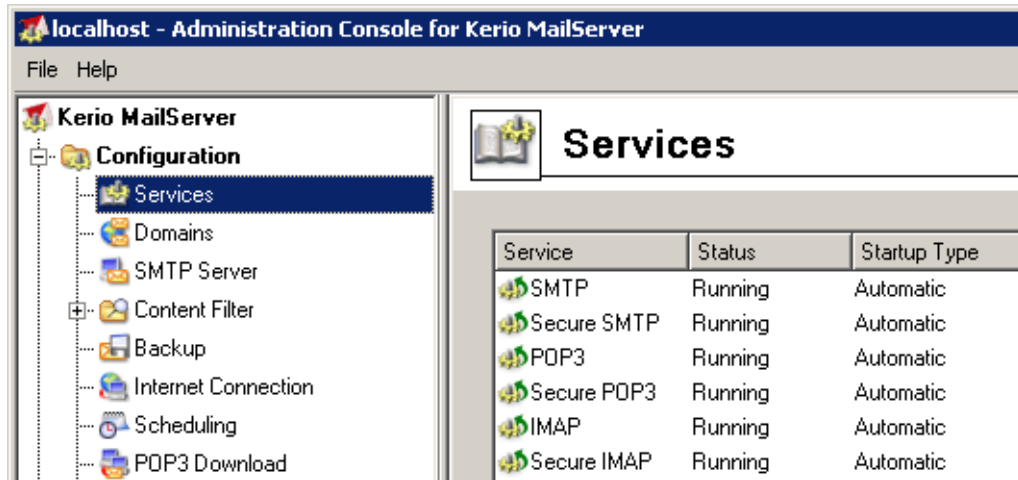


Figure 6.1 Kerio Administration Console

Administration Window — Main menu

The main menu provides the following options:

File

- *Reconnect* — using this option, the connection to the *Kerio MailServer Engine* after a connection drop-out (e.g. after the *Engine* restart or network failure) can be restored.

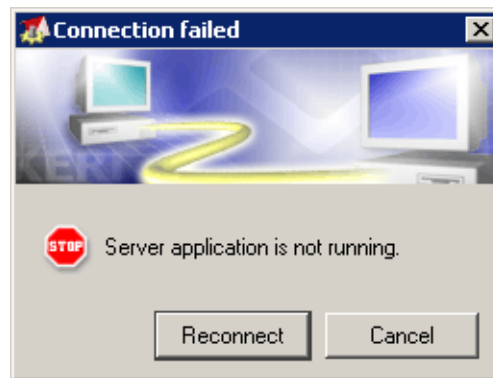


Figure 6.2 Reconnections

- *New connection* — this feature is useful for administration of multiple server applications (e.g. *Kerio MailServer* at multiple servers). The *New connection* option opens the main *Kerio Administration Console* window, where the tab or login dialog box can be used for logging to the desired server (for details, see the *Kerio Administration Console — Help* manual). *New connection* is identical to running the *Kerio Administration Console* from the *Start* menu.
- *Quit* — this option terminates the session (users are logged out of the server and the administration window is closed). The same effect can be obtained by

clicking the little cross in the upper right corner of the window or pressing *Alt+F4*.

Help menu

- *Administrator's guide* — this option displays the administrator's guide in *HTML Help* format. For details about help files, see *Kerio Administration Console — Help* manual.
- *About* — this option provides information about the version of the *Kerio MailServer* and a link to the Kerio Technologies website.

Status bar

The status bar at the bottom of the administration window displays the following information (from left to right):

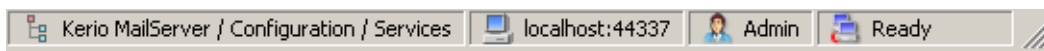


Figure 6.3 Status bar

- The section of the administration window currently selected in the left column. This information facilitates navigation in the administration window when any part of the section tree is not visible (e.g. when a lower screen resolution is selected).
- Server name or IP address and server application port (*Kerio MailServer* uses port 44337).
- Name of the user logged in as administrator.
- Current state of the *Kerio Administration Console*: *Ready* (waiting for user's response), *Loading* (retrieving data from the server) or *Saving* (saving changes to the server).

Detection of the Kerio MailServer Engine connection failure

Administration Console is able to detect the connection failure automatically. The failure is usually detected upon an attempt to read/write the data from/to the server (i.e. when the *Apply* button is pressed or when a user switches to a different section of *Administration Console*). In such case, a connection failure dialog box appears where the connection can be restored.

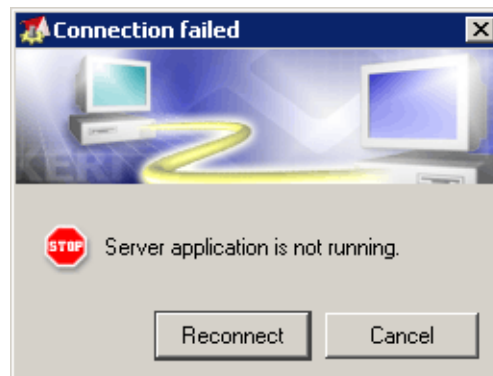


Figure 6.4 Detection of the Kerio MailServer Engine connection failure

After you remove the cause of the connection failure, the connection can be restored. If the reconnection attempt fails, only the error message is shown. You can then try to reconnect using the *File / Restore connection* option from the main menu, or close the window and restore the connection using the standard procedure.

6.2 View Settings

In most sections of the *Kerio Administration Console*, the view consists of a table where each row contains one record and the columns contain single items of this record.

The *Kerio MailServer* administrator can customize the settings for displaying information in individual sections. When you right-click each of the above sections, a popup menu with *Modify columns* option is displayed. This option opens a dialog box where the hidden and displayed columns can be selected by checking the appropriate options.

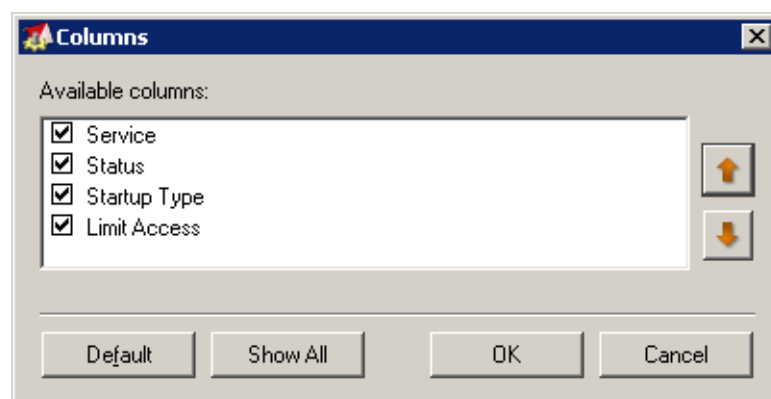


Figure 6.5 Selection of columns

Use the *Move Up* and *Move Down* buttons to move the selected column up and down in a group. This way, the order of columns can be specified.

The order of the columns can be also set directly in the view: click the column name, hold the mouse button and drag to the desired location.

Move the dividing line between the column headers to modify the width of the individual columns.

Chapter 7

Services

In *Configuration* → *Services* the user can set which *Kerio MailServer* services will be run and with which parameters. Use the *Start* and *Stop* buttons below the table to either run or stop appropriate service. The following services are available:

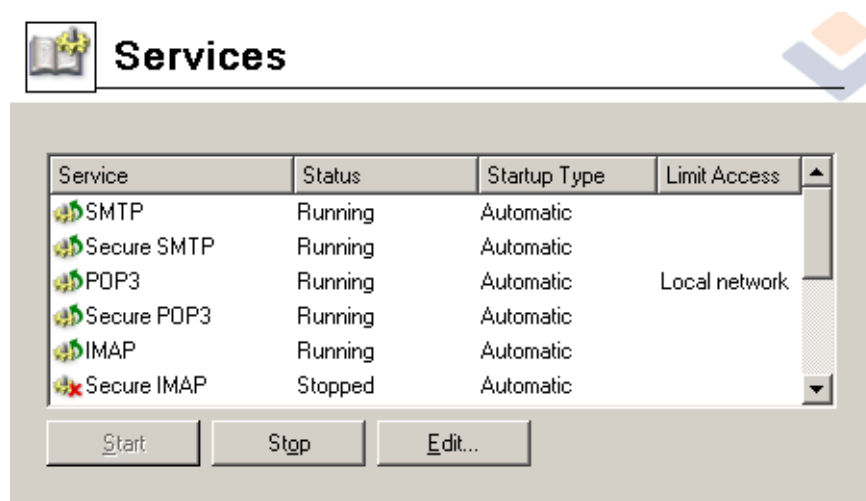


Figure 7.1 Services

SMTP

SMTP protocol server (Simple Mail Transfer Protocol), handling open (non-encrypted) or SSL secured connections. SMTP server is used for sending outgoing mail messages, for receiving incoming mail (if it is the primary or backup domain mail server) and for messages delivered via mailing lists created in *Kerio MailServer*. *Secure SMTP* is an SMTP server whose communication is encrypted by SSL.

POP3

POP3 protocol server (Post Office Protocol). This server allows users — clients to retrieve messages from their accounts. It is also often referred to as the incoming mail server.

Secure POP3 is a POP3 server whose communication is encrypted by SSL. The encryption prevents the communication from being tapped.

IMAP

IMAP protocol server (Internet Message Access Protocol). This server also allows users to access their messages. These, however, stay in folders and can be accessed from multiple locations at any given time.

Secure IMAP is an IMAP server whose communication is encrypted by SSL.

NNTP

NNTP protocol (News Network Transfer Protocol) — transfer protocol for news-groups over the Internet. This service allows users to view an archive of postings to a mailing list.

Secure NNTP is the NNTP server version whose communication is encrypted by SSL.

LDAP

Simple LDAP server that enables users to access centrally managed contacts. The LDAP server provides read-only access to the information; you are not allowed to create nor edit the existing ones.

Secure LDAP is an LDAP server whose communication is encrypted by SSL.

HTTP

The HTTP protocol is used for:

- accessing user mailboxes via *Kerio WebMail*,
- accessing the user administration via web interface (see chapter 27),
- accessing mail using cellular phones with WAPmail,
- accessing mail using *Microsoft Entourage* mail client (see chapter 33),
- accessing the *Free/Busy* server (for detailed information, refer to chapters 31.17 and 33.1).
- automatic upgrades of *Kerio Outlook Connector*.
- for synchronization via *Kerio Synchronization Plug-in*.

Secure HTTP is an encrypted version of this protocol (HTTPS — SSL or TLS encrypted).

7.1 Service Parameter Settings

The list of services contains the following entries:

- Service
- Status (*Stopped* / *Started*)
- Startup (*Manual* / *Automatic*)
- Listen IP addresses and ports from which access to service is allowed.

The parameters of a selected service can be changed (using the *Edit* button). These functions are also available from a context menu that is displayed upon right-clicking a particular service.

Service Configuration

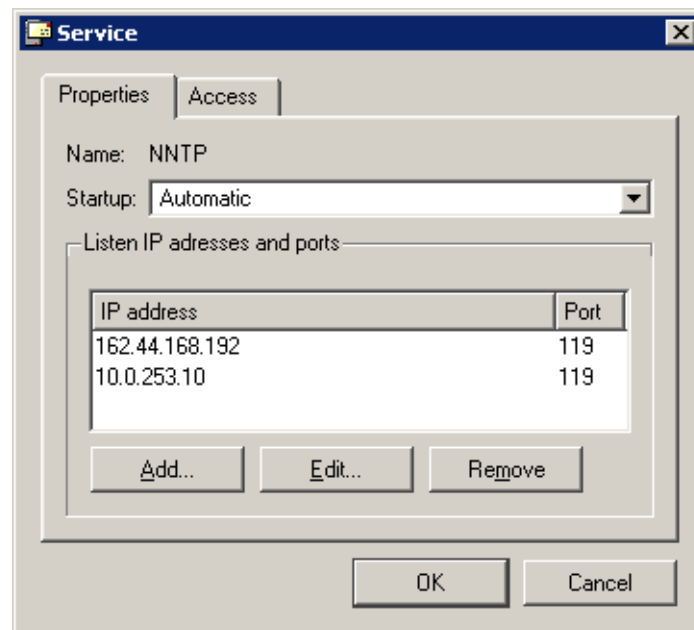


Figure 7.2 Service Parameters

Name

Type of service.

Startup

Service startup mode (automatic/manual). When automatic startup is selected, the service is run immediately after *Kerio MailServer* is started. With manual startup, the service is stopped and it has to be restarted manually by the administrator.

Listen IP Addresses and Ports

By default, *Kerio MailServer* listens at all default ports at all IP addresses of the its host. The *Ports* dialog enables to assign particular IP address to the port where the service is running.

Assignment of an IP address to a standard port of a service running in *Kerio MailServer* may be helpful in the case that *Kerio MailServer* and another application using the same services (e.g. another LDAP server, webserver or mail server) are installed at the same host. In such a case, it is possible to reserve only one IP address for each service of *Kerio MailServer* so that port collisions are avoided.

This means that two different web servers may use port 80 at two different IP addresses.

Note: Indeed, it is necessary to reserve an IP address for the same service in another application, that is not used by *Kerio MailServer*.

Warning: Assignment of IP addresses to ports is not recommended if IP addresses are reserved dynamically, e.g. using DHCP.

Click *Add* to bind the IP address to the port.

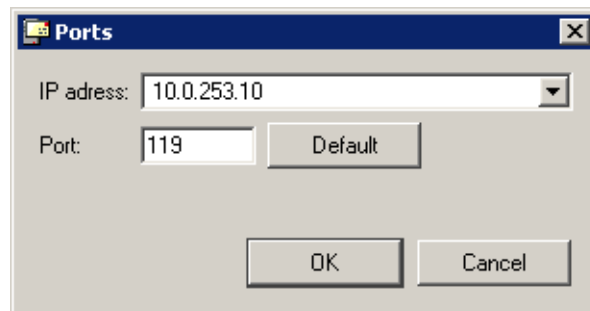


Figure 7.3 Ports

Most services use standard ports and it is not recommended to change them unless necessary (e.g. in case of conflict with another application of the same type). Click *Default* to restore the default settings.

Limiting access to service

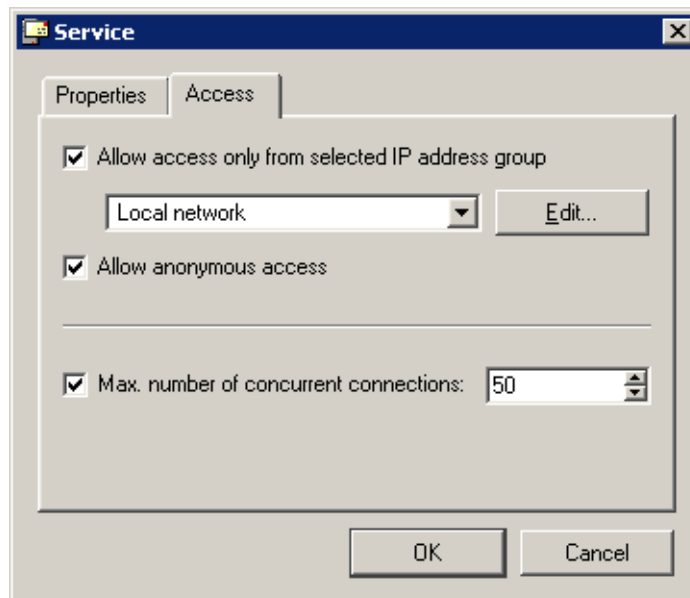


Figure 7.4 Limiting access to service

Allow access only from...

Allows access to a selected service to be limited to certain IP addresses only (defined in the selected group). The IP address group can be defined in the *Configuration/Definitions/IP Address Groups* section or directly in this dialog window by pressing the *Edit* button.

Detailed access policy for the SMTP service can be set in the *Configuration/Antispam* section.

Allow anonymous access

This option relates only to the NNTP(S) service, therefore it is not contained in other dialog windows of other services. This option allows unauthenticated access to the NNTP server. This means that everyone can register to a mailing list with anonymous access.

Max. number of concurrent connections

This option limits the number of concurrent connections to the selected service. Too many concurrent connections may cause the server overload which can subsequently lead to its failure. This is also the main idea of the so-called DoS (Denial of Service) attack where the attacker tries to overload the server by too many concurrent connections. Setting the limit for the number of connections therefore helps to prevent the DoS (Denial of Service) attacks against your server.

Warning: When you plan to limit the number of connections, consider the number of server users.

7.2 Important Notes

Non-secure and secure versions of the same service act as two separate services. This means that there are two different ways of accessing the same server and the user (client) can choose which one to use. For security and privacy protection reasons we strongly recommend using a secure version of any communication means. However, this must be supported by client software.

IMAP and *HTTP* access the same IMAP account in the same way. These two services can both be used (one at a time) without any limitations or risk. POP3 and IMAP/*HTTP* access the same physical account but POP3 can only retrieve messages stored in the *INBOX* folder, as it cannot “see” other folders. All incoming messages are stored in the *INBOX* folder. POP3 also downloads all messages from the server to the client machine. This can lead to the following complications:

1. If a user logs into the account using POP3 first, all messages from the *INBOX* folder will be downloaded to his/her machine. After logging in using IMAP, these messages will no longer be at the server.

2. If a user logs into the account using IMAP first (or uses *HTTP*) and moves messages to a folder other than *INBOX*, these messages will not be downloaded later using POP3.
3. If a user has set rules such that all messages are moved to different folders, no messages will be accessible via POP3.

Chapter 8

Domains

Kerio MailServer can handle multiple independent email domains for which various parameters can be defined.

In *Kerio MailServer*, one domain is always set as primary (the one which was created first). When other domains are added, any of the domains can be set as primary. Users log into the primary domain with their usernames only, whereas they have to log into all other domains using their full email addresses. This is again best shown on an example:

The domain `ourcompany.com` has been set as the primary domain. A user is defined in both domains with the name `user`. The user will log into the domain `ourcompany.com` with the name `user`, whereas for the second domain the user will have to use `user@anothercompany.com` as a username.

Note: Users in the primary domain can also authenticate to the server using their complete email address.

This implies that unless a serious reason to set a particular domain as primary occurs, a domain which includes the highest number of users should be set as primary. That will make it simpler for as many users as possible to specify their usernames when connecting to the server.

User accounts are defined separately in each domain. Therefore, domains must be defined before accounts are created.

8.1 Definition of Domains

Domains are defined in the *Configuration → Domains* section.

In the *Internet hostname* field, enter the Internet (DNS) name of the computer where *Kerio MailServer* is installed (typically, this would be the name of the computer with the appended primary domain name — this way the server name is automatically generated by the configuration wizard). Server names are used for server identification while establishing SMTP traffic.

Upon initializing SMTP communication, the EHLO command is used for retrieving reverse DNS record. The server that communicates with *Kerio MailServer* can perform checks of the reverse DNS record.

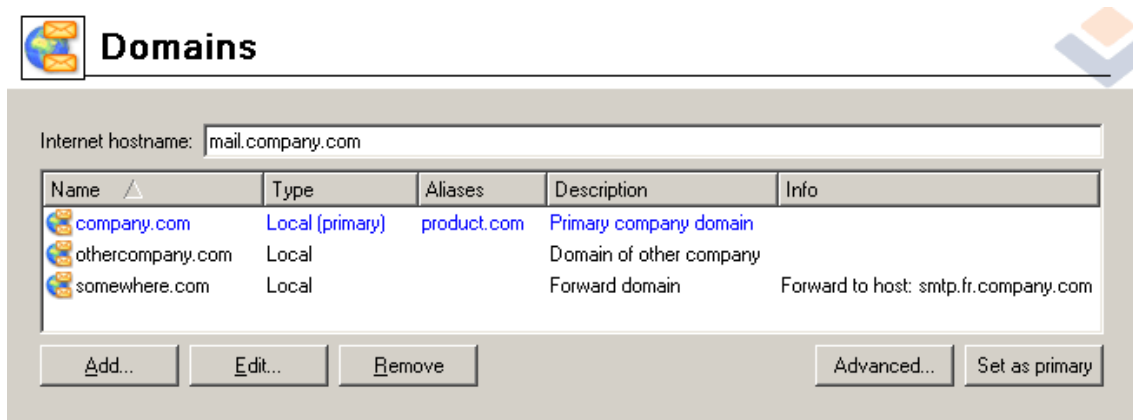


Figure 8.1 Domains

Note: If Kerio MailServer is running behind NAT, enter the *Internet hostname* that can be converted to the IP address of the sending server, i.e. the internet hostname of the firewall.

Click *Advanced* to set location of public folders:

- *Unique for each domain* — each domain contains its own public folders. This configuration does not allow any user for accessing a folder of another domain.

If there are more domains with user mailboxes created in Kerio MailServer, each of these domains must have at least one public folder administrator specified in the *User accounts* section (see chapter 14).

- *Global for all domains* — users of all domains share the same public folders.

Use the *Set as primary* button to change domain type (the same may be performed using the context menu). Any domain ordered as the first one is always primary [*Local (primary)*]. Other domains can be set either as *Local (primary)* or as *Local*.

Note: Any new domain you add can be set as *Local (primary)*, even when another domain already has this status. By taking this step, however, the new domain becomes primary and the former primary domain becomes local only.

Create a new domain by clicking on the *Add* button.

Deleting of domains

You can delete the domain using the *Delete* button. A domain cannot be deleted if:

- user accounts or groups have been already defined within the domain. All accounts must be deleted first (for details, see chapter 14.5).

- the aliases are defined in it. First, delete all the aliases (for details, see chapter 16.3).
- it is the primary domain. However, you can create another domain and define it as primary. Then, the former domain can be deleted.

8.2 General

Basic domain parameters — the General bookmark:

The screenshot shows a 'Domain' settings window with the following fields and options:

- Domain:** company.com
- Description:** Primary company domain
- Message size limit:**
 - ☒ Limit outgoing message size to: 20 MB
 -
- Deleted items recovery:**
 - ☒ Allow deleted items recovery
 - Keep deleted items for 90 day(s) after deletion
- User count limit:**
 - Maximum number of users in the domain: 50
 -

Buttons: OK, Cancel

Figure 8.2 Domain settings — basic parameters

Domain

The name of the new domain

Note: No national or special characters are allowed for the name of the new domain (see *Allowed and prohibited characters in the domain name table*).

Examples of correct names:

company.com; server.company.com; server-company.com;
server---company.com

Examples of incorrect names:

company..com; company...com; .company.com; company.com.;;
server_company.com

Character	Allowed	Character	Prohibited
a-z	allowed	/	prohibited
0-9	allowed	\	prohibited
A-Z	allowed	. .	prohibited
.	allowed when not at the beginning and/or the end of the string and when there are not two dots next to each other	.	prohibited when at the beginning and/or at the end of the string
-	allowed	*	prohibited
		—	prohibited

Table 8.1 Allowed and prohibited characters in the domain name

Description

A notation about the domain created (for the administrator only).

Message size limit

The maximum size limit for all sent messages (via SMTP, WebDAV, etc.). The limit applies only to the domain specified.

It is recommended to activate this option for each domain that contains user mailboxes. This way, you can prevent the internet connection from being overloaded with messages with large attachments (images, clips, music, etc.).

If the limit is set to 0, *Kerio MailServer* behaves the same way as if no limit was set. The message size limit can be also set for individual users separately (see chapter 14.2). The limit set for a particular user has higher priority than the limit set for the domain.

Restoring deleted items

Using this option, the deleted items (messages, events, contacts, tasks) can be moved back to the *Deleted items* folder. Users can also specify how long the items should be preserved so that they can be restored when needed.

The settings depend on the number of user mailboxes in *Kerio MailServer* and free disc space. However, the time must not exceed one year, i.e. 365 days. If the specified number is too large, the domain settings cannot be saved.

It is recommended to enable this option for all domains that contain user mailboxes, so that the items deleted by mistake (messages, events, contacts or tasks) can be easily restored.

To restore the items and move them back to *Deleted items* folder, select *Configuration* → *Domain settings* → *User accounts*. For more information about restoring items for selected users, see chapter 14.7.

User count limit

This option is useful especially when administration of user accounts via web interface is used (see chapter 27). Users with administration rights cannot break this limit.

8.3 Aliases

It is possible to define any number of virtual domains (aliases) for the each email domain. Virtual domains are alternative names (aliases) for a particular domain. Names of the virtual domains can be specified in the *Aliases* section. Email addresses within the virtual domains are identical (delivery is performed to the identical mailboxes). If this option is used, individual user accounts can belong to multiple domains.

Usage of domain aliases will be better understood through the following example:

A company uses two domains: `company.us` and `company.com`. The `company.us` domain is set as a mail domain in *Kerio MailServer*. Email addresses of the domain users are `user@company.us`. If we create the `company.com` domain alias for the `company.us` domain, it is also possible to use the `user@company.com` for identical users. It does not matter, whether the `user@company.us` or the `user@company.com` is used. In both cases, the mail is delivered to the same user.

Warning: Unless this is a local alias (virtual domain), corresponding MX DNS records must be defined for each of such domains. A simple definition of the domain as an alias of another domain does not make the alias exist in the Internet.

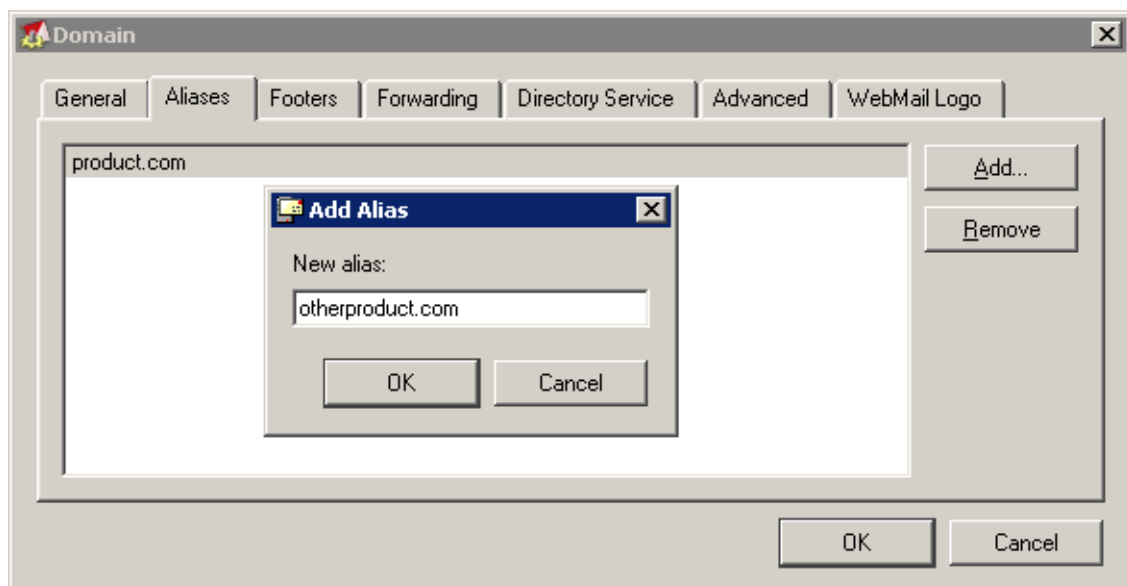


Figure 8.3 Domain settings — equivalent domains (aliases)

Domain aliases can be used only for email delivery. It is not possible to use them for user authentication at *Kerio MailServer* or to view the *Free/Busy* server. Domain aliases cannot be used for administration purposes.

8.4 Footers

Use this tab to add a footer to each message sent from this domain (footer will be added to each message where the address of the sender includes the domain).

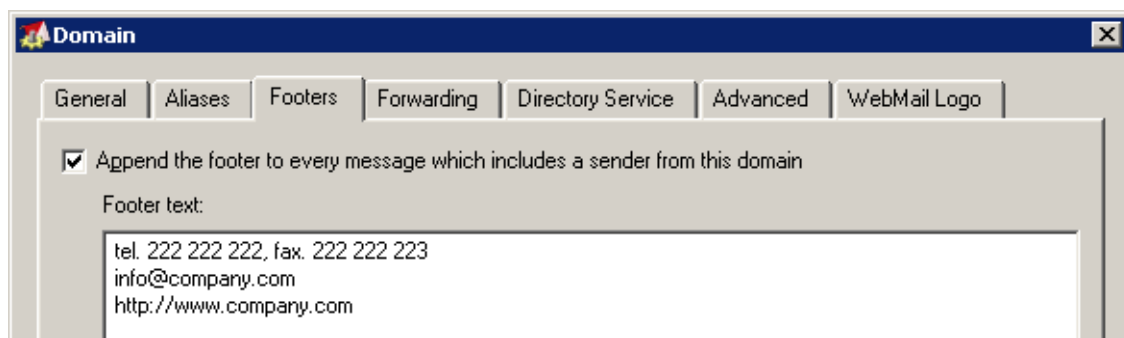


Figure 8.4 Domain settings — footers

Note: The HTML format cannot be used for the footer text. Only plain text is displayed in the message footer.

8.5 Forwarding

Using the *Forwarding* tab parameters you can forward messages to another SMTP server automatically. Forwarding can be used especially for:

- splitting the domain into more servers (for more information, see chapter 25.4),
- creating a backup mailserver (for more information, see chapter 25.5).

If the recipient was not found...

Messages will be forwarded to another SMTP server if a recipient is not found in the domain. Messages are forwarded only if the recipient's address is not an address of any user, group or alias included in this domain. If there is no user, group or alias defined in this domain, all messages will be forwarded (this function is equal to the *Forward* feature in versions former to *Kerio MailServer 5.5*).

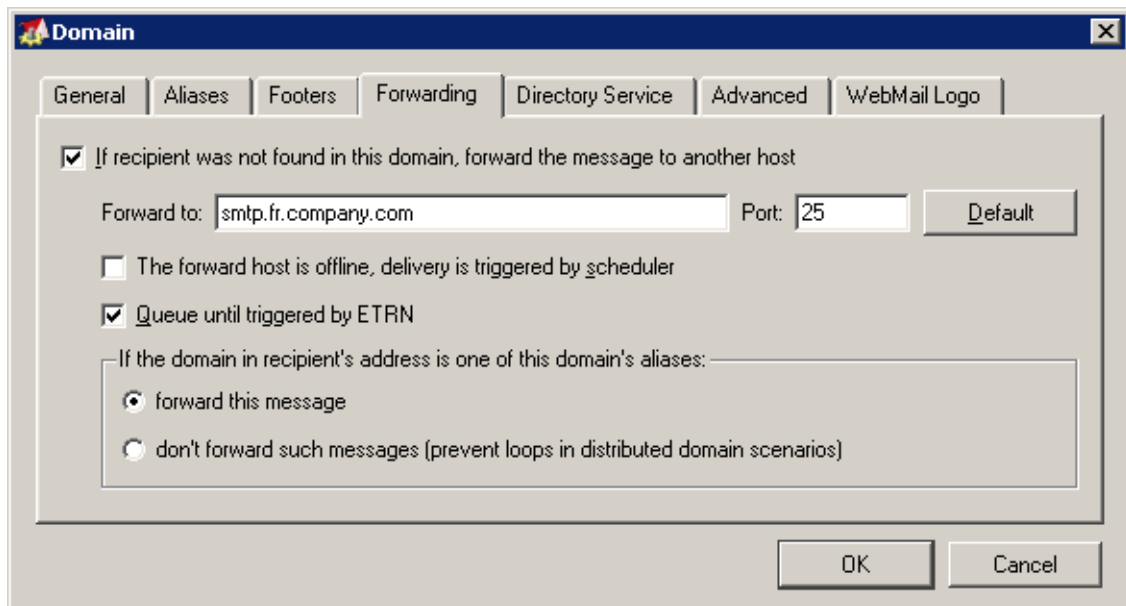


Figure 8.5 Domain settings — forwarding

Forward to server

DNS name or IP address of SMTP server to which all email messages for this domain will be forwarded.

Port

SMTP server port. The *Default* button sets the standard 25 port.

The forward host is Offline...

Under normal circumstances, *Kerio MailServer* sends email for the *Forward* domain to the specified SMTP server immediately. If the server has a dial-up connection to the Internet, then this may cause very often dialing and hanging up of the line (and high costs for the connection). Enabling this option will allow email for the *Forward* domains to be queued and delivered at scheduled times only (see chapter 10).

Queue until triggered by ETRN

Kerio MailServer keeps all messages addressed to this domain up to the moment when the ETRN command with this domain included as a parameter (for details, see chapter 16.1) is received before sending them to the defined SMTP server. This way *Kerio MailServer* can be used as a secondary server for a domain whose primary SMTP server is not permanently connected to the Internet.

If the domain...

Here you can define whether messages that contain one of domain's aliases in the recipient's address will be forwarded or not. The *Don't forward such messages* option disables loops in case that the particular recipient cannot be found at any server operating with this domain.

8.6 Setting of Directory Services

Kerio MailServer can also work with accounts or groups that are managed through an LDAP database (currently, *Microsoft Active Directory* and *Apple OpenDirectory* database — a database for Apple Macintosh — are supported). Using LDAP, user accounts can be managed from one location. This reduces possible errors and simplifies administration.

Example: A company uses a Windows 2000 domain with Active Directory as well as *Kerio MailServer*. A new employee was introduced to the company. This is what has been done until now:

1. A new account has been created in *Active Directory*.
2. The user has been imported to *Kerio MailServer* (or an account using the same name has been created and this name was verified by the Kerberos system).

If LDAP database is used, only the step 1 would be followed.

Note: *Kerio MailServer* allows internally managed user accounts (stored in LDAP database) to be added within the same email domain as Active Directory users. This can be helpful when creating an administrator account that will be available even when the directory server cannot be accessed.

In the *Directory service* tab, LDAP parameters can be defined.

Active Directory

To enable *Kerio MailServer* to cooperate fully with *Active Directory* (i.e. to enable the database to store all data about user accounts — see chapter 14.2), install *Kerio Active Directory Extensions* on the *Active Directory* server. For details see the chapter 28.

Map user accounts and groups...

Use this option to enable/disable cooperation with the LDAP database (if this option is inactive, only local accounts can be created in the domain).

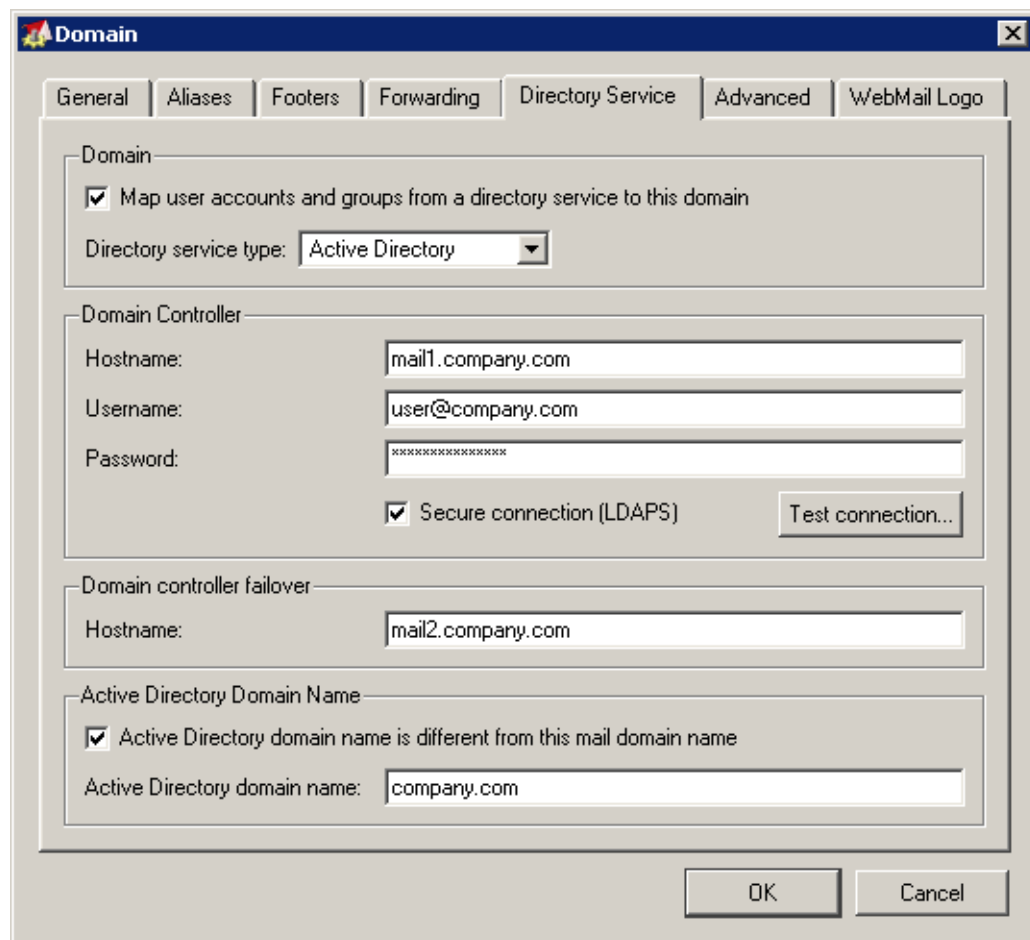


Figure 8.6 Domain settings — Active Directory

Type

Type of LDAP database that will be used by this domain (Active Directory).

Hostname

DNS name or IP address of the server where the LDAP database is running

For communication, the LDAP service uses port 389 as default (port 636 is used as default for the secured version). If a non-standard port is used for communication of *Kerio MailServer* with the LDAP database, it is necessary to add it to the DNS name or the IP address of the server (e.g. mail1.company.com:12345 or 212.100.12.5:12345).

Note: If the secured version of LDAP service is used for connection, it is necessary to enter also the DNS name to enable the SSL certificate's verification.

Username

Name of the user that has read rights for the LDAP database in the following form:
xxxxxx@company.com.

Password

Password of the user that have read rights for the LDAP database.

Secured connection (LDAPS)

Within the communication of the LDAP database with *Kerio MailServer*, sensitive data may be transmitted (such as user passwords). For this reason, it is recommended to secure such traffic by using SSL. Two conditions must be met to make the traffic function:

- To enable LDAPS in *Active Directory*, it is necessary to run a certification authority on the domain controller that is considered as trustworthy by *Kerio MailServer*.
- The LDAPS service in *Kerio MailServer* must be running (section *Configuration* → *Services*).

Warning: SSL encryption is demanding in respect of connection speed and processor operation. Especially when too many connections are established between the LDAP database and *Kerio MailServer* or a great amount of users are included in the LDAP database, the traffic might be slow. If the SSL encryption overloads the server, it is recommended to use the non-secured version of LDAP.

Domain controller failover

DNS name or IP address of the backup server with the same LDAP database.

Note: If the secured version of LDAP service is used for connection, it is necessary to enter also the DNS name to enable the SSL certificate's verification.

Active Directory Domain Name

If the domain name differs from the name defined in *Active Directory*, match this option and insert a corresponding name into the *Active Directory Domain Name* text field.

Click the *Test connection* button to check the defined parameters. The test is performed on the server name and address (if it is possible to establish a connection with the server), username and password (if authentication can be performed) and if *Kerio Active Directory Extensions* are installed on the server with *Active directory* (see chapter 28).

Note: Cooperation with the LDAP database that has been described above has nothing to do with the built-in LDAP server. The built-in LDAP server is used to access contact lists from mail clients (for details refer to the chapter 20). If *Kerio MailServer* is installed on the same computer as the *Active Directory*, it is necessary to avoid collisions by changing a port number for the LDAP service (*Configuration* → *Services*).

Apple Open Directory

To enable *Kerio MailServer* to cooperate fully with *Open Directory* (i.e. to enable the database to store all data about user accounts — see chapter 14.2), install the *Kerio Open Directory Extensions* on the *Open Directory Master* and all replica servers. For details see the chapter 29.

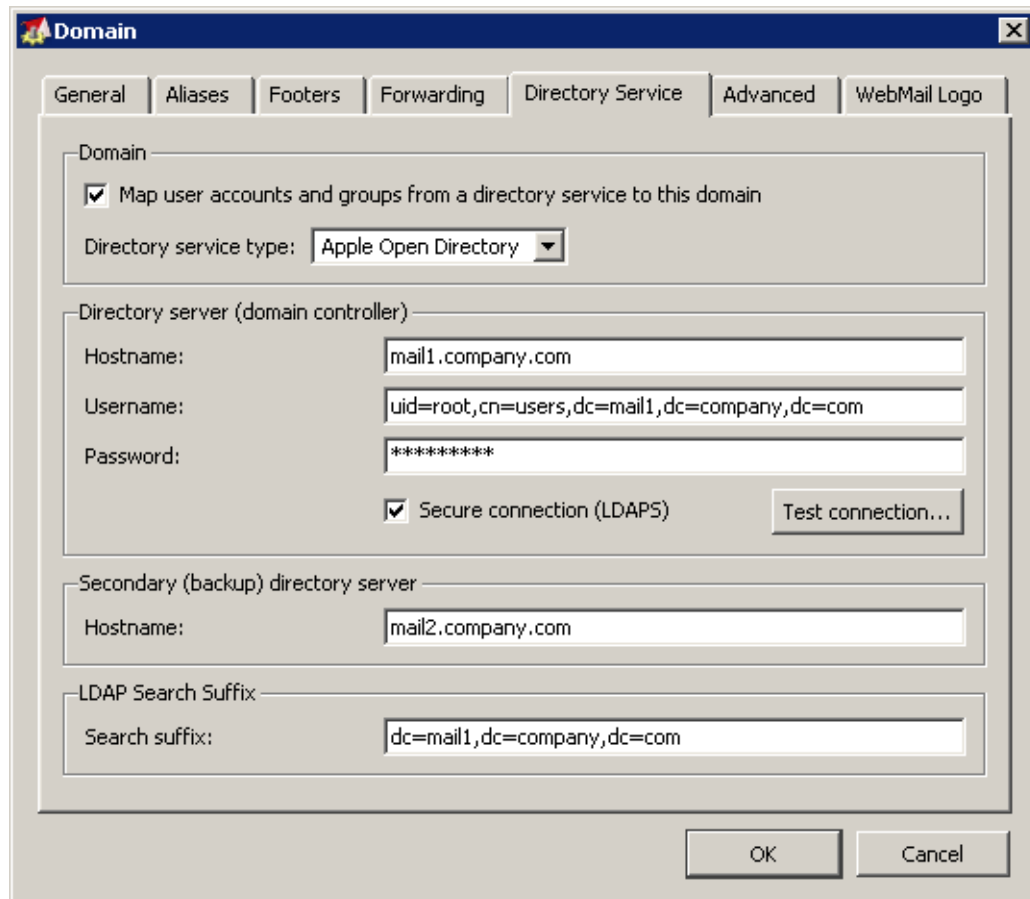


Figure 8.7 Domain settings — Apple Open Directory

Map user accounts and groups...

Use this option to enable/disable cooperation with the LDAP database (if this option is inactive, only local accounts can be created in the domain).

Type

Type of LDAP database that will be used by this domain (Apple Open Directory).

Hostname

DNS name or IP address of the server where the LDAP database is running

For communication, the LDAP service uses port 389 as default (port 636 is used as default for the secured version). If a non-standard port is used for commu-

nication of *Kerio MailServer* with the LDAP database, it is necessary to add it to the DNS name or the IP address of the server (e.g. `mail1.company.com:12345` or `212.100.12.5:12345`).

Note: If the secured version of LDAP service is used for connection, it is necessary to enter also the DNS name to enable the SSL certificate's verification.

Username

Name of the user that have read rights for the LDAP database, either of the root user or of the *Open Directory* administrator (admin for *Mac OS X 10.3* or *diradmin* for *Mac OS X 10.4*). In case that the administrator's username is used, it is necessary to make sure the user is an *OpenDirectory* Administrator, not just a local administrator on the *OpenDirectory* computer.

To connect to the *Apple OpenDirectory* database insert an appropriate username in the following form:

`uid=xxx,cn=xxx,dc=xxx`

- uid — username that you use to connect to the system.
- cn — name of the users container (typically the `users` file).
- dc — names of the domain and of all its subdomains (i.e. *mail.company.com* → `dc=mail,dc=company,dc=com`)

Password

Password of the user that have read rights for the LDAP database.

Secured connection (LDAPS)

Within the communication of the LDAP database with *Kerio MailServer*, sensitive data may be transmitted (such as user passwords). It is possible to secure the communication by using an SSL tunnel.

Warning: SSL encryption is demanding in respect of connection speed and processor operation. Especially when too many connection are established between the LDAP database and *Kerio MailServer* or when too many users are included in the LDAP database, the communication might get slow. If the SSL encryption overloads the server, it is recommended to use the non-secured version of LDAP.

Domain controller failover

DNS name or IP address of the backup server with the same LDAP database.

Note: If the secured version of LDAP service is used for connection, it is necessary to enter also the DNS name to enable the SSL certificate's verification.

LDAP search suffix

If the *Apple OpenDirectory* option is selected in the *Directory service type* entry, insert a suffix in the following form: `dc=subdomain,dc=domain`.

Click the *Test connection* button to check the defined parameters. The test is performed on the server name and address (if it is possible to establish a connection with the server) as well as the username and password (if authentication can be performed).

Note: Cooperation with the LDAP database that has been described above has nothing to do with the built-in LDAP server. The built-in LDAP server is used to access contact lists from mail clients (for details refer to the chapter 20). However, if the *MailServer* is installed on an *OpenDirectory* server the LDAP listening port in the *MailServer's Configuration* → *Services* must be changed to an alternate port to avoid a port conflict.

8.7 Advanced

In the *Advanced* tab you can set parameters for user authentication in the created domain:

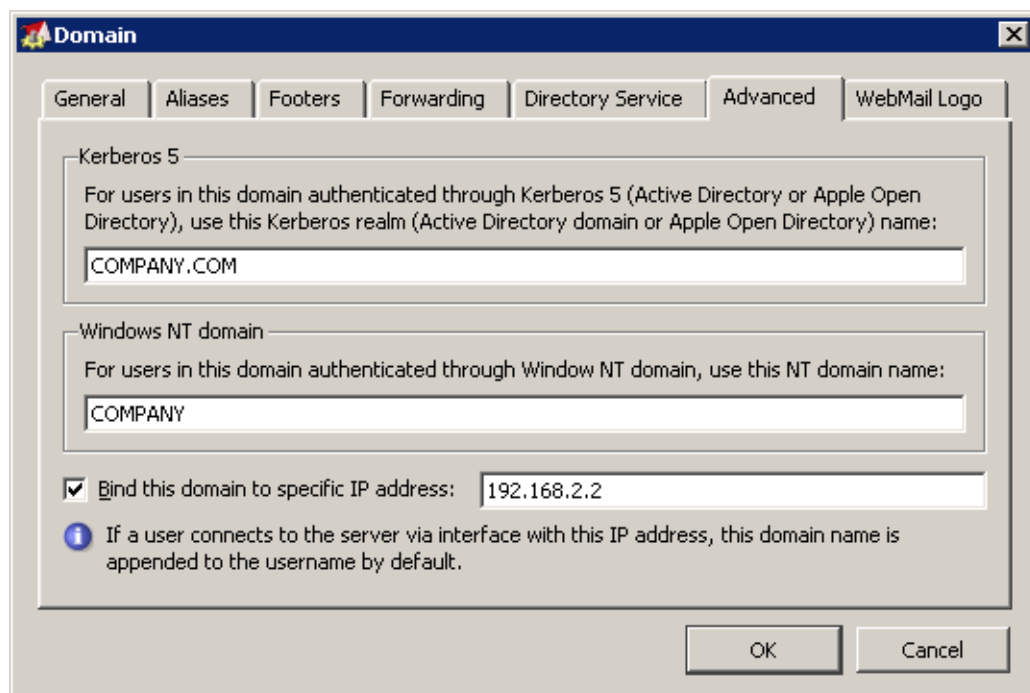


Figure 8.8 Domain settings — parameters for users authentication

Linux PAM

In the *Kerio Administration Console*, this option is available only in installations for Linux.

PAM (Pluggable Authentication Modules) are authentication modules that are able to authenticate the user from a specific domain (e.g. `company.com`) against the Linux server on which *Kerio MailServer* is running. Use this option to specify the name of the PAM service (configuration file) used for authentication of users in this

domain. The *Kerio MailServer* installation package includes a configuration file for the *keriomail* PAM service (it can be found under `/etc/pam.d/keriomail`). It is strongly recommended to use the file. Details about PAM service configuration can be found in the documentation to your Linux distribution.

Kerberos 5

Kerberos is a protocol used for authorization and authentication. It secures network traffic. *Kerio MailServer* uses it to authenticate users against the Kerberos server (e.g. in *Active Directory*)

In the appropriate item of the dialog box, specify the Kerberos system domain, where the users will be authenticated. The name of the domain must be in capital letters.

Note: If user accounts are saved in *Microsoft Active Directory* or *Apple OpenDirectory*, the *Active Directory* domain name or *Open Directory* realm name must be entered. If you use the *LDAP database* tab for *Active Directory* definition, this entry will be specified automatically.

Authentication settings for the individual platforms are described in chapter 30.

Windows NT domain

The NT domain in which all users will be authenticated. The computer which *Kerio MailServer* is running on must be a part of this domain.

Example:

For the `company.com` domain, the NT domain is `COMPANY`.

Bind this domain to specific IP address

Here you can enter IP address of the *Kerio MailServer* host's interface. Then, whenever a client uses this interface to connect to *Kerio MailServer*, they can log in using only their usernames without domain specification.

Example: *Kerio MailServer* host uses two interfaces. `192.168.1.10` is deployed to the network of the company called *Company* and `192.168.2.10` is deployed to the network of *AnotherCompany*. A new user account called `smith` is added to the `anothercompany.com` domain (this domain is not primary).

The `anothercompany.com` is bound to the IP address `192.168.2.10`. Users of this domain will not need to specify their domain name while connecting to *Kerio MailServer*.

Note: On the other hand, primary domain users have to specify their complete email addresses to connect to this interface.

Note: When creating a user account you can choose how the given user will be authenticated (see chapter 14.2). Different users can be authenticated using different methods in a single email domain.

8.8 Webmail Logo

Each domain in *Kerio MailServer* can have its own *Kerio WebMail* logo (for detailed information about the logo settings, see chapter 12.2).

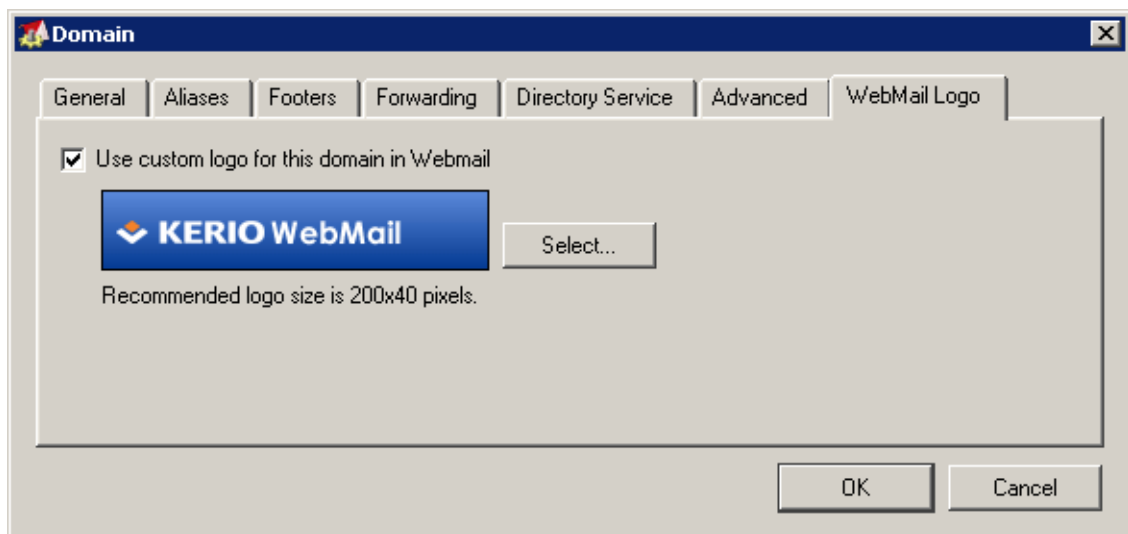


Figure 8.9 Domain settings — Kerio WebMail logo

The recommended parameters of the logo:

- Format: GIF
- Size: 200x40 pixels

Click *Select* to browse to the logo file.

Chapter 9

Internet Connection

To set the Internet connection type go to *Configuration* → *Internet Connection*.

9.1 Internet Connection

Kerio MailServer can either be installed on a computer that has a permanent connection to the Internet (leased line, wireless connection, cable modem, xDSL, etc.) or on a computer with a dial-up connection (analog or ISDN modem). Using the built-in scheduler you can set when the mailserver will automatically dial out a connection and perform a mail exchange.

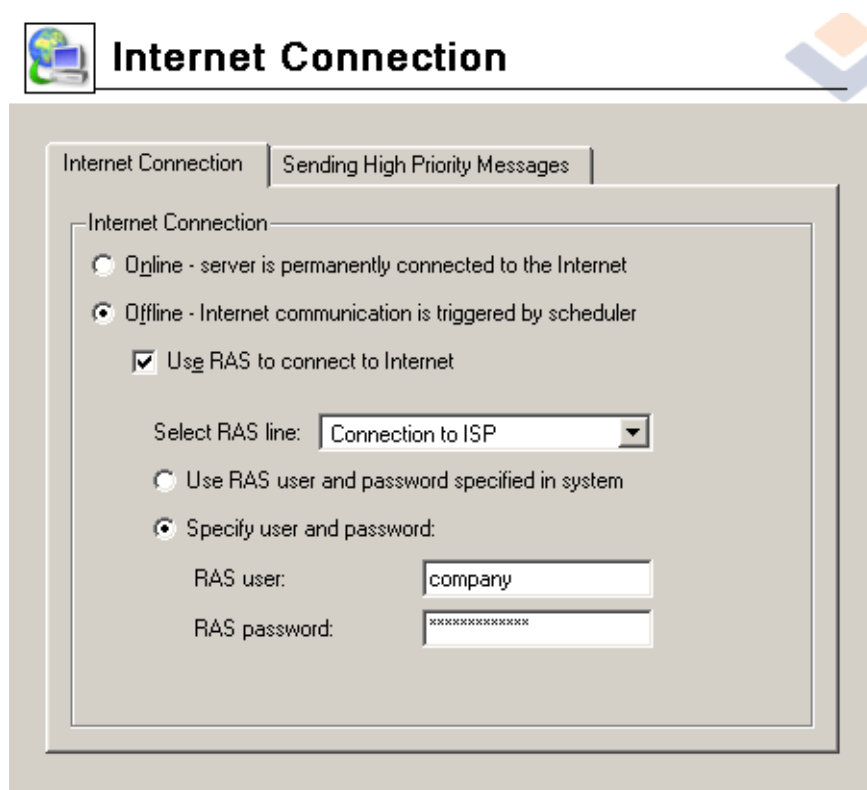


Figure 9.1 Internet Connection tab

Online

Kerio MailServer is permanently connected to the Internet. Outgoing mail is sent immediately.

Offline

The server is not permanently connected to the Internet. Outgoing mail is stored in a queue and is sent in time intervals set in the *Scheduler*.

Warning: Offline connection is available only in *MS Windows*. This option is not supported in *Linux* and *Mac OS* systems. That is the reason why the dialog is not available for these operating systems.

Check the *Use RAS to connect to Internet* option if you intend to dial the line within these time intervals. Dial-up entries created in Windows are offered in the *Select RAS line* menu. *Kerio MailServer* can use the username and the password which have been assigned to the appropriate dial-up connection by a user (the *Use user and password specified in system* option) or you can enter the username and password directly into this dialog (the *Specify user and password* option).

Warning: The dial-up connection must be created for all users within the system (this can be defined within definition of an appropriate connection).

Notes:

1. The *Offline* option can also be used when *Use RAS to Connect to Internet* is not checked. *Kerio MailServer* can run on a computer within a local network connected to the Internet by a dial-up line. In the *Online* mode frequent and uncontrollable requests for dial-out will be made. In the *Offline* mode *Kerio MailServer* will request a dial-out only in the time intervals set in the scheduler, which helps optimize connection costs.
2. *Kerio MailServer* uses the system telephone connection phone list (`rasphone.pbk`). No other phone list can be used.
3. The *Online* option does not switch off the scheduler. Although outgoing mail is sent immediately, the mailserver can retrieve messages from remote POP3 accounts in regular intervals. For details, see chapter [16.4](#).
4. Details about setting the scheduler can be found in chapter [10](#).

9.2 Sending High Priority Messages

If the server is not permanently connected to the Internet (it operates in the offline mode), you can set server to send messages immediately.

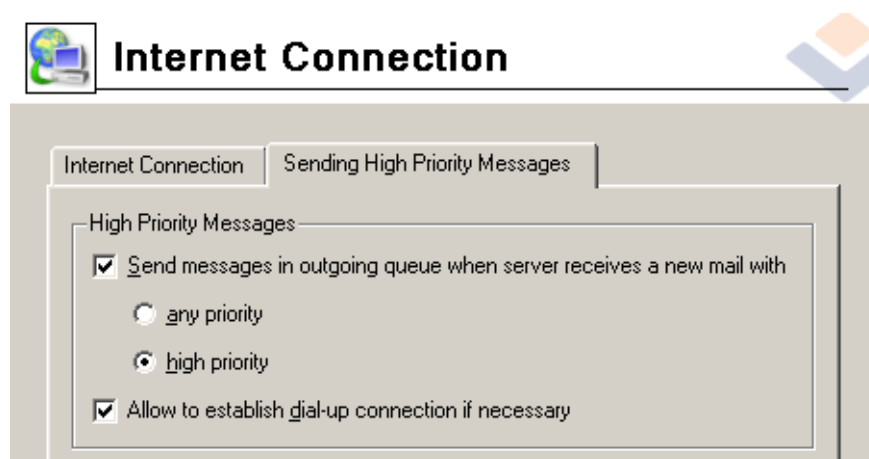


Figure 9.2 Sending High Priority Messages tab

Send messages in outgoing queue...

Use this option to send outgoing messages immediately. You can also define if all messages (messages with any priority) or only messages with high priority will be sent.

Allow to establish Dial-up connection...

Use this option to allow to establish dial-up connection automatically if the server receives an outgoing message that is to be sent.

Chapter 10

Scheduling

Kerio MailServer contains a built-in scheduler that can perform three types of actions:

Retrieve mail from remote POP3 mailboxes

— always if at least one POP3 account is defined

Send the ETRN command to defined servers

Use this option if at least one ETRN server is defined.

Send mail from the mail queue

— Use this option if the *Kerio MailServer* host is not permanently connected to the Internet . In all above cases, *Kerio Mail Server* can dial out a connection (if the settings indicate that the computer where *Kerio MailServer* is installed is not permanently connected to the Internet — see chapter 9).

10.1 Setting Up the Scheduler

The scheduler is set in the *Configuration* → *Scheduling* section.

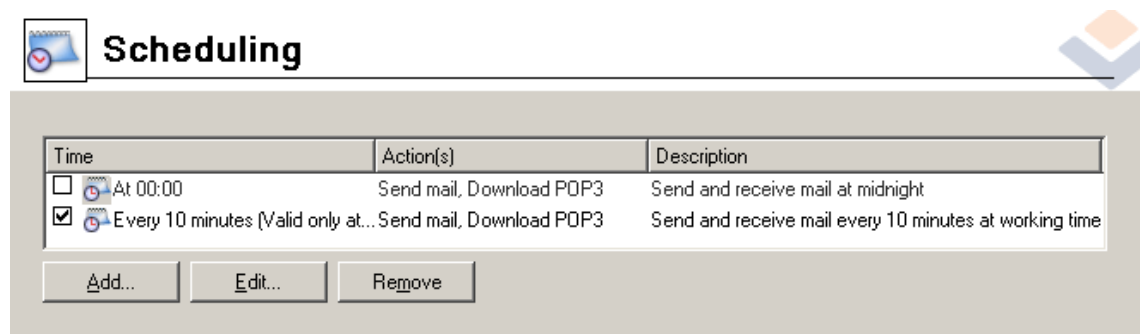


Figure 10.1 Scheduling

Use the *Add*, *Edit* and *Remove* buttons to add, edit or remove an item in the list of scheduled tasks. When adding a new item or editing an existing one a dialog window with the following parameters will be displayed:

Time condition — when the task is to be performed:

Every or At

Once in an interval (*Every*) or at a certain time (*At*). For example *Every 10 Minutes* or *At 12:00* every day.

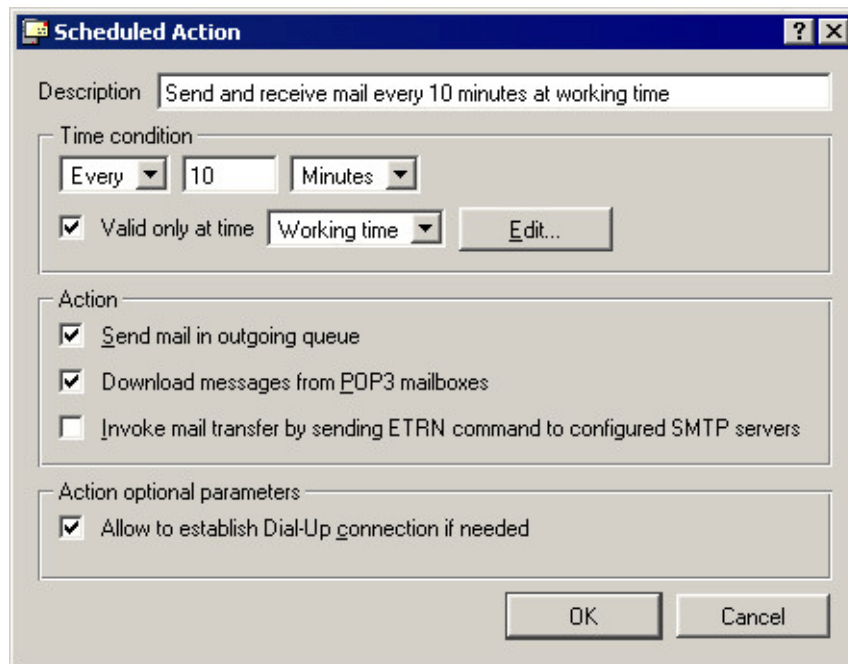


Figure 10.2 Scheduled Action

Valid only at time

Scheduled action is valid only in a selected time interval. All defined time intervals are displayed in the window; you can edit an interval (by clicking on *Edit*) or create a new one. See chapter 13.2 for details.

Action — what task is to be performed:

Send mail in outgoing queue

Send all mail in the queue (if you selected *Online* in the *Configuration* → *Internet Connection* section all mail is sent immediately and this option has no effect).

Download messages from POP3 mailboxes

Retrieve mail from remote POP3 mailboxes (only valid if at least one remote mailbox is defined in the *Configuration* → *POP3 Download* section). The same scheduling applies to all POP3 mailboxes.

Invoke mail transfer by sending ETRN...

Receive email using the ETRN command (only valid if there is at least one SMTP server defined in the *Configuration* → *ETRN Download* section). The same scheduling applies to all SMTP servers.

Optional parameters:

Allow to establish Dial-up connection...

Dials out a connection if the line is currently down. If this option is not ticked, the task will only be performed when the line is dialed out.

10.2 Optimal Scheduling

Optimal scheduling settings depend on the way the incoming mail is received and on the Internet connection type available to *Kerio MailServer*.

- If the computer with *Kerio MailServer* is permanently connected to the Internet (*On-line*) and all incoming email is received using the SMTP protocol (MX records for all local domains point to the computer where *Kerio MailServer* is installed and there is no remote POP3 account or ETRN server) there is no need to set up any scheduling.
- If a permanent connection to the Internet is available and at least one POP3 account is defined or mail reception is conducted using the ETRN command, scheduling must be set.

In this case intervals between individual actions can be quite short (e.g. 5 minutes) as the number of connections does not influence the cost and there is no need to consider the time needed for dialing.

- If *Kerio MailServer* is connected to the Internet via a dial-up line, it is not permanently accessible from the Internet and mail reception is conducted using the ETRN command or from remote POP3 mailboxes. In this case it is necessary to set up scheduling to enable *Kerio MailServer* to dial out, send mail from the queue and receive email when needed.

In all of the above examples where scheduling is recommended, all options in the *Action* field can be selected (*Send mail in outgoing queue* and *Invoke mail transfer by sending ETRN command to configured SMTP servers*). If the mail queue is empty or no POP3 account is defined, *Kerio MailServer* will automatically move on to the next task.

Chapter 11

SSL certificate

The principle behind secure services in *Kerio MailServer* (services encrypted by SSL — e.g. HTTPS, IMAPS, POP3S, etc.) is that all communication between the client and the server is encrypted to protect it from tapping and to prevent it from misuse of transmitted information. The SSL encryption protocol used for this purpose uses an asymmetric cipher first to exchange a symmetric key.

The asymmetric cipher uses two keys: a public one for encrypting and a private one for decrypting. As their names suggest, the public (encrypting) key is available to anyone wishing to establish a connection with the server, whereas the private (decrypting) key is available only to the server and must remain secret. The client, however, also needs to be able to identify the server (to find out if it is truly the server and not an impostor). For this purpose there is a certificate, which contains the public server key, the server name, expiration date and other details. To ensure the authenticity of the certificate it must be certified and signed by a third party, the certification authority.

Communication between the client and server then follows this scheme: the client generates a symmetric key and encrypts it with the public server key (obtained from the server certificate). The server decrypts it with its private key (kept solely by the server). Thus the symmetric key is known only to the server and client.

Note: To secure *Kerio MailServer* as much as possible, allow only SSL-secured traffic. This can be set either by stopping all unencrypted services (see chapter 7) or by setting appropriate security policy (refer to chapter 16.6). Once the server is configured, it is necessary to install a certificate (even a self-signed one) on clients of all users using *Kerio MailServer's* services.

11.1 Kerio MailServer Certificate

To find out how these principles work in practice, look at *Secure HTTP*. Web browsers can display certificate information, as opposed to *Secure POP3* or *Secure IMAP*, where such information will not be revealed.

When *Kerio MailServer* (version 6.0 and above) is run for the first time, it generates the self-signed certificate automatically. It is saved in the `server.crt` file in the `sslcert` folder where *Kerio MailServer* is installed. The second file in this directory, `server.key`, contains the server's private key.

If you attempt to access the *Secure HTTP* service immediately after installing *Kerio MailServer* a security warning will be displayed with the following information (depending on your browser, name of the computer, etc.):

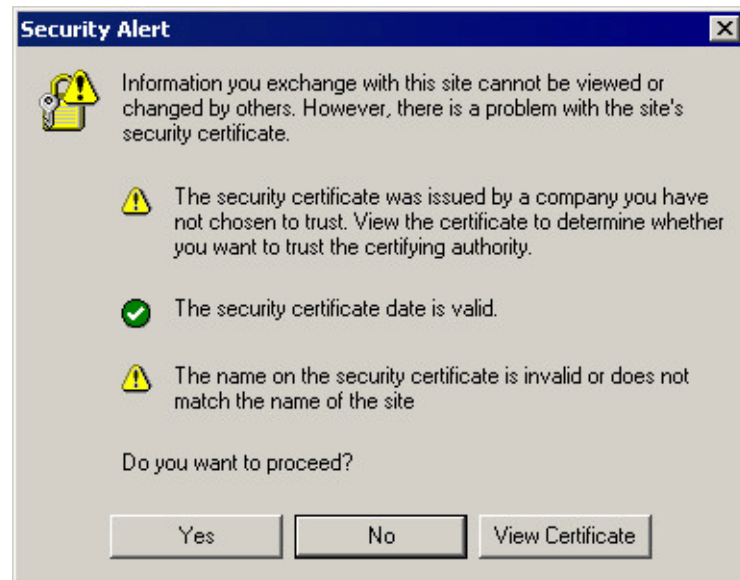


Figure 11.1 Security Alert

- The certificate was not issued by a company defined as trustworthy in your configuration. This is caused by the fact that the certificate is self-signed. This warning will not be displayed if you install the certificate (you can do this because you know the certificate's origin).
- The certificate date is valid (the certificate is valid for a certain limited period, usually 1-2 years).
- The name of the certificate does not correspond with the name of the server. The certificate is issued for a certain server name (e.g. `mail.ourcompany.com`), which you must also use in the client (this certificate has been issued for a fictitious name `keriomail`).

This implies that you need your own certificate!

You can obtain your own certificate, which verifies your server's identity, by two means.

You can create your own self-signed certificate (i.e. you will sign it). This can be done in the *Configuration/SSL Certificates* section where the current server certificate is displayed.

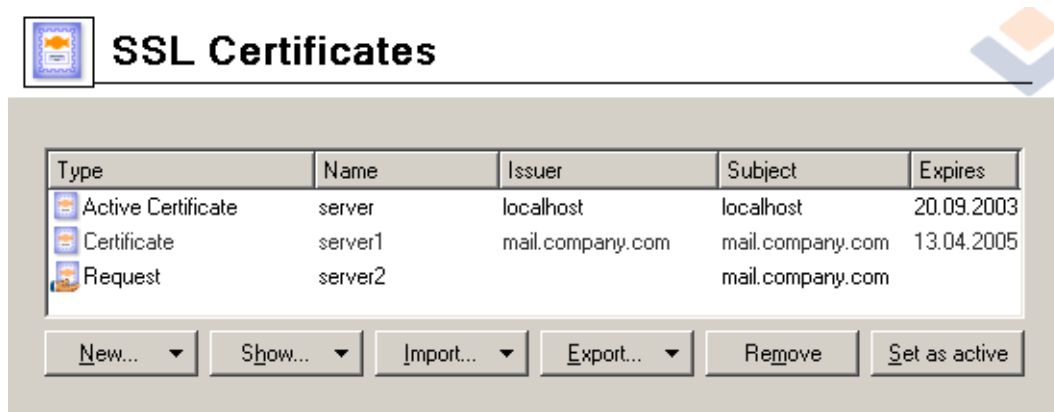


Figure 11.2 SSL Certificates

New...

Click on *New* to specify information about your server and your company. When confirmed, the `server.crt` and `server.key` files are created under `sslcert`.

The certificate you create will be original and will be issued to your company by your company (self-signed certificate). This certificate ensures security for your clients as it explicitly shows the identity of your server. The clients will be notified by their web browsers that the certification authority is not trustworthy. However, since they know who created the certificate and for what purpose, they can install it. Secure communication is then ensured for them and no warning will be displayed again because your certificate has all it needs.

If you wish to obtain a “full” certificate you must contact a public certification authority (e.g. Verisign, Thawte, SecureSign, SecureNet, Microsoft Authenticode, etc.). The process of certification is quite complex and requires a certain expertise. *Kerio MailServer* enables certification request that can be exported and the file can be delivered to a certification authority.

Attention: A new certificate will be used the next time *Kerio MailServer Engine* is started. If you wish to use it immediately, stop the *Engine* and then start it again. The *New* button can be used to create a new certificate (the *New certificate* option) or to demand on a new certificate (*New certificate request*). You will be asked to specify entries in the *Generate Certificate* dialog. The *Hostname* and *Country* entries are required fields.

- *Hostname* — name of the host on which *Kerio MailServer* is running.
- *Organization Name* — name of your organization.



The 'Generate Certificate' dialog box contains the following fields and controls:

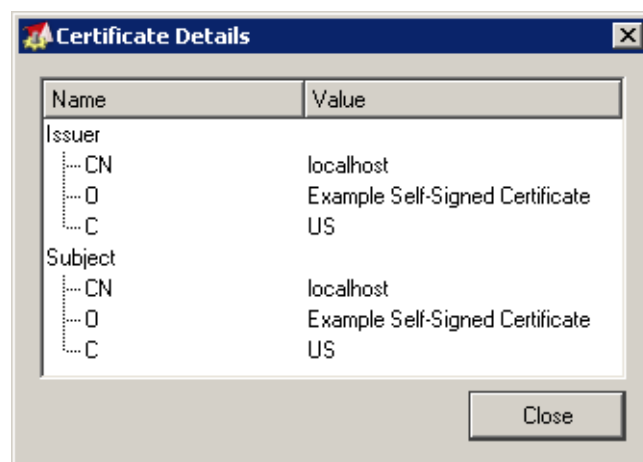
- Attributes** section:
 - Hostname***: mail.company.com
 - Organization Name**: Company
 - Organization Unit**: (empty)
 - City**: Our City
 - State or Province**: California
 - Country***: United States (dropdown menu)
- Footer text: The required fields are marked with an asterisk (*).
- OK** and **Cancel** buttons.

Figure 11.3 Certificate Creation

- *Organization Unit* — will be used only if the organization consists of more than one unit.
- *City* — city where the organization's office is located.
- *State or Province* — state or province where your organization has its office(s).
- *Country* — this entry is required.

View Certificate

Select a certificate and click on the *View Certificate* button to get details about the selection.



The 'Certificate Details' dialog box displays the following information in a table:

Name	Value
Issuer	
...CN	localhost
...O	Example Self-Signed Certificate
...C	US
Subject	
...CN	localhost
...O	Example Self-Signed Certificate
...C	US

A **Close** button is located at the bottom right of the dialog.

Figure 11.4 Certificate Details

Import...

Use this button to import a new certificate, regardless if certified by a certification authority or not.

Export...

Use this button to export an active certificate, a certification request or a private key. Using this option you can send an exported certificate request to a certification authority.

Remove

Using this button you can remove a selection (a certificate or a certification request).

Set as active

Use this button to set the selected certificate as active.

Chapter 12

Kerio WebMail parameters

Detailed information about *Kerio WebMail* is provided in a standalone document *Kerio MailServer 6.1, Kerio WebMail*. This manual is available at *Kerio Technologies* website (<http://www.kerio.com/kms>). The document includes guidance for setting access to email by WAP.

12.1 Skins

Kerio WebMail contains a couple of default skins (skin = *Kerio WebMail*) appearance). These skins are stored in `\Kerio\MailServer\webmail\default\skins` directory.

`Kerio\MailServer\webmail\default\skins`

Skins consist of cascading stylesheets (CSS) and images. Cascading stylesheets (CSS) enable users to customize the appearance of web pages (colors, fonts, object offset, etc.). If a user is able to work with cascading stylesheets and images, he/she can customize the most of the *Kerio WebMail* interface. Users can either edit the default skins or create one's own. The new skin must be stored in `\Kerio\MailServer\webmail\default\skins\MySkin` directory.

`Kerio\MailServer\webmail\default\skins\xyz`

where xyz stands for the name of the new skin.

12.2 Logo

Page headers show the *Kerio Technologies* logo. You can replace it with your own logo or any other image.

The logo can be changed either globally (it applies to all domains in *Kerio MailServer*) or individually for each domain (since *Kerio MailServer 6.1*). To change the logo globally, use the *Logo* tab in the *Advanced options* (for detailed information, see chapter 16.6). The logos for the individual domains are set in the *Domains* section (see chapter 8.8). If both domain as well as individual logos are set in *Kerio Administration Console*, the logos for the individual domains will be of higher priority.

The administration console can be used for changing the logo only if the *Kerio WebMail* interface uses the default skin. If any other skin is used in *Kerio WebMail*, the new logo

file must be copied directly into the skin folder and the file must be renamed as shown in the following example (the xyz is the name of the appropriate skin):

Kerio\MailServer\webmail\default\skins\xyz\logo_my.domain.gif (if different logos for individual domains are used)

Kerio\MailServer\webmail\default\skins\xyz\logo.gif (if one global logo is used)

If there is one of the following two files in the skin folder (logo_my.domain.gif, logo.gif), none of the global logos will be used. If the skin currently in use contains both the domain logos as well as the individual ones, the domain logos will be used by default.

12.3 Language

All texts displayed in the *Kerio WebMail* interface are saved in separate XML localization files. This file has to be created for each language that the user intends to use.

Localization files are stored in subdirectory webmail/translations (in the directory where *Kerio MailServer* is installed). UTF-8 is required for file encoding. The name of each file is created from the language abbreviation (e.g. de for German, en for English etc.) and the suffix .def. Another language can be added anytime by creating the relevant definition file. The administrator of *Kerio MailServer* can also create a custom language version by simply copying one of the definition files in a file with a new name and translating the texts contained within.

XML format is delimited by <translation> tag. The individual rows must have the following form:

```
<text id="head-user">User</text>
```

Procedure for creating a custom localization file for a new language:

1. Copy the localization file from the source language (from which we will translate) to the file named according to the new language.
2. Translate all texts on individual lines in the file.

A new localization file will be loaded during the next start of the *MailServer Engine* service.

Spellcheck and dictionaries

The spellcheck in *Kerio WebMail* is based on comparing the phrases with the dictionary, and it is therefore available only for the language versions available in the folder where *Kerio MailServer* is installed. The default language versions for the spellcheck dictionaries are English and Czech. The other language versions can be copied in the `Kerio\MailServer\myspell` folder. In order for the dictionaries to work properly, they must meet the `myspell` standard. They can be downloaded from the Internet for free. Use the settings dialog in *Kerio WebMail* to switch to a different language version.

13.1 IP Address Groups

IP address groups help easily define who has access to certain services (e.g. remote administration, anti-spam, etc.). When setting access rights a group name is used. The group itself can contain any combination of computers (IP addresses), IP address ranges, subnets or other groups.

Creating and Editing IP Address Groups

You can define IP address groups in the *Configuration → Definitions → IP Address Groups* section.

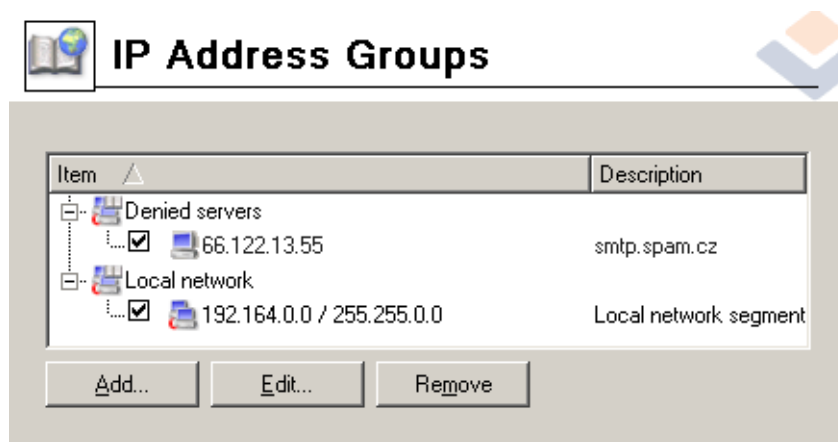


Figure 13.1 IP Address Groups

Click on *Add* to add a new group (or an item to an existing group) and use *Edit* or *Delete* to edit or delete a selected group or item.

The following dialog window is displayed when you click on the *Add* button:

Name

The name of the group. You can enter a new name (create a new group) or enter or select an existing one — this adds the new item to an existing group

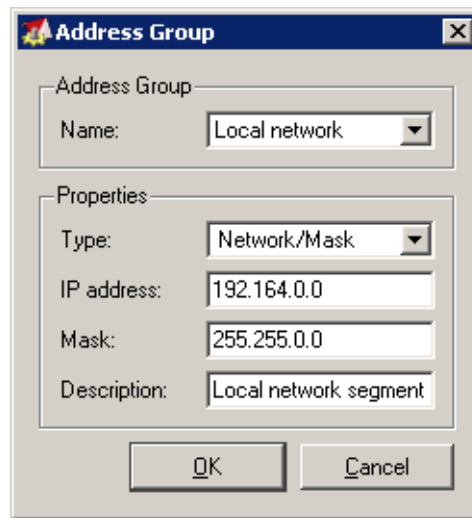


Figure 13.2 IP Address Groups Creation

Type

The type of new item. Options: one IP address (*Host*), range of IP addresses (*Network/Range*), subnet with a corresponding mask (*Network/Mask*) or a different IP address group (*Address group*). This implies that address groups are cascable.

IP address, Mask...

Parameters of new item (dependent on selected type).

Description

Commentary for the IP address group. This helps guide the administrator.

13.2 Time Intervals

Time intervals in *Kerio MailServer* restrict all scheduled tasks to certain time ranges. They are not intervals in the true meaning of the word. They are a group containing any number of single or repeating time ranges. Time intervals can be defined in the *Configuration* → *Definitions* → *Time Ranges* section.

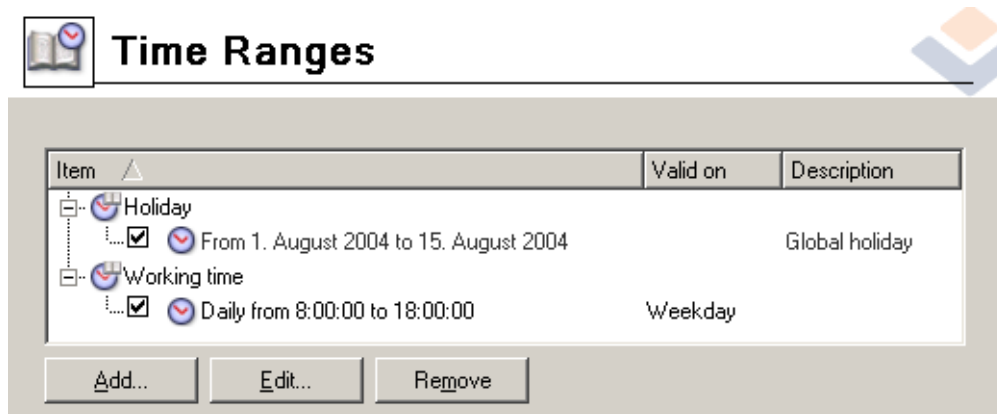


Figure 13.3 Time Intervals

Validity of Time Intervals

When defining a time interval three types of time ranges (subintervals) can be used:

Absolute

- interval has explicit start and end dates, it does not repeat

Weekly

- interval repeats every week (on selected days)

Daily

- interval repeats every day (in selected hours)

If a certain time interval consists of multiple ranges of different types, it is valid in the time defined by the intersection of absolute ranges with the union of daily and weekly ranges. In symbols:

$$(d1 \mid d2 \mid w1 \mid w2) \& (a1 \mid a2)$$

where

d1, d2 — daily ranges

w1, w2 — weekly ranges

a1, a2 — absolute ranges

Defining Time Intervals

You can create, edit or delete time intervals in the *Configuration* → *Definitions* → *Time Ranges* section.

Clicking on the *Add* button will display the following dialog window:

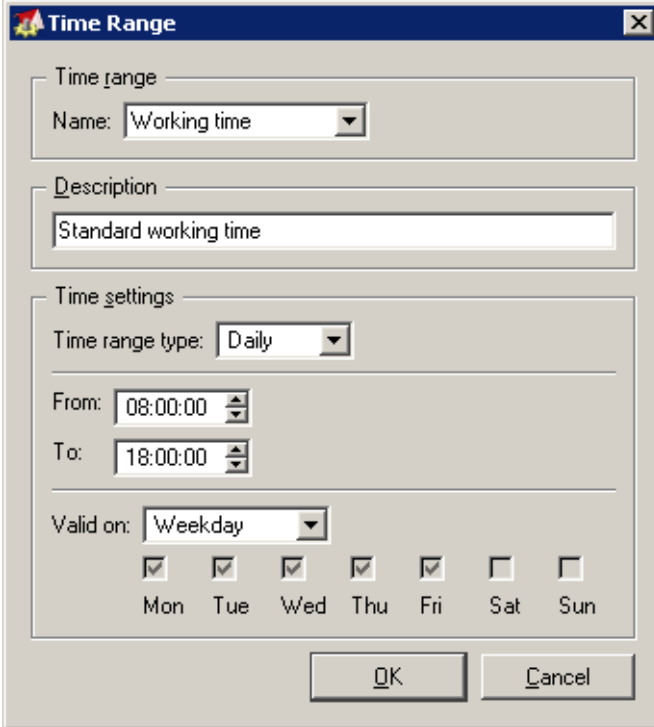


Figure 13.4 Defining Time Interval

Name

Name (identification) of the time interval. You can enter a new name (create a new interval) or select an existing one and add a new item to it.

Description

A text description (for informative purposes only).

Time Interval Type

The type of interval: Daily, Weekly or Absolute.

From, To

The beginning and the end of the time range. Here you can enter the start and end time, a day of the week or a date (depending on the interval type).

Valid at days

The day of the week on which the interval will be valid. You can select certain days (Selected days) or use one of the pre-set items (Everyday, Weekday, Weekend).

Time intervals cannot be cascaded.

13.3 Setting Remote Administration

If you wish to administer *Kerio MailServer* from a different computer than the one on which it is installed, you need to enable remote administration. You can set remote administration in the *Configuration* → *Remote Administration* section.

Remote administration can be enabled for *Kerio Administration Console* and/or for *KMS Web Administration*:

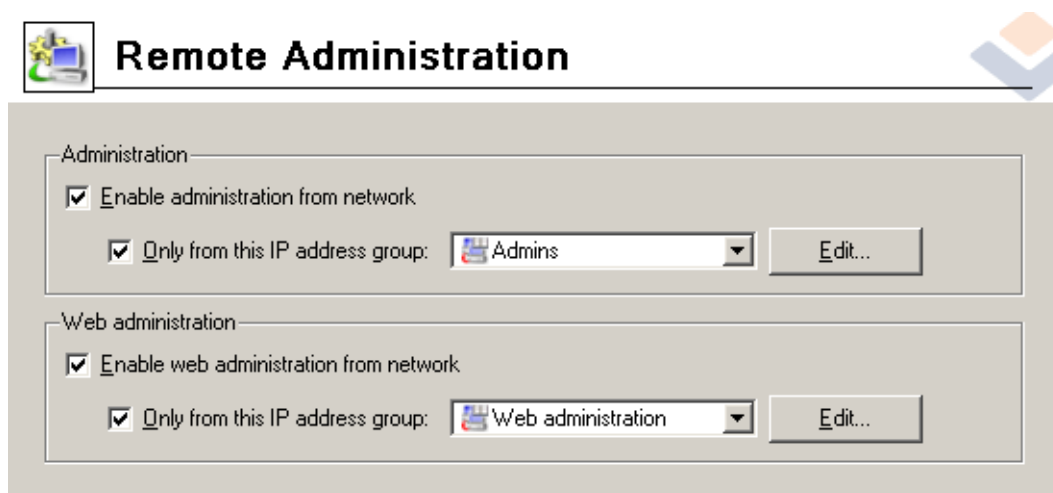


Figure 13.5 Remote Administration

Remote administration of Kerio MailServer

The port used for communication between *Kerio Administration Console* and *Kerio MailServer Engine* is 44337 (both TCP and UDP protocols are used).

Enable remote administration from network

Enables remote administration (if this option is not selected, you can only administer *Kerio MailServer* from the computer it is installed on).

Only from this IP address group

The traffic between *Kerio MailServer* and the *Kerio Administration Console* is protected by SSL encryption. As a result, remote administration is secure and the data transmitted cannot be tapped and misused. Access to the administration should be always allowed against a valid password only (it is not recommended to use blank passwords for administration accounts).

Here you can choose the IP address group from which remote administration will be allowed. Click *Edit* to modify the group or to create a new one (the same dialog is used in *Configuration* → *Definition* → *IP Groups* — see chapter 13.1).

Web administration of users, groups and aliases

Enable web administration from network

This option enables administration via the Web interface. If disabled, it is not possible to access the interface (for more information on web administration, refer to chapter 27).

Only from this IP address group

To even increase security, remote administration can be enabled only for exclusive IP addresses. In the menu, select the group of IP addresses, from which web administration will be enabled. Click *Edit* to modify the group or to create a new one (the same dialog is used in *Configuration* → *Definition* → *IP Groups* — see chapter 13.1).

Chapter 14

User accounts

User accounts in *Kerio MailServer* represent physical email boxes. Users access mailboxes through user name and password authentication. Since *Kerio MailServer* can serve several independent domains, the user accounts are not valid globally but are only valid for a particular domain. This implies that domains must be defined before user accounts are created (for details, see chapter 8).

User accounts can be located as follows:

1. locally — user mailboxes are located in *Kerio MailServer* and any management of user accounts is performed in *Kerio MailServer* (see chapter 14.2).
2. in the LDAP database — accounts are just mapped to *Kerio MailServer*. Mapping of user accounts is available from the *Active Directory* and/or from the *Apple Open Directory* (refer to chapter 8.6).

User accounts can be simply imported to *Kerio MailServer* from another user database, as follows:

- import from the Novell eDirectory (more information in chapter 14.9),
- import from the NT domain (see chapter 14.9),
- import from the Active Directory domain (refer to chapter 14.9),
- import from a text file (for detailed information, read the corresponding article in the knowledge base at <http://support.kerio.com/>).

14.1 Administrator account

Apart from mailbox access, a user account can also be used for access to *Kerio MailServer* administration, provided that the user has such rights. The basic administrator account is created during the installation process. It has the same properties as other user accounts and can be deleted by any user with read/write access rights.

The default administration account can create and manage public folders.

The default administrator account also manages archive folders (if archiving is enabled — see chapter 19.2). Any message which passed through *Kerio MailServer* can be found in the archive.

Administrator can allow other users to access an archive folder (for details, see chapter 31.10). However, since messages of all users are archived, only a confidential administrator (or a tiny group of confidential persons) should be allowed to access these folders.

Warning: Passwords for those user accounts that have full administration rights should be kept close so that they cannot be misused by an unauthorized user.

14.2 Creating a user account

New user accounts can be defined in the *Domain Settings* → *Users* section.

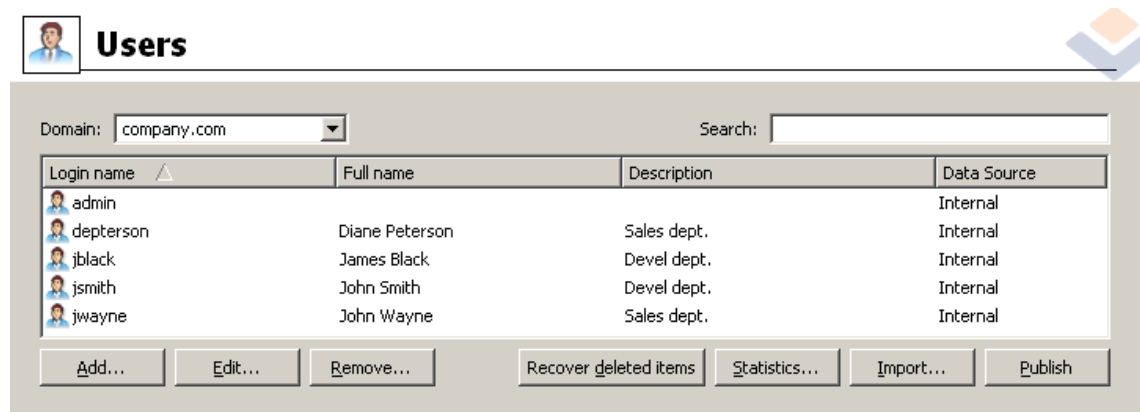


Figure 14.1 User accounts

First, choose a local domain in the *Domain* field, in which the accounts will be defined. Each domain may include local accounts as well as accounts saved in a directory service (e.g. Microsoft Active Directory). Both can be displayed in the *Users* section in the *Kerio Administration Console*. However, only local accounts can be added (accounts for directory services must be created with the respective administration tools, e.g. *Active Directory Users and Computers*). Some of the features of accounts within a directory service can be edited.

Warning: If an account mapped from the directory service is deleted in the administration console, the account is disabled in *Kerio MailServer*.

Note: The roles of each column of this window will be better understood through the following descriptions. The only exception — the *Data source* column — displays account types:

- *Internal* — the account is stored in the internal user database
- *LDAP* — the account is saved in a directory service (*Active Directory*, *Open Directory*)

Click on the *Add* button to open a guide to create a new user account. If the domain is configured to be used with directory services (see chapter 8.6), a dialog where you can define whether you would like to activate users from a directory service or create a new local account will be displayed.

If a user is activated, a user account is saved into the directory service. Since the activation it can be used by *Kerio MailServer*. All events and information will be saved into the directory service.

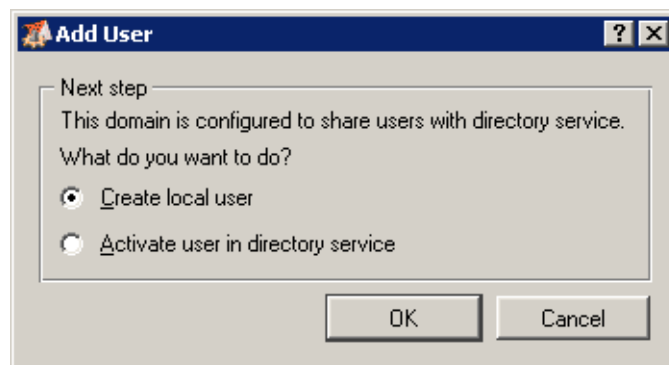


Figure 14.2 Activate user in directory service

If the *Activate user in directory service* option is selected, a dialog with user list of the LDAP database used by *Kerio MailServer* will be opened. Select appropriate users and confirm the selection. The buttons bottom left make user selection more comfortable. *Select all* — this button selects all users. The *Unselect all* option clears any selection.

The following guide shows how local user accounts can be defined.

Step 1 — Template

The first step is shown only in case at least one template is created. To create the new user mailbox template, select *Definition* → *User templates*. The template is useful especially for creating multiple user accounts at once that have some parameters in common (e.g. authentication type, quotas, etc.). When all these common parameters are entered in a template, it can save a lot of time.

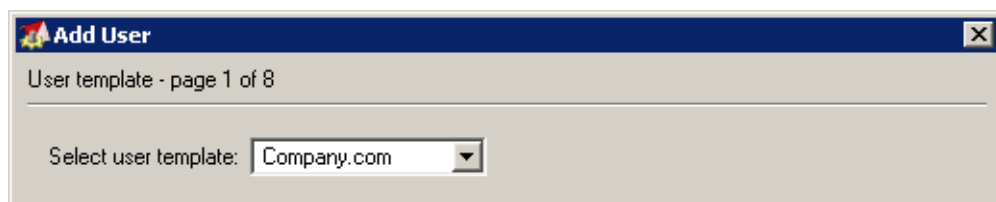


Figure 14.3 New user addition — a template

For information about creation of a new template, refer to chapter [14.11](#).

Step 2 — Basic data

Login name

User login name (note: the domain must be the local primary domain; otherwise enter the full email address, e.g. `user@anothercompany.com`, not only `user`).

The username is not case-sensitive.

Warning: The login name must not contain national characters and some of the special characters (see the *Allowed and prohibited characters in the user name*)

Examples of correct names:

wayne, john.wayne, ing.john.wayne, john_wayne, wayne, john---wayne, john_paul-wayne, john_-_wayne-

Examples of incorrect names:

john..wayne, john...wayne, john.wa.yne, .wayne, wayne.

Full Name

A full name of the user (usually first name and surname). This option is required, if the user data from this account are to be exported to a public contacts folder.

Add User

General - page 2 of 8

Login name:

Full name:

Description:

Authentication:

Password:

Confirm password:

WAP service

☒ Enable access to WAP service

Enter authorization PIN:

☐ Account is disabled

☒ Enable a default spam filter (move messages marked as spam to the Junk E-mail folder)

☒ Store password in highly secure SHA format (recommended)

This user cannot be authentication using APOP, CRAM-MD5 and DIGEST-MD5

< Back Next > Finish Cancel

Figure 14.4 New user addition — basic data

Character	Allowed	Character	Prohibited
a-z	allowed	/	prohibited
0-9	allowed	\	prohibited
A-Z	allowed	.	prohibited
.	allowed when not at the beginning and/or the end of the string and when there are not two dots next to each other	.	prohibited when at the beginning and/or at the end of the string
-	allowed	*	prohibited
_	allowed		

Table 14.1 Allowed and prohibited characters in the user name

Description

User description (e.g. a position in a company). The *Description* entry is for infor-

matory purposes only. They can contain any type of information or they can be left blank.

Authentication

Possible authentication methods:

- *Internal user database*
Users are only authenticated within *Kerio MailServer*. In this case a password must be entered in the *Password* and *Confirm Password* fields (the user can then change his/her password in the *Kerio WebMail* interface).
Warning: Passwords may contain printable symbols only (letters, numbers, punctuation marks). Password is case-sensitive.
- *Windows NT domain*
Users are authenticated in a Windows NT domain. The NT domain name must be entered in the email domain properties (*Windows NT domain* in the *Advanced* tab). This authentication method can be used only if *Kerio MailServer* is running on Windows 2000/XP/2003. For details, see chapter 8.7.
- *Kerberos 5*
Users are authenticated in the Kerberos 5 authentication system..
- *PAM service*
Authentication using the PAM service (Pluggable Authentication Module), available only in the Linux operating system.
- *Apple Open Directory*
Authentication against *Apple Open Directory* database (only for mailservers installed on a *Macintosh*). The option can be selected only if the user is mapped from *Apple Open Directory*.

Password / Confirm Password

Only the local user password can be entered or changed. We strongly recommend to change the password immediately after the account is created.

If the password contains special (national) characters, users of some mail clients will not be able to log in to *Kerio MailServer*. It is therefore recommend to use only ASCII characters for passwords.

WAP Service

Kerio MailServer enables access to email using a cellular telephone from the WAP protocol. This interface is called *WAPmail* (it uses the same ports as *HTTP* and *Secure HTTP* services).

To enable the service, check *Enable access to WAP service* and enter at least 4 digits (max. 32 characters) to specify your PIN numeric code. (including from 4 to 32 characters). This code will be used for authentication to the service.

Warning: Since *Kerio MailServer* 6.0.5, the PIN code is stored in the new SHA format — see *Store password in high secure SHA format (recommended)*. For this

reason, the original PIN will not work if downgraded to a previous version of *Kerio MailServer* and must be changed.

Enable a default spam filter ...

Upon creating a new user account, check this option to set the antispam rule. All incoming emails marked as spam will be automatically moved to the *Junk mail* folder. The rule can be set up only during the process of user account creation. For more information about the filter and rules for incoming messages, see chapter 31.11.

Warning: It is not recommended to create this rule when the user accesses emails via POP3. In such case, only the *INBOX* folder is downloaded to the local client and the user is not able to check if the emails moved to the *Spam* folder are really spam emails.

Store password in high secure SHA format (recommended)

By default, user passwords are encrypted by DES. The *Store password in highly secure SHA format* allows for a more secure encryption (SHA string). This option has one disadvantage — some methods of *Kerio MailServer* access authentication (APOP, CRAM-MD5 and Digest-MD5) cannot be applied. The only methods available for this option are LOGIN and PLAIN (it is highly recommended to use only SSL connection for authentication).

If this option is enabled, it is necessary to change the user password. This can be done either by administrator or the user (e.g. by *Kerio WebMail*).

Warning: Passwords saved in SHA are supported by *Kerio MailServer 6.0.5* and later. If a configuration with SHA passwords is applied to an older version of *Kerio MailServer*, the authentication will not function.

Account is disabled

Temporary blocking of the account so that you do not have to remove it.

Step 3 — Mail addresses

In this step, all required email addresses of the user can be defined. The other addresses are called aliases. The other addresses are called *aliases*. These can be defined either during the user definition or in *Domain Settings/Aliases*. We recommend to use the first alternative — it is easier and the aliases are available through *Active Directory*.

Note: If user accounts are maintained in *Active Directory* (see chapter 8.6), their aliases can be defined in *Active Directory Users and Computers*. Global aliases (in *Domain Settings* → *Aliases*) cannot be defined this way.

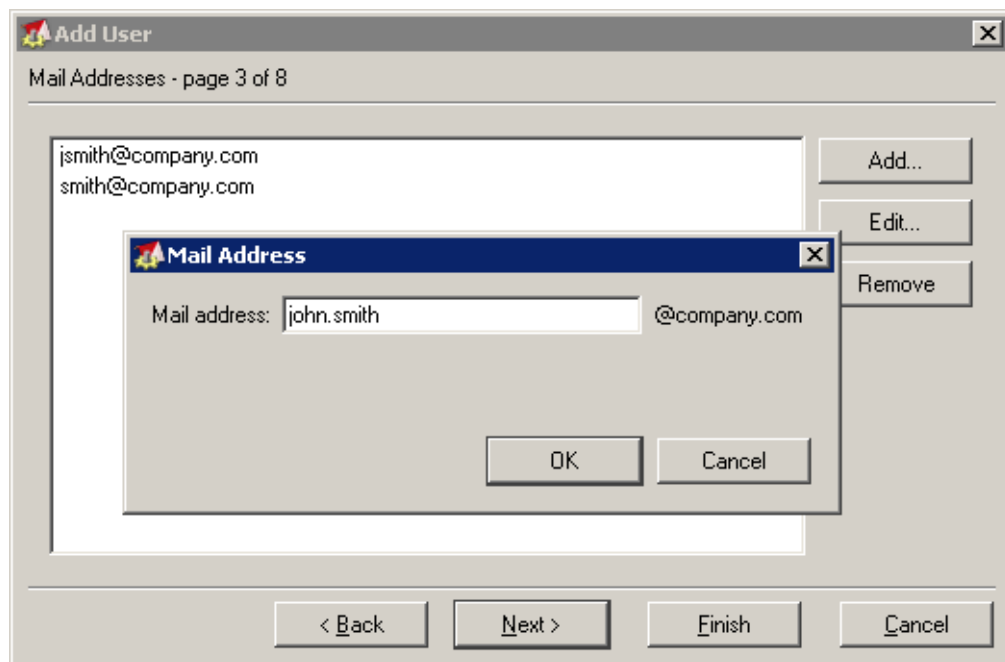


Figure 14.5 New user addition — email addresses

Step 4 — Forwarding messages to other addresses

Messages for a user can be forwarded to other email accounts if defined. If the *Deliver messages to...* button is activated, messages will be saved in the local account and forwarded to the addresses defined by user (if not, messages will be forwarded only, not saved).

Note: The same functionality can be accomplished through the Domain Settings → Aliases dialog; however, aliases created within the user definition dialog is smoother and easier to follow.

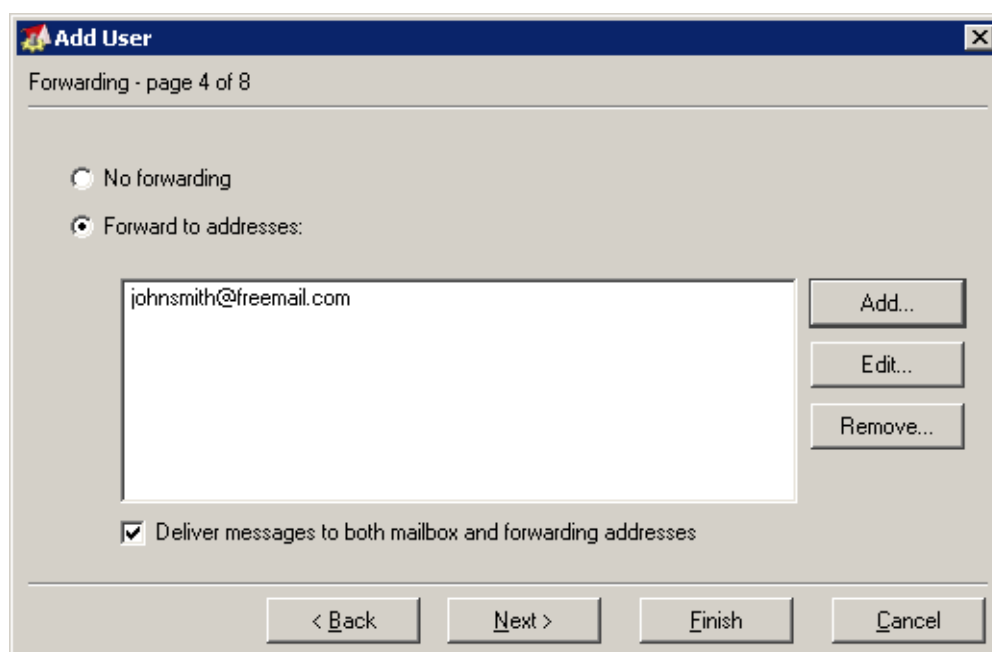


Figure 14.6 New user addition — forwarding messages to other addresses

Step 5 — Groups

In this dialog window, you can add or remove groups of which the user is a member. Groups must be created first in the *Domain Settings* → *Groups* section. You can add users to groups during definition of groups. Therefore, it is not important which is created first — users or groups.

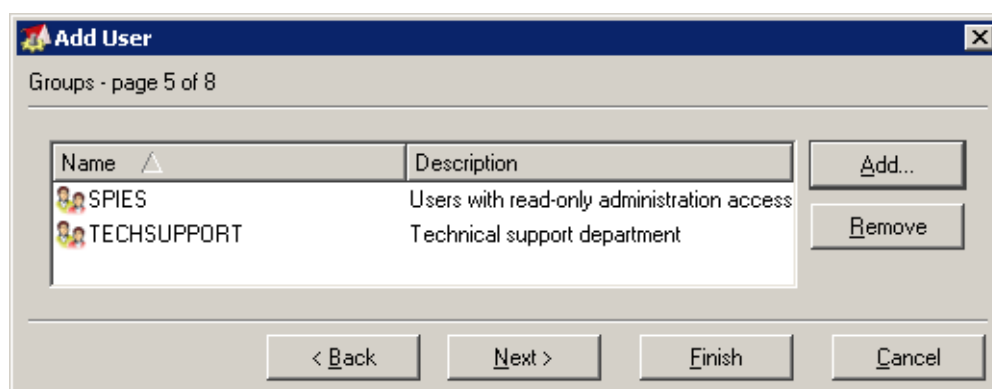


Figure 14.7 New user addition — groups

Step 6 — Access rights

Each user must be assigned one of the following three levels of access rights.

No access to administration

These users do not have any access to *Kerio MailServer* administration. Most users will have this setting so they will only be able to access their own mailboxes.

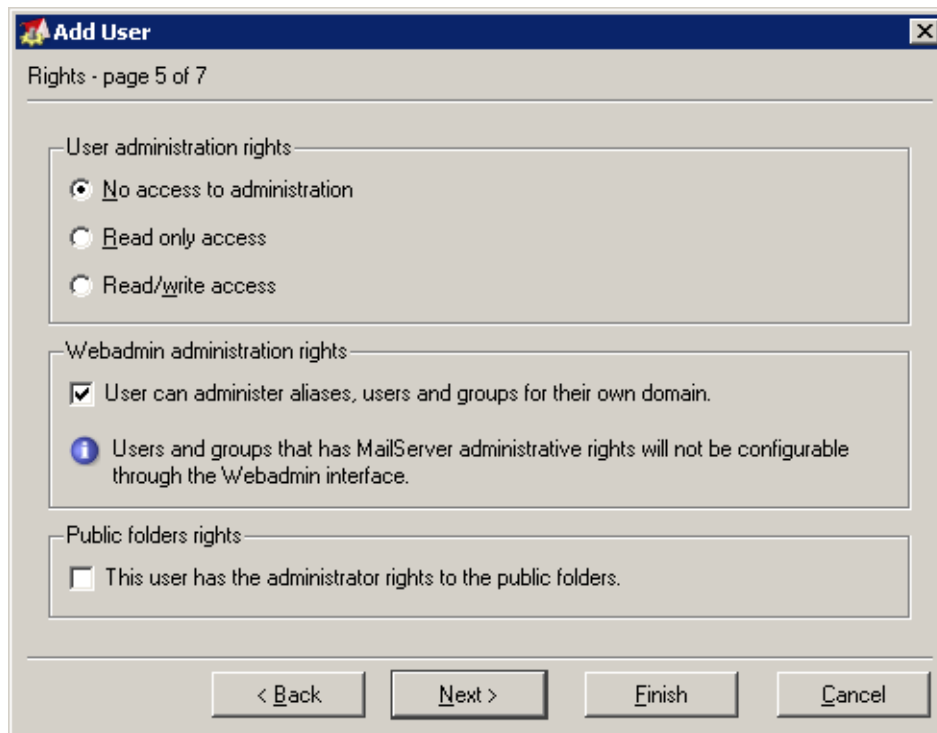


Figure 14.8 Creating a user — user rights

Read only access

These users can connect to *Kerio MailServer* administration but they can only view the logs and settings; they cannot make any changes.

Read/Write access

The user can read or edit all the records and settings and his or her rights are equal to the administrator rights (Admin). If there is at least one user with such rights, the Admin account can be removed.

User can administer aliases and users/groups ...

A special access right to *Kerio MailServer Web Administration* (for more information, see chapter 27). This setting is independent on the access rights settings for *Kerio Administration Console*.

This user has the administrator rights...

By default, only *Admin* of the primary domain is allowed to administer the public folders. If there are multiple local domains with user accounts in *Kerio MailServer*, this option must be selected at least for one user in each domain. Each domain in *Kerio MailServer* has its own public folders and users of a different local domain are not allowed to access it (you can change this setting so that all public folders are accessible from all domains and from all users — for detailed information about this setting, see chapter 8.1).

By default, all users from one domain have read only rights for the public folders. The rights for public folders can be assigned by any user that has the administrator rights. The rights can be also assigned using the *Kerio WebMail* interface and *MS Outlook* with *Kerio Outlook Connector*.

Step 7 — Quota

You can set limits for each user's mailbox.

The screenshot shows a window titled "Add User" with a subtitle "Quota - page 7 of 8". Inside, there is a section labeled "User quota" containing two input fields: "Disk space:" with the value "20" and a unit dropdown menu set to "MB", and "Number of messages:" with the value "0". Below these fields is a small blue information icon followed by the text "0 means unlimited". At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 14.9 New user addition — quota

Disk space

The maximum space for a mailbox. For greater ease in entering values you can choose between kilobytes (*KB*), megabytes (*MB*) or gigabytes (*GB*).

Number of messages

The maximum number of messages in the mailbox.

The value of either of these items can be set to 0 (zero), which means that there is no limit set for the mailbox.

The user quota prevents cluttering of the server disk. If either of the limits is reached, any new messages will be refused by the server.

When the quota is reached, the user will receive a warning message including recommendation on deleting some messages. It is also not important if the quota was exceeded by number of messages or by the reserved disc space capacity. The quota is reached at the moment when an incoming message (or an event, a contact or a task) exceeds one of these limits.

The threshold of 90 per cent of the quota value is set (90 per cent of the limit set for the number of messages or 90 per cent of the disc space reserved). When this threshold is reached, an informative message is sent to the particular user. This value can be edited manually in the *Kerio MailServer*'s configuration file, as follows:

1. Stop the *Kerio MailServer Engine*.
2. In the directory where *Kerio MailServer* is installed, search the `mailserver.cfg` file
3. Open the `mailserver.cfg` file and look up the `QuotaWarningThreshold` value. The line is as follows:

```
<variable name="QuotaWarningThreshold">90</variable>
```
4. Change the value as needed and save the file.
5. Run *Kerio MailServer*.

These warning messages are sent each 24 hours (not more frequently). Even if a user removes messages to get under the quota threshold and then exceeds it again, the next informative message will be sent after 24 hours from the first informative message.

Step 8 — Advanced settings

This user can send/receive ...

Using this option, the administrator of *Kerio MailServer* can limit communication only to the local domain. This can be useful for internal communication settings in many companies. Users will not be able to send or receive emails to/from any other domain.

Add User

Advanced settings - page 8 of 8

☒ This user can send/receive email to/from his/her own domain only

Maximum message size

☐ Use the limit defined for this domain: 20 MB

☒ Limit outgoing message size to: 30 MB Set Unlimited

(overrides the domain limit)

☒ Publish this user information to the public contacts folder

< Back Next > Finish Cancel

Figure 14.10 New user addition — publish user information to the public contacts folder

Maximum message size

Use this option to set the size limit for outgoing messages. The size limit can be either set for each user separately, or globally for the whole domain (see chapter 8.1). If no size limit is specified for the whole domain, it is recommended to set this option.

By setting the size limit, you can prevent the internet connection from being overloaded by emails with large attachments.

If both limits are set to 0, *Kerio MailServer* behaves the same way as if no limit was specified.

Limit set for a specific user has higher priority than limits applied to the entire domain.

Publish this user information to ...

Check this option to add the user contact to the public contacts folder. The contact will be added to the public folder only if the *Full name* field is populated (in the first or second step of the wizard).

Note: When importing users from *Kerio MailServer 5*, only the primary domain users will be added to the public contacts folder.

14.3 Editing User Account

The *Edit* button opens a dialog window where you can edit the parameters of the user account.

Edit User

General | Mail Addresses | Forwarding | Groups | Rights | Quota | Restrictions

Login name:

Full name:

Description:

Authentication:

Password:

Confirm password:

WAP service

☒ Enable access to WAP service

Enter authorization PIN:

☐ Account is disabled

☒ Store password in highly secure SHA format (recommended)

This user cannot be authenticated using APOP, CRAM-MD5 and DIGEST-MD5

OK Cancel

Figure 14.11 Editing User Account

This dialog window contains all of the components of the account creation guide described above, divided into tabs in one window. Current usage of this quota can be viewed in the *Quota* tab. Percent usage is not displayed unless the quota is defined (limited).

Quota usage

Disk space: 1.2 MB Messages: 9

Figure 14.12 Quota is not defined

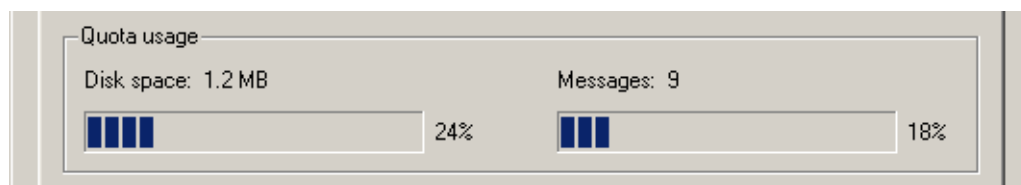


Figure 14.13 Quota is defined

14.4 Editing multiple users

Kerio MailServer allows for mass editing of user accounts. Simply use the mouse pointer to select accounts and click *Edit*.

The dialog window regarding mass modification of user accounts consists of four tabs where quota and user access rights parameters as well as other settings (user description, authentication type, password format settings, etc.) and user restrictions can be edited for the selected users.

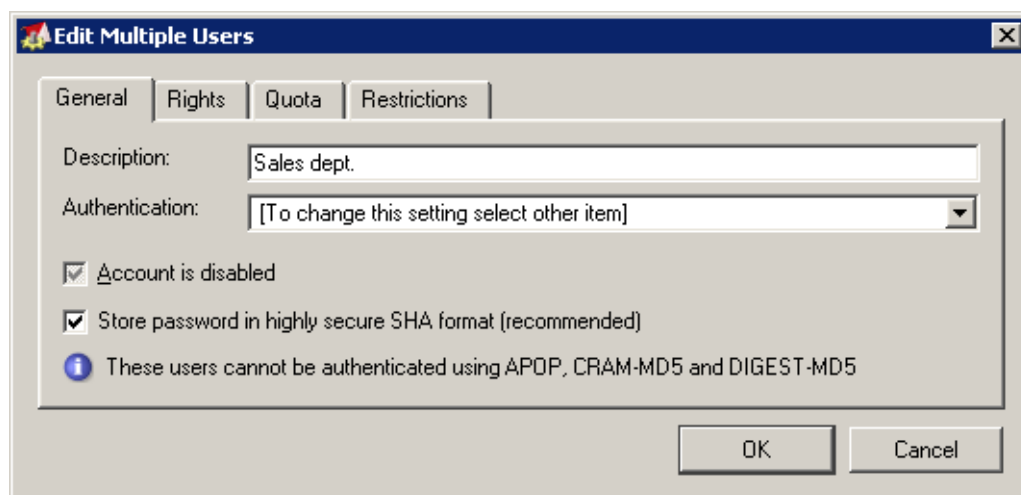


Figure 14.14 Mass change of user accounts

In this dialog window, only items and parameters that will be changed en bloc for all selected accounts are set. Three status modes are available for the *Store password in highly secure SHA format* and *Account is disabled* options on the *General* tab that can be switched by checking/unchecking the checkboxes:

- *inactive, grey* — the former settings will be kept in the accounts,
- *checked* — the item will be enabled in all accounts selected,
- *unchecked* — the item is disabled in all accounts selected.

The first status (inactive) is available only if set differently for the accounts included. If all account are set in the same way, only the *checked* and *unchecked* options are available.

The *Rights*, *Quota* and *Restrictions* tabs can be edited in the same way as while editing their parameters for individual accounts.

Example:

One of the typical cases where mass change is helpful is setting maximal size of outgoing/incoming mail. The *Kerio MailServer* administrator set maximal size of outgoing mail (for one message) for the *company.com* to 20 MB. However, some users need to send larger attachments.

Kerio MailServer enables selecting users of the domain by **Ctrl** and the mouse pointer. Simply select accounts of the *company.com* domain and set a new value for the outgoing mail on the *Restrictions* tab.

14.5 Removing user accounts

Click the *Remove* button to delete a user account. With the original user account in *Kerio MailServer*, many actions can be performed. Once an account is selected and the *Remove* button is clicked, one of the following actions can be selected. In the dialog box you can set the account to be removed or moved to another user or simply to be kept in the store directory.

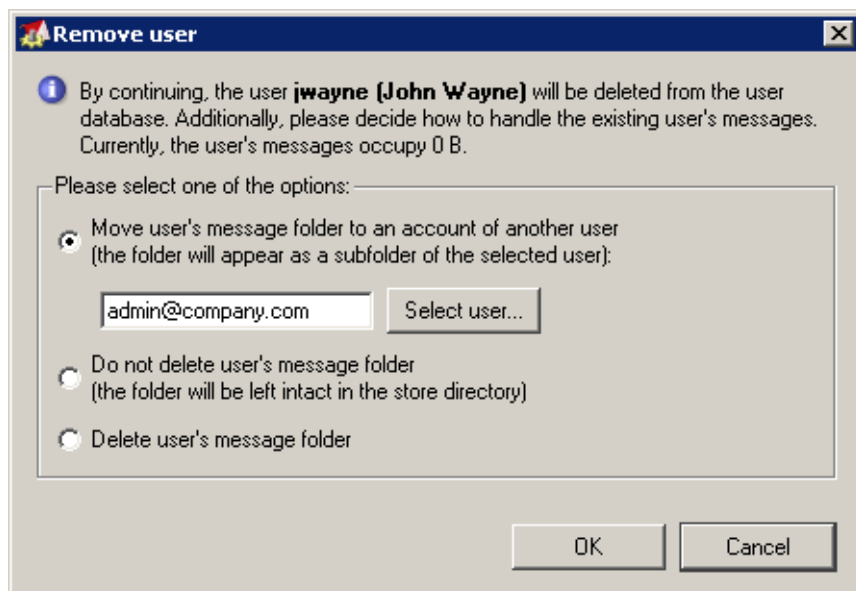


Figure 14.15 Removing a user account

Move user's message folder to an account of another user

The entire folder will be moved as a subfolder of the selected account's root folder. The folder name will follow this pattern: *Deleted mailbox — user_name@domain*. This folder will include all original folders of the deleted mailbox. This option is useful especially when another user needs to work with messages, events and tasks from this folder.

Note: If any problem arises during moving of the a user account, details are recorder in the *Warning* log (see chapter 23.5).

Do not delete user's message folder

The folder will be kept in the store directory.

Delete user's message folder

Use this option if there is no item in the folder that should be kept for any reason.

14.6 Search for:

The *Search* option makes looking up items in the users list easier. Insert a string in the *Search* field to list only items containing the string specified.

14.7 Restoring deleted items

This button is shown only if the correspondent option is enabled in the first tab of the domain settings (see chapter 8.2) and if the time settings for restoring deleted items are specified. The option must be enabled for each domain separately.

If the appropriate options are enabled in the domain settings, the *User accounts* section will show the *Restore deleted items* button. Simply mark the user that has deleted an important message by mistake and all items (messages, events, tasks and contacts) received or created during the time interval specified will be moved to the *Deleted items* folder.

If an older item is to be restored (see chapter 19.2), you can use the archiving option; however, it is not designed for this purpose by default.

14.8 Statistics

User statistics are recorded immediately after *Kerio MailServer* is installed. To store the statistics even when the server is off, each user's data is saved into the `stats usr` file under its parent directory.

Use the *Statistics* button in the *Domain Settings* → *User Accounts* section to open the table of statistics that contains selected user accounts, *services* to which the statistics refer to, *last login* (day and time of the most recent user authentication to the service) and *login count* (total number of authentications of individual users).

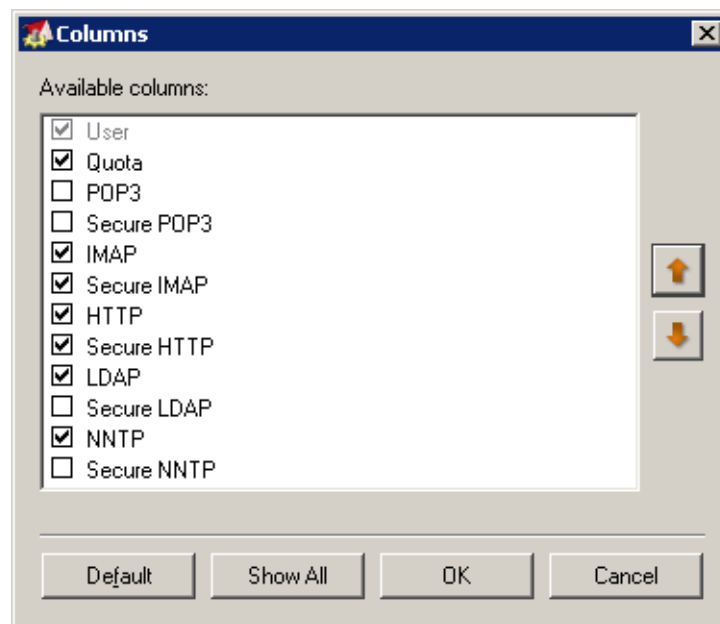


Figure 14.16 Column selection in statistics

The *Kerio MailServer* administrator can customize the way information is displayed in individual sections. Right-click in *Statistics* dialog to display a pop-up menu with the *Modify columns* option. When this option is selected, it brings up a dialog box where the administrator can specify the columns to be displayed or hidden.

The user statistics can be exported in two formats: XML and CSV (the comma-separated values). The export button is located under the statistics.

14.9 Import Users

User accounts can be either defined manually or they can be imported from other sources.

Warning: If you use a Windows 2000 or windows 2003 domain (Active Directory), it is easier to set *Kerio MailServer* so that it cooperates directly with the Active Directory database (see chapter 8.6). When users are imported, local accounts are created in *Kerio MailServer*. Therefore, when you are editing Active Directory (removing or adding users), the *Kerio MailServer* configuration must also be edited (new user import or deleting an account).

The *Import* button placed below the user list will open the dialog for user import. Use the *Import users from* option to select a source from which users will be imported.

NT Domain

In this case, the only required parameter is the *NT domain name*. The computer which *Kerio MailServer* is running on must be a part of this domain.

Do NOT import users this way if the domain controller runs the Windows 2000, XP or 2003 Server operating system! In such a case, import them from the *Active Directory* — see below.

Warning: Import of NT domain users works only if *Kerio MailServer* is installed on the *MS Windows* platform.

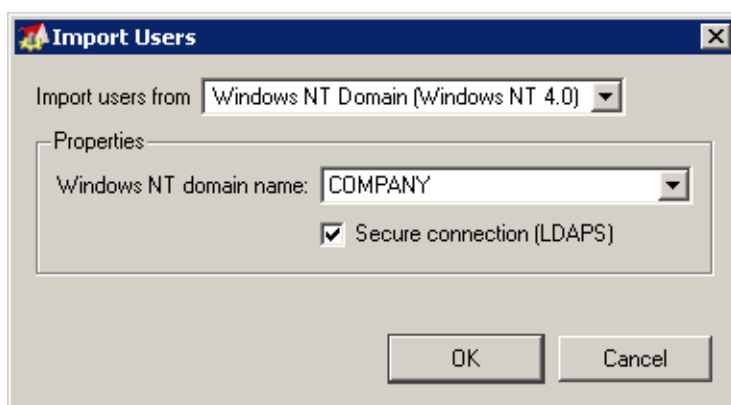


Figure 14.17 Import users from NT Domain

Within the import of user accounts from the LDAP database with *Kerio MailServer*, sensitive data may be transmitted (such as user passwords). It is possible to secure the communication by using an SSL encryption.

Active Directory

To import users from *Microsoft Active Directory*, you need to specify the following information:

- *Active Directory domain name* — the name of the domain users will be imported from (the format is as in DNS domain — e.g. `domain.com`)
- *Import from server* — the name of the server, on which Active Directory for this domain is running.

If a special port is specified for the LDAP(S) service, the port number can be added to the server name (e.g.: `mail1.company.com:12345`).

- *Login as user, Password* — the username and password of the user who has an account open in the domain. Write access rights are not required for saving and changing settings.

- *LDAP filter* — using this item, queries to an LDAP server for importing users can be specified. It is recommended that only experienced programmers use this option. For details about the query syntax, see the instruction manual to your LDAP server.
- Within the import of user accounts from the LDAP database with *Kerio MailServer*, sensitive data may be transmitted (such as user passwords). It is possible to secure the communication by using an SSL encryption.

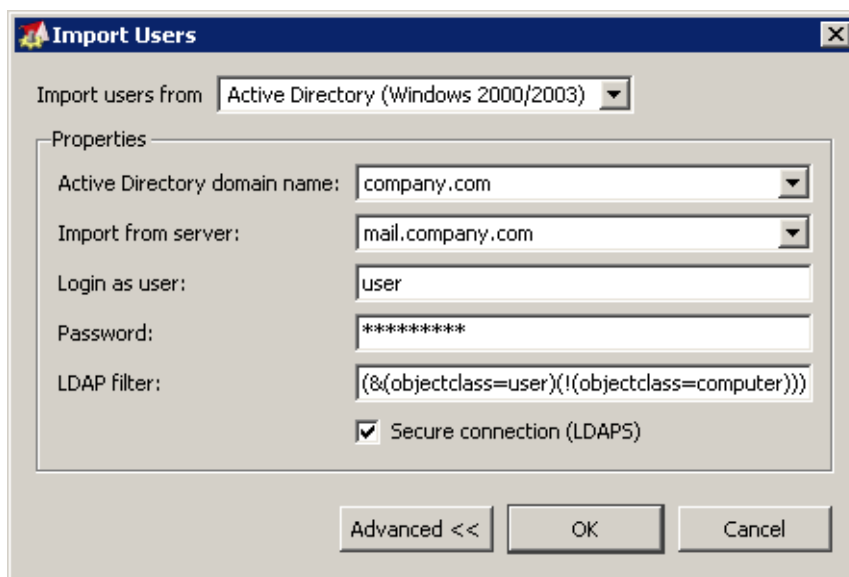


Figure 14.18 Import users from Active Directory

Novell eDirectory

To import users from *Novell eDirectory*, specify the following items:

- *NDS organization* — the name of the organization users will be imported from
- *Import from server* — the name of the server, on which the service for this domain is running.

If a special port is specified for the LDAP(S) service, the port number can be added to the server name (e.g.: mail1.company.com:12345). The *Kerio Administration Console* for *Mac OS X* is the only one which includes the *Secure connection (LDAPS)* option.

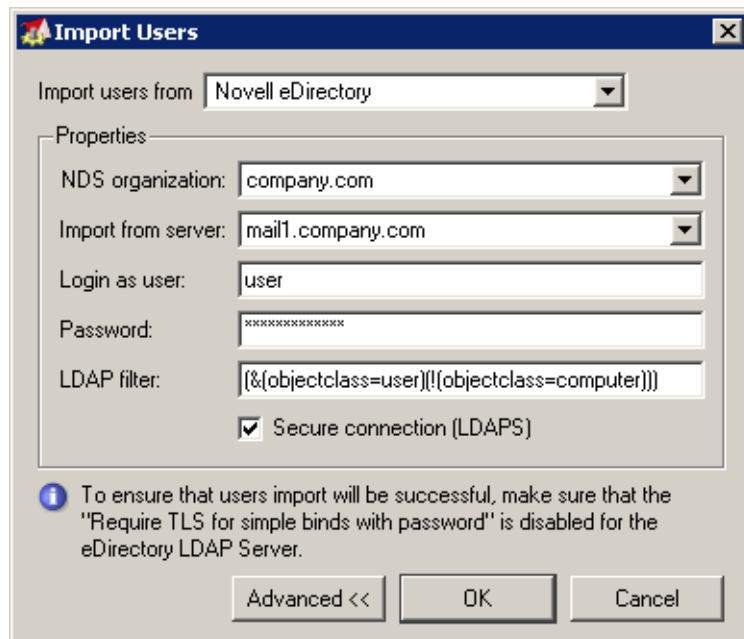


Figure 14.19 Import users from Novell eDirectory

- *Login as user, Password* — the username and password of the user who has an account open in the domain. Write access rights are not required for saving and changing settings.
- *LDAP filter* — using this item, queries to an LDAP server for importing users can be specified. It is recommended that only experienced programmers use this option. For details about the query syntax, see the instruction manual to your LDAP server.
- Within the import of user accounts from the LDAP database with *Kerio MailServer*, sensitive data may be transmitted (such as user passwords). It is possible to secure the communication by using an SSL encryption.

User selection

If all required information is entered correctly and the appropriate server is accessible, a list of users will be displayed after clicking on the *OK* button. From there you can select users that will be imported to *Kerio MailServer*. You can also select a template that will be used for creating these users' accounts in *Kerio MailServer*. If no template is selected the default template will be used.

If the users are imported from *Active Directory*, the platform on which *Kerio MailServer* is running is not important.

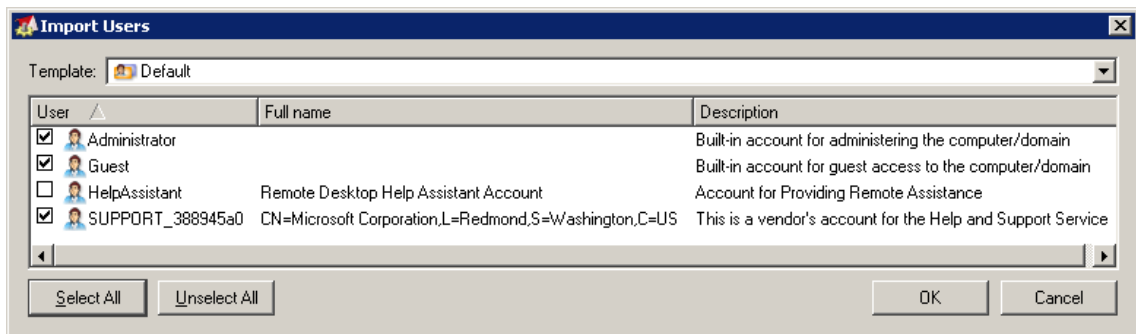


Figure 14.20 Users selection for import

The authentication type will be set according to where users were imported from: *NT Domain* for users imported from an NT domain and *Kerberos 5* for users imported from Active Directory (Active Directory uses Kerberos 5 authentication system by default).

14.10 Publish users in address book

Information about selected users (regardless whether these are local accounts or directory service accounts) can be published to the public address book (to any public *Contacts* folder). To export accounts, click on the *Publish* button (below the user account list). The button is inactive unless users to be published are selected. This button displays a dialog where a folder for the data and users to be published in can be selected.

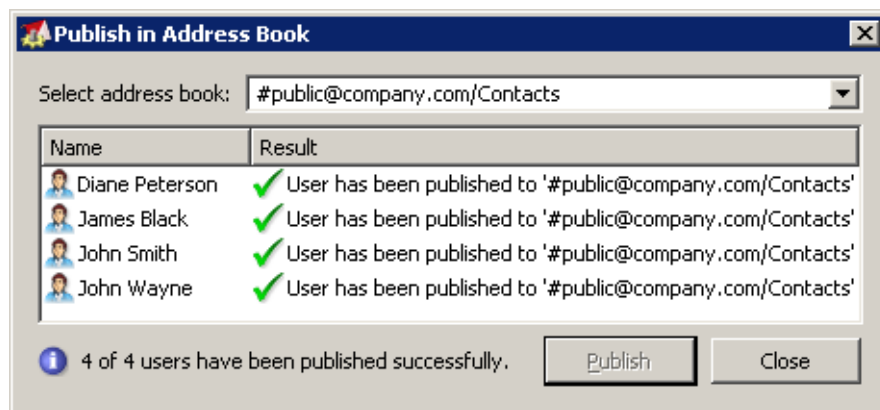


Figure 14.21 Export to Address Book

If there is no public address book defined, the *#public/Contacts* folder will be generated automatically during the first publishing.

Only the full name and email address are published. Other parameters are irrelevant, however they can be added by users with appropriate rights, e.g. via the *Kerio WebMail* interface.

Note: Contacts can be published in the address book by any user that have both read and write rights in the *Kerio MailServer* administration (see chapter 14.10). Rights for public folders are not required.

When the publishing process is completed, its results are provided (see figure 14.21).

14.11 User Account Templates

Templates simplify creation of a large number of user accounts (typically for users of one domain). In a template you can define all account parameters except the user name and password (if internal authentication is used). User accounts can be defined using a created template by simply filling in the *Name*, *Full Name* and *Description* fields (plus perhaps *Password* and *Confirm Password*). The *Full Name* and *Description* fields are not obligatory. In the simplest case you only need to fill in one field — the user name.

Defining a Template

You can define a template in the *Configuration* → *Definitions* → *User Templates* section. The dialog window for creating or editing a template is almost identical to the dialog window for creating a user account.

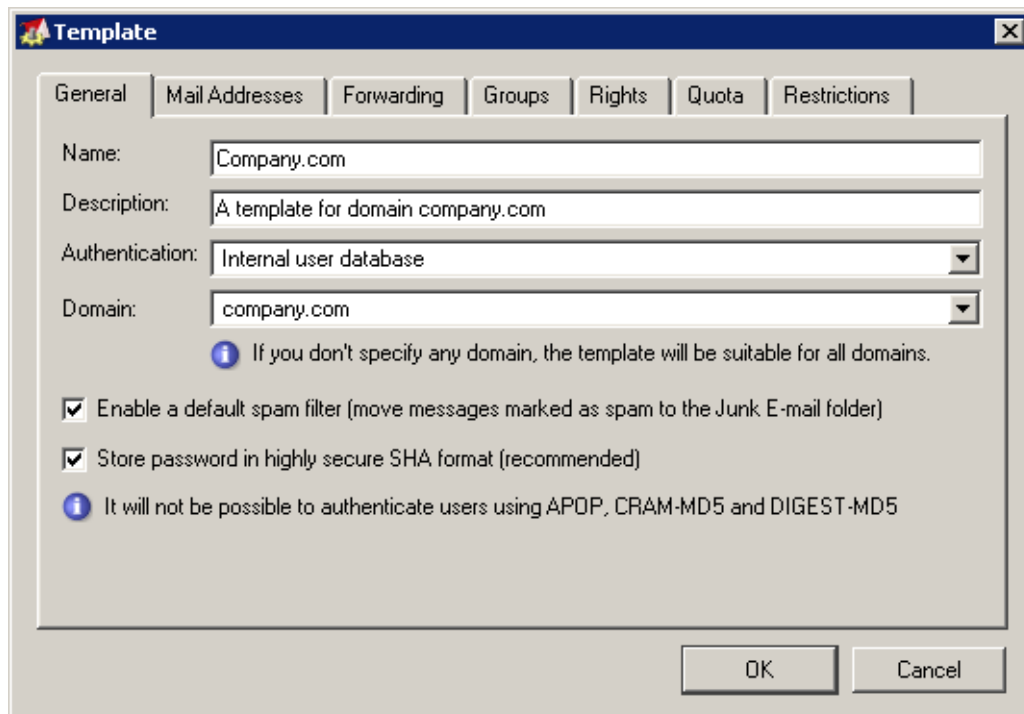


Figure 14.22 Defining a template

Name

Name of the template (unique name used for the template identification).

Description

This field has two meanings. First, it is the template's description that will be displayed next to its name in the template list and, second, it is copied to the *Description* field in the user account created with this template.

Authentication

The authentication method to be performed (for details, see chapter 14).

Domain

Selection of the domain for which the template will be used. Here you can choose one of the local domains defined in *Kerio MailServer* or you can decide not to specify any domain. If no domain is specified, the template can be used for creating and editing user accounts in any domain (general template).

Enable a default spam filter ...

Check this option to move all recognized spam messages to the junk email folder.

Store password in highly secure SHA format

By default, user passwords are encrypted by DES. The *Store password in highly secure SHA format* allows for a more secure encryption (SHA string). This option has one disadvantage — some methods of *Kerio MailServer* access authentication (APOP, CRAM-MD5 and Digest-MD5) cannot be applied. The only methods available for this option are LOGIN and PLAIN (it is highly recommended to use only SSL connection for authentication).

If this option is enabled, it is necessary to change the user password. This can be done either by administrator or the user (e.g. by *Kerio WebMail* or by another email client).

The other fields in the dialog window are the same as the fields in the user account dialog window. The values entered here will be automatically entered into corresponding fields in the created account. For details, see chapter 14.2.

Using the Template

A created template can be used immediately for creation of a user account in the *Domain Settings* → *Users* section. If at least one template is defined, the first step of a wizard is displayed when you click on *Add* that prompts you to choose a template.

Only templates created for the particular domain or templates with an unspecified domain (general domains) will be displayed in the wizard dialog. The *No template* option means that no template will be used for creating the account (most fields will be blank or default values will be entered).

Once you choose a template a user account creation guide will be opened where appropriate values will be entered into individual fields. For details, see chapter [14.2](#).

Chapter 15

User Groups

User accounts within each domain can be sorted into groups. The main reasons for creating user groups are as followed:

- Group addresses can be created for certain groups of users with aliases (see chapter 16.3) — mail sent to this address will be delivered to all members of the group.
- Specific access rights can be assigned to a group of users. These rights complement rights of individual users.

You can define user groups in the *Domain Settings* → *Groups* section.

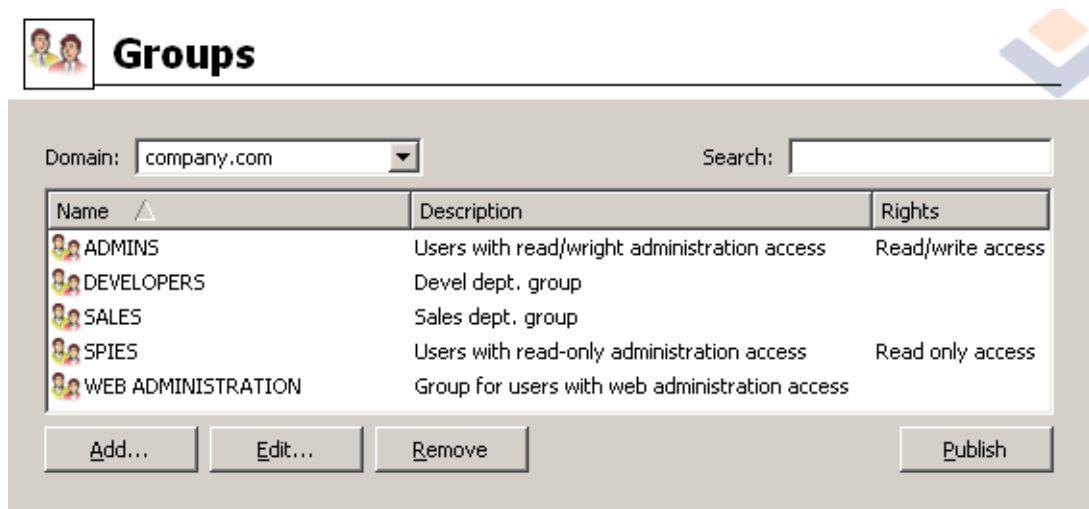


Figure 15.1 User groups

The *Search* field and the *Publish* button have the same function as described in section *Users*. For detailed description of these items, see chapter 14.

15.1 Creating a User Group

Create a new group by clicking on the *Add* button. A guide for user group creation will be opened.

Step 1 — Name and description of the group

Name

Unique name of the group.

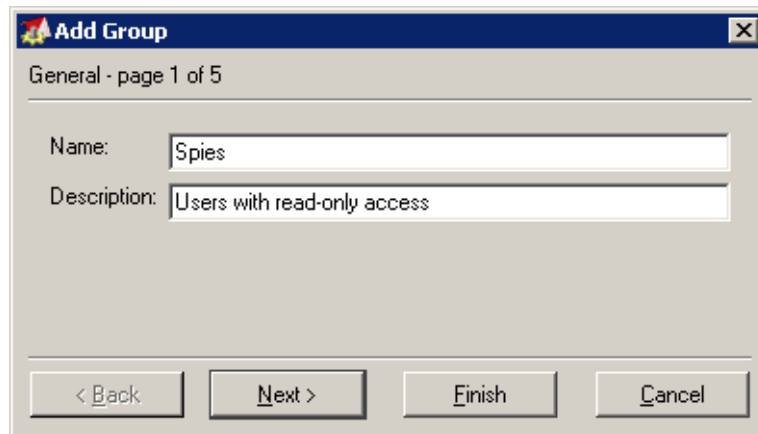
The image shows a Windows-style dialog box titled "Add Group" with a close button (X) in the top right corner. Below the title bar, it says "General - page 1 of 5". There are two text input fields: "Name:" with the value "Spies" and "Description:" with the value "Users with read-only access". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 15.2 Creating a group — basic data

Description

Description of the group; may be left blank.

Note: Pressing the *Finish* button the wizard can be finished in any step. The group will be created and the “skipped” fields will be filled with default values.

Step 2 — Email accounts

This step defines all desired email accounts (aliases) of the group. There might be no address assigned to the group (unlike user accounts, the group address is not created automatically from the group name and domain where the group is defined).

Group addresses can be defined either in group definitions or in the *Domain Settings* → *Aliases* section. The first method is recommended — it is easier.

Note: If user accounts are maintained in *Active Directory* (see chapter 8.6), their aliases can be defined in *Active Directory Users and Computers*. Global aliases (in *Domain Settings* → *Aliases*) cannot be defined this way.

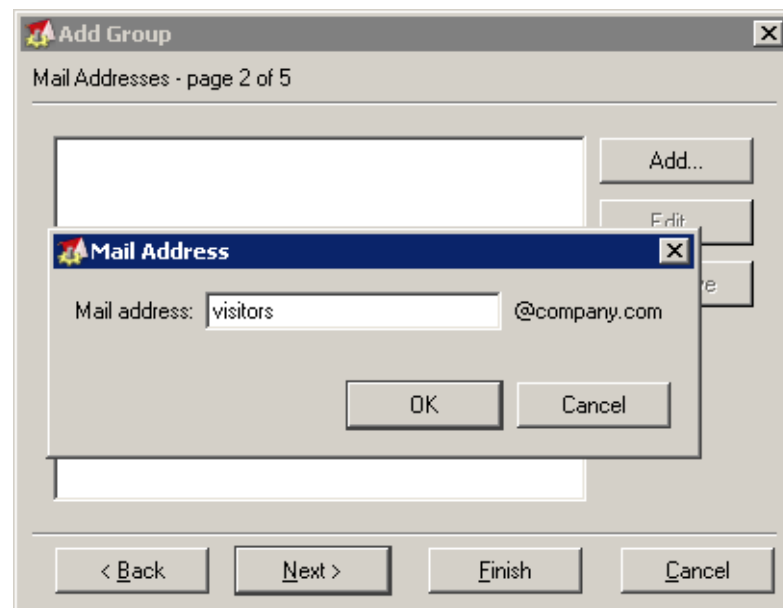


Figure 15.3 Creating a group — e-mail address

Step 3 — Members of the group

Using the *Add* and *Remove* buttons you can add or remove users to/from the group. If there are no user accounts created, a group may remain empty and users will be assigned to it when their user accounts are defined (see chapter 14.2).

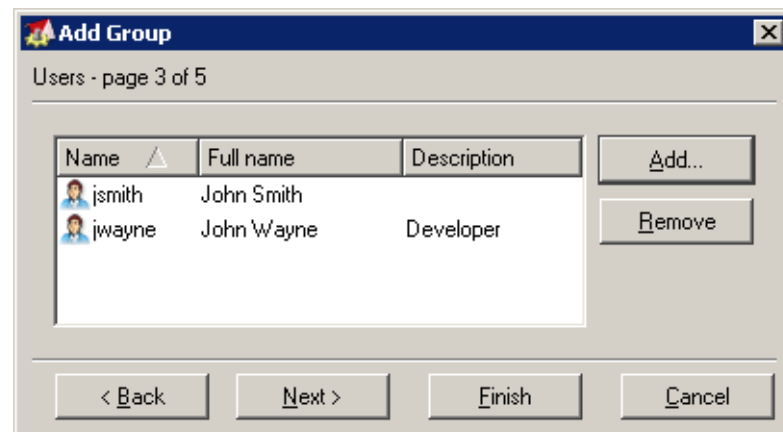


Figure 15.4 Creating a group — users addition

Step 4 — Access rights for the group

The group must be assigned one of the following three levels of access rights:

No access to administration

Users in this group have no access to *Kerio MailServer* administration.

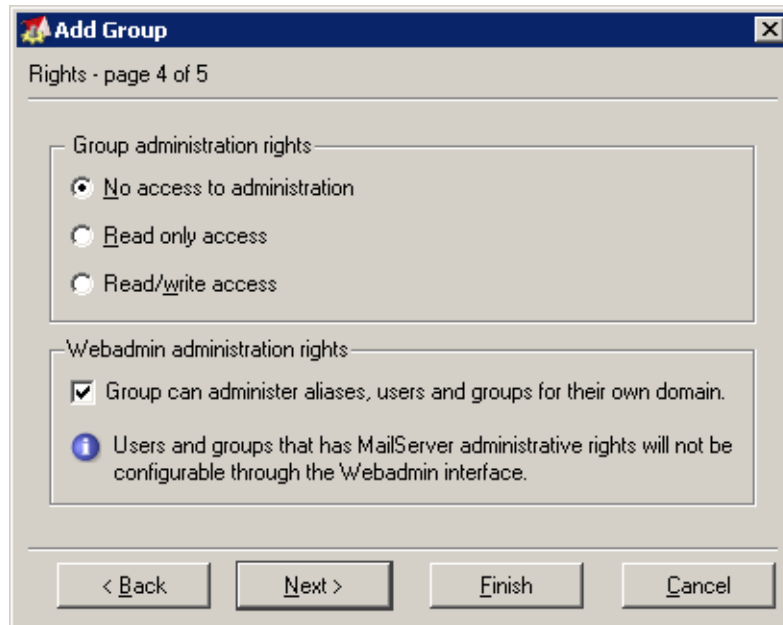


Figure 15.5 Creating a group — user rights

Read only access

Users in this group can log in to *Kerio MailServer* administration but they can only view the logs and settings. They cannot alter any settings.

Read/Write access

Users in this group have full access rights.

Group can administer aliases and ...

A special access right for *Kerio Web Administration* (for more information, see chapter 27). This setting is independent on the access rights settings for *Kerio Administration Console*.

Group access rights are combined with user access rights. This implies that resulting user rights correspond either with their own rights or with rights of the appropriate group according to which ones have higher priority.

Step 5 — Advanced settings

This group can send/receive email from ...

Using this option, the administrator of *Kerio MailServer* can limit communication only to the local domain. This can be useful for internal communication settings in many companies. Users will not be able to send or receive emails to/from any other domain.

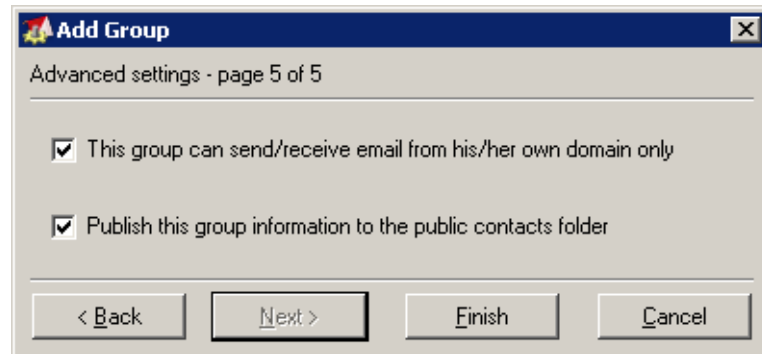


Figure 15.6 Creating a group — publish information to the public contacts folder

Publish this group information to the ...

Check this option to add the group and its email address to the public contacts folder.

Sending and Receiving Mail

16.1 Mail Delivery over the Internet

Understanding the basic principles of mail delivery over the Internet will help you correctly set your mailserver. This chapter gives a brief overview of the most important information on this topic. Experienced network administrators can skip this chapter.

MX Records

Appropriate records must be entered into the DNS (DNS is a world-wide distributed database of domain names) for each Internet domain. One of these records is called a MX record (Mail eXchanger or the mailserver). An MX record for the domain `company.com` might look like this:

These records indicate that the mailserver with a preference of 10 is a computer named `mail.company.com` and the server with a preference of 20 is a computer named `smtp.isp.com`. Preference means value of the server. The lower the preference the higher the priority of that server — this implies that the server `mail.company.com` is the highest priority mail server for the domain `company.com` and the server `smtp.isp.com` is the second highest priority mail server for the domain. Arbitrary number of MX records can be defined for the given domain. If two or more records have the same priority, then one of these servers is chosen randomly (load balancing).

The other two records are A type (Address). These tell us which IP address is assigned to a given computer (a MX record can only be assigned to a DNS name, but not an IP address).

Email Delivery

How does an email travel from the sender to the addressee?

The sender's mail client sends the email to its SMTP server. The server checks the recipient's address and if the domain contained within the address is qualified as local the email is saved directly into the appropriate mailbox. If the domain is not local, the SMTP server finds the name of the primary mailserver (SMTP) for the target domain from the DNS (by sending a DNS request) and sends the email to this server. This saves it to a mailbox from which the recipient downloads it using his/her email client.

If the primary mailserver for the target domain is not accessible, the sending SMTP server tries to contact the secondary server (the server with the next priority) and send the email there. If no server listed in the MX record for the target domain is accessible the SMTP server will try to send the mail again repeatedly in defined intervals. If it does not succeed after a certain time the email is returned to the sender as undeliverable.

If, for example, only the secondary server is accessible the email is sent to this secondary server. This server then tries to send the email to the primary server in certain time intervals. In principle, any SMTP server can function as a secondary (tertiary, etc.) server for a domain.

Sending Email via a Different SMTP Server (Relaying)

There is also another way email can be delivered to addressees. The client sends the email message to its SMTP server. This server forwards it to another SMTP server which delivers it to the target domain as described above. This method of delivering email is known as relaying (passing to the relay server).

The advantage of this relaying is that sending email is an on-off action. Furthermore, email can be placed in a queue and sent in defined time intervals. The sending SMTP server does not need to ask the DNS about the target domains' mailservers or try to send the email again if the target servers are inaccessible. This is important mainly for slow or dial-up Internet connections and it can significantly decrease costs of such connections.

Most SMTP servers on the Internet are protected against relaying to prevent misuse of servers for sending spam email. If you wish to send email via a different SMTP server, you should contact the server's administrator and ask them that relaying be enabled for you (usually based on checking your IP address or using username/password authentication).

ETRN Command

ETRN is a command of SMTP protocol. It serves for requesting emails stored on another SMTP server. Typically, it is used in the following situations:

1. The client has its own domain (e.g. `company.com`) and his server is connected to the Internet via a dial-up line. Dial-up must have a fixed IP address. The primary MX record for the domain `company.com` is directed to the ISP's SMTP server (e.g. `smtp.isp.com`). When it is connected to the Internet, the client's SMTP server sends an ETRN command that informs that it is online and ready to receive mail. If the primary server has some emails for the given domain, then it sends them. If not, it can send a negative response or it need not reply at all. That's why the client's

server must have the timeout to specify how long it will wait for the response from the primary server.

Note: The primary server will create a new connection to the client's server after the ETRN command reception. This connection is used for mail transmission. If the client's server is protected by firewall, TCP port 25 must be accessible (open) to the Internet.

2. Let's suppose that the domain `company.com` has a primary server `smtp.company.com` and a secondary server `smtp2.company.com`. Both servers are permanently connected to the Internet. Under normal circumstances, all messages for this domain are sent to the primary server `smtp.company.com`. If failure of this server occurs (overloading, disconnected line etc.), all messages are sent to the secondary server `smtp2.company.com`. When the primary server becomes available it can send an ETRN command to the secondary server to request stored mails. Communication is the same as in the previous example (for detailed description of secondary SMTP server settings, see chapter 25.5).

Mail delivery is faster and more reliable in this way than waiting till the secondary server sends the mails itself (see section *Email Delivery*). In addition, the ETRN command can be used also for dial lines.

domain mailbox

The domain's primary mailserver does not always need to be the server where user mailboxes are stored. If the company to which the domain is registered connects to the Internet via a dial-up line, it can have a Domain Mailbox at its ISP. A domain mailbox is an account where mail for the entire domain is stored. The company's mailserver can retrieve mail from this mailbox (in certain time intervals) and sort the email into individual user mailboxes. The ISP's SMTP server, where the domain mailbox is stored, is listed as the primary mailserver for the company's domain in the MX records.

Domain mailbox receives the messages via SMTP protocol. Each message therefore contains the body as well as the SMTP envelope. Only the body of the message is downloaded to the domain mailbox. The envelope information is copied to a message header (depending on the domain mailbox settings).

Kerio MailServer performs authentication to the domain mailbox. Then it downloads messages via POP3 and sorts them according to the rules specified in *Kerio MailServer*. In order for the rule to be sorted properly, it must contain the recipient information (either in any of the special message headers or in the *To* or *Cc* fields). If there is no information about the recipient contained in the message, the system returns it to

the sender. However, if a special sorting rule is created in *Kerio MailServer* (see chapter 16.4), the messages without any recipient data will be stored in a predefined user mailbox.

Note: It is recommended to specify a special `X-Envelope-To:` header for message sorting, because it contains information about recipients. This helps you avoid situations where a message addressed to multiple users is delivered several times according to the number of recipients.

16.2 Relay server hostname

SMTP server settings protect the server on which *Kerio MailServer* is running from misuse.

Antispam protection of the mailserver enables users to define who will be allowed to use this server and what actions he/she can perform. This way, the server is protected from being misused. If the SMTP server is available from the Internet (anytime when at least one MX record is directed to it and the port 25 is available for access), any client can connect and use the server to send an email message. Thus the server can be misused to send spam messages. Recipients of such email messages will see your SMTP server as the sender in the source text and might block receiving messages sent from this server. Thus your company might be considered a spam sender and your server can be added to a database of spam servers.

Kerio MailServer provides a protection system that enables users to define who will be allowed to send email via this server and where. Anyone can connect to the SMTP server to send messages to local domains. However, only authorized users will be allowed to send email to other domains.

In this section, the delivery parameters can be also set:

Relay Control Tab

Use the *Relay control* tab to set groups of allowed IP addresses and/or user authentication against SMTP server.

Allow relay only for

Use this option to activate user authentication by IP addresses or usernames and passwords (see below). Generally, authenticated senders can use email messages to any domain via this server, whereas unauthorized users can send messages only to local domains.

Also add all trustworthy servers to this IP group. These servers will not be checked by the *SPF* and *Caller ID* modules (for details, see chapter 17.3). Trusted servers will not be even checked by *SpamEliminator*. However, this filter can be enabled by

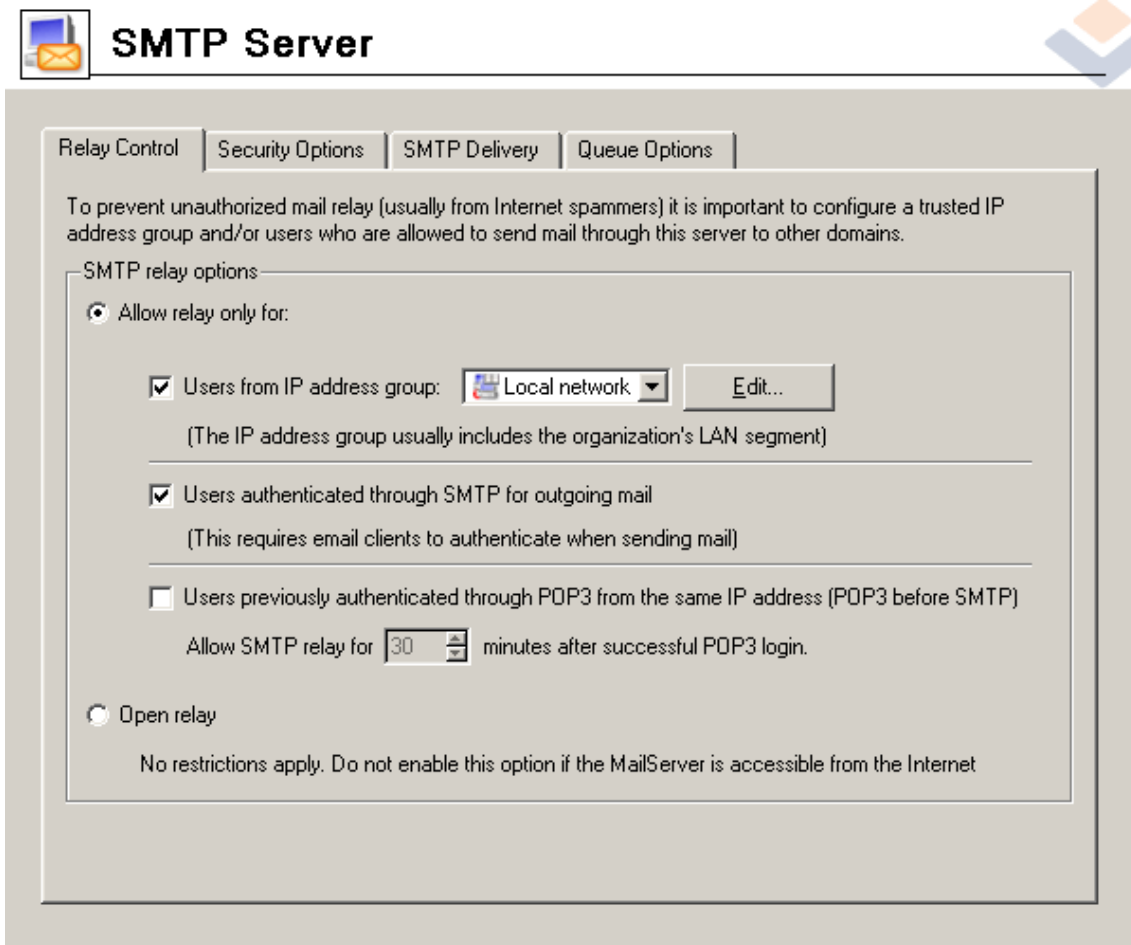


Figure 16.1 Relay Control tab

a special option in the *Spam Filter* section on the *Spam Rating* tab if necessary (for more information, refer to chapter 17.1).

Users from IP address group

Use this option to define a group of IP addresses from which email can be sent to any domain. Use the *IP address group* menu to choose an item from the list of groups defined in *Configuration → Definition → IP Address Groups*. Use the *Edit* button to edit a selected group or to create a new one (see chapter 13.1).

Users authenticated through SMTP server for outgoing mail

Users authenticated through SMTP server using a valid username and password will be allowed to send email to any domain. Thus, all users that have their own accounts in *Kerio MailServer* will have this right.

Users authenticated through POP3 from the same IP address

Users authenticated through POP3 (username and password) will be granted relay access from their IP address for a given period of time.

Authentication by IP addresses is independent from authentication by usernames; therefore users must meet at least one of these conditions. If both *Users from IP address group* and *Users authenticated through SMTP server...* options are selected and the SMTP authentication fails, *Kerio MailServer* does not verify, if the user belongs to the allowed IP addresses.

Open relay

In this mode, the SMTP server does not check users who use it to send email. Thus any user can send email messages to any domain.

Warning: We recommend you not to use this mode if *Kerio MailServer* is available from the Internet. If *Kerio MailServer* is available from the Internet uses a public IP address and port 25 is not behind the firewall, it is highly probable that it will be misused to send spam. This could overload your Internet connection. This might also cause that your server will be included in databases of spammer SMTP servers (see below).

Security Options Tab

Apart from completely blocking certain senders *Kerio MailServer* provides options that limit, for example, sending too many messages or opening too many connections (known as DoS attack). These options can be set in the *Security Options* section.

Max. number of messages per hour...

Maximum count of messages that can be sent from one IP address per hour. This protects the disc memory from overload by too many messages (often identical and undesirable).

Note: Maximum count of messages received from a single IP address is checked always for the last hour. If this option is enabled, any new message sent from the IP address where the limit was exceeded in the recent hour is discarded.



Figure 16.2 Security Options — IP address based limits

Max. number of concurrent SMTP connections...

Maximum number of concurrent TCP connections to the SMTP server from one IP address. This is a method of protection against DoS attacks (Denial of Service — too many concurrent connections overload the system and no other users can connect to the server).

Max. number of unknown recipients ...

Also known as a Directory harvest attack, this condition is met when an application that guesses common usernames of recipients' fails up to the number of allowed unknown recipients. If this type of protection is enabled, the server sending messages to an unknown recipient is blocked for an hour.

Do not apply these limits to IP address group

Group of IP addresses on which the limitations will not be applied. This rule is often used for groups of local users (see the *Relay Control* tab). These users send all their outgoing mail through *Kerio MailServer* — the count of messages sent by these users to this server is therefore much higher than the number of messages sent by external users (servers) that use it only to deliver mail to local domains.

It is also recommended to include the secondary SMTP server to the list of allowed IP addresses, because in some cases, its behavior can be similar to that of an attacking server.

Block if sender's mail domain...

When a message is received *Kerio MailServer* checks whether the sender's domain has a record in DNS. If not, the message will be rejected. This feature protects from senders with fictional email addresses.

Note: This function may slow down *Kerio MailServer* (responses of DNS servers may take up to several seconds).

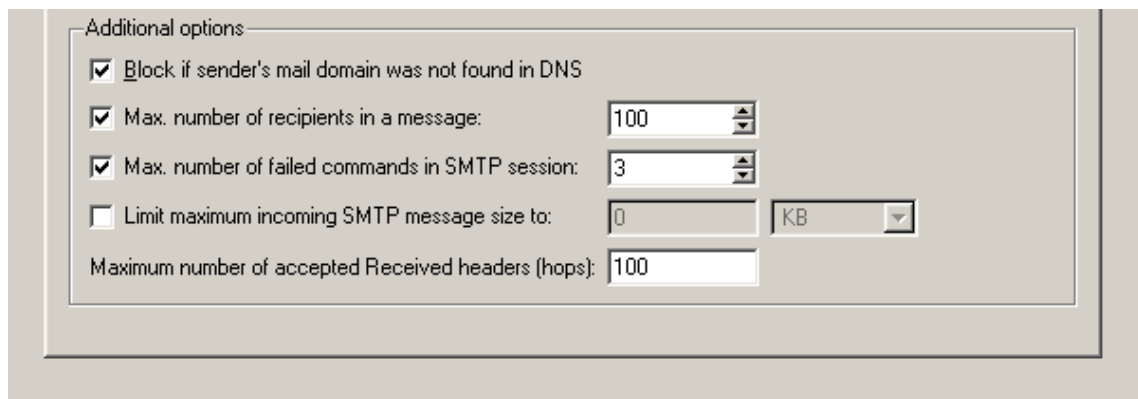


Figure 16.3 Security Options — Advanced options

Max. number of recipients in a message

Maximum number of message recipients that will be accepted (in number of Rcpt commands in the SMTP envelope).

Max. number of failed commands...

Spam is often sent by special applications that connect to SMTP servers and ignore its error reports. If this option is enabled, *Kerio MailServer* will close the SMTP connection automatically after the defined number of failed commands has been expired.

Limit maximum incoming SMTP message size to

Maximum size of a message that will be accepted by the SMTP server. This protects the server from being overloaded by large messages, therefore we strongly recommend to activate this option. The 0 value means that no limitation is set. For easy definition you can switch between kilobytes (KB) and megabytes (MB).

Maximum number of accepted Received headers (hops)

This parameter helps the server block messages that have been trapped in a loop.

SMTP Delivery tab

In this section, the delivery parameters can be also set:

Deliver directly using DNS MX records

Mail will be delivered directly to destination domains using MX records.

Figure 16.4 SMTP Delivery tab

Use relay SMTP server

All outgoing mail will be sent via another relay SMTP server.

Relay server hostname

DNS name or IP address of relay SMTP server.

Relay server port

Port where the relay SMTP is running. Typically the standard port 25 is used (this value is also set as *Default*).

Relay server requires authentication

Use this option if relay server requires authentication of sender (*Kerio MailServer*) using username and password. Specify the *User* and *Password* entries.

Authentication

A method used for authentication at the parent server: *SMTP AUTH Command* or *POP3 before SMTP*

First, the user authenticates to the POP3 account at the server. After this authentication the user is known already and they can send email via the SMTP server. Username and password used here will be used to login to the mailbox and no mes-

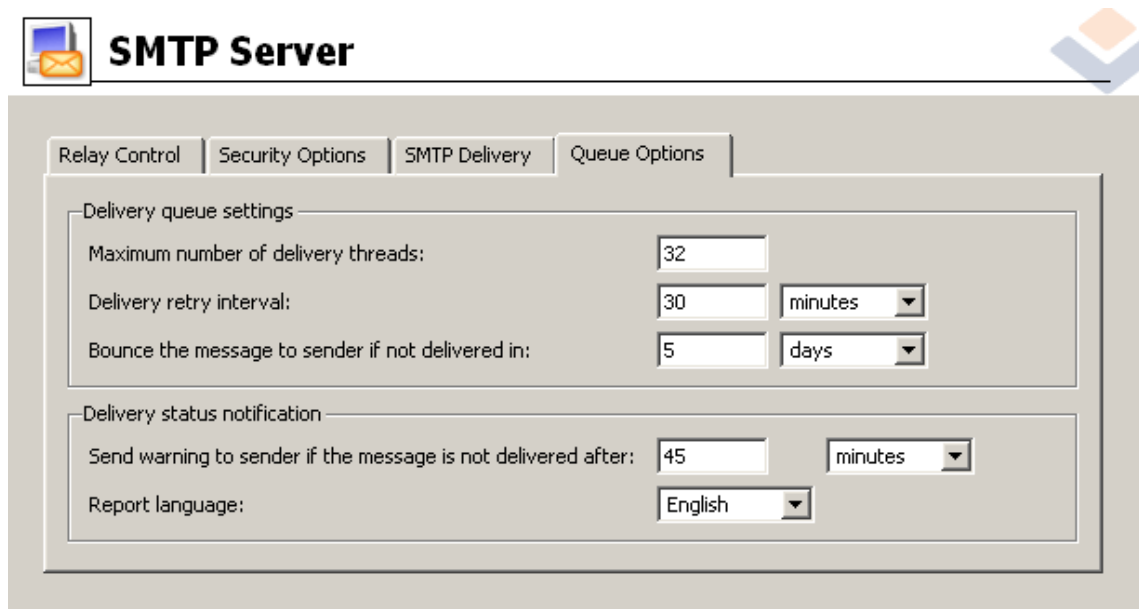
sages can be read. Therefore you do not need to define mailbox in *Configuration* → *POP3 Download* to send an email message.)

Use SSL if supported by remote SMTP server...

When sending a message, SMTP server attempts to use encrypted connection first (SSL). If SSL connection is not supported, unencrypted connection will be used. Thus the maximal possible security of sent messages is ensured.

Queue Options

In this tab, mail queue can be set. It can be viewed in *Status* → *Mail Queue*.



The screenshot shows the 'SMTP Server' configuration window with the 'Queue Options' tab selected. The window has a title bar with an envelope icon and the text 'SMTP Server'. Below the title bar are four tabs: 'Relay Control', 'Security Options', 'SMTP Delivery', and 'Queue Options'. The 'Queue Options' tab is active and contains two sections: 'Delivery queue settings' and 'Delivery status notification'. The 'Delivery queue settings' section has three rows: 'Maximum number of delivery threads:' with a text box containing '32'; 'Delivery retry interval:' with a text box containing '30' and a dropdown menu set to 'minutes'; and 'Bounce the message to sender if not delivered in:' with a text box containing '5' and a dropdown menu set to 'days'. The 'Delivery status notification' section has two rows: 'Send warning to sender if the message is not delivered after:' with a text box containing '45' and a dropdown menu set to 'minutes'; and 'Report language:' with a dropdown menu set to 'English'.

Figure 16.5 Queue Options

Maximum number of delivery threads

Maximum number of delivery threads that will send messages from the queue (maximum count of messages sent at one moment). The value should be chosen with respect to processor capacity and to speed of the Internet connection.

Delivery retry interval

Interval that will be used for repeated retry attempts for sending an email message.

Bounce the message to sender if not delivered in...

If the message is not delivered in the time defined, it will be discarded and its header including DSN (*Delivery Status Notification*) will be bounced to the sender. It will be also automatically removed from the queue and no more delivery attempts will be taken by the server.

You can also use preset time units (minutes, hours, days) to specify the interval.

However, these time units will not be considered if the messages are delivered via relay SMTP server.

Send warning to sender...

If the message could not be delivered by expiration of this period, sender will be sent a warning (server will continue in sending attempts).

Report language

Language that will be used for error, warning and informative reports.

Note: Reports are stored in the **reports** subdirectory of the directory where *Kerio MailServer* is installed (UTF-8 coding is used). Administrator can modify individual reports or add a new language report version.

16.3 Aliases

Use aliases to create virtual email addresses. The principle of virtual addresses is best understood through examples:

1. Mr. Smith would like all his messages sent to `info@ourcompany.com` to be stored to the *Info* public folder. This can be achieved by the following alias:

`info → #public/Info`

2. Messages sent to invalid addresses (addresses in which the part before @ does not correspond with any user account nor alias) can be delivered to a specified user (typically to the administrator). Use the following alias to achieve this:

`* → Admin`

If this (or the next) alias is not defined, *Kerio MailServer* returns such messages to their senders as undeliverable.

3. The `*` symbol is used as a substitution of any number of characters in an alias (e.g.: `*sms*`, `a*00*`, etc.). The alias will be applied to all email addresses that conform to this mask.
4. To replace just one symbol or character in an alias, use the `?` symbol. (for example, `?ime` stands for `t`ime, `d`ime, etc.).
5. Messages will be delivered to both addresses at once:

`jwayne → info`

`jwayne → jwayne`

It is recommended to specify this alias directly in the user account settings (see [chapter 14](#)), because it is more comprehensive.

Each account or group can be associated with any number of aliases. It is also possible to bind a new alias to an alias already existing. If a message is sent to a username, it is marked by a flag so that the aliases not get looped. If such message arrives to the username marked by the flag, it will be stored in the mailbox that belongs to the last unmarked alias:

jwayne → wayne

wayne → john.wayne

john.wayne → wayne

Note: Aliases can be used also for assigning another email address to a user or a group, or forwarding messages for a user or a group to other addresses. However, it is recommended to specify these settings directly during the process of user definition (see chapter 14.2), or group definition (see chapter 15.1).

Defining Aliases

Define aliases in the *Domain Settings* → *Aliases* section.

First you need to choose a domain for which the aliases will be defined. Aliases always relate to one of the local domains. Therefore, you only need to use the local part of the email address (i.e. the part preceding @) in the alias header.

Add the alias by clicking on the *Add* button. The following dialog window will be displayed:

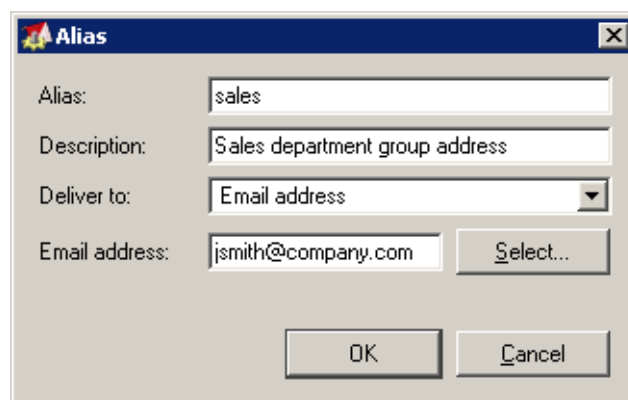


Figure 16.6 Defining Alias

alias

A virtual address (e.g. sales or john.wayne).

Character	Allowed	Character	Prohibited
a-z	allowed	/	prohibited
0-9	allowed	\	prohibited
A-Z	allowed		
.	allowed		
-	allowed		
_	allowed		
?	allowed		
*	allowed		

Table 16.1 Allowed and prohibited characters in aliases

Description

Text description of the alias. May be left blank.

Deliver To

Where messages to this address will be sent to. Select the place where the messages will be stored:

- *Email address* — an email address. Click *Select* to select a user or a group from the list.
- *Public folder* — name of the public folder in this format: #public/Folder. This item is active only in case at least one public folder of *Mail* type has been created.

The same dialog window will be displayed by clicking on the *Edit* button. Remove the alias using the *Remove* button.

Alias Check

When creating more complex aliases (multiple aliases), it is easy to make mistakes (e.g. by mistyping a name). *Kerio MailServer* has an Alias Check feature that displays a list of local accounts and external addresses to which the email will be delivered.

Use the *Check Address* button to check aliases. Enter the address that you would like to run a check on (if an alias is selected in a list, it will be displayed as a choice). After the check has been performed, the result is displayed (i.e. the list of addresses to which the alias will deliver messages).

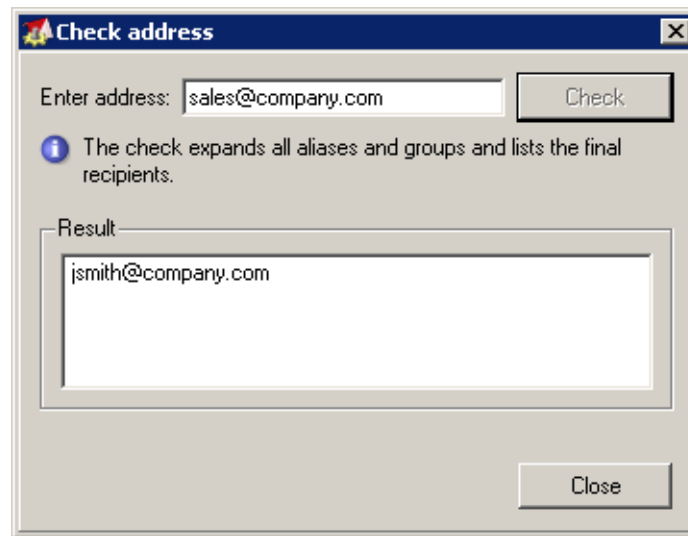


Figure 16.7 Check Address

16.4 remote POP3 mailboxes

Kerio MailServer can retrieve messages from POP3 boxes at different mailservers and deliver them to local mailboxes or send them to different email addresses.

Warning: Retrieving POP3 mailboxes is controlled only by a scheduler (see chapter 10). It is important to realize that mail will not be downloaded from remote POP3 accounts automatically when a client connects to his/her *Kerio MailServer* mailbox or sends an email.

Defining Remote Mailboxes

Remote mailboxes from which email should be retrieved can be defined in the *Configuration* → *POP3 Download* section using the *Accounts* tab.

Use the *Add* button to display a dialog box that allows users to add a new account (a remote mailbox). With the *General* tab, set the basic parameters for accessing the mailbox and the delivery method for the downloaded email.

POP3 Server

The DNS name or IP address of the POP3 server where the mailbox is located

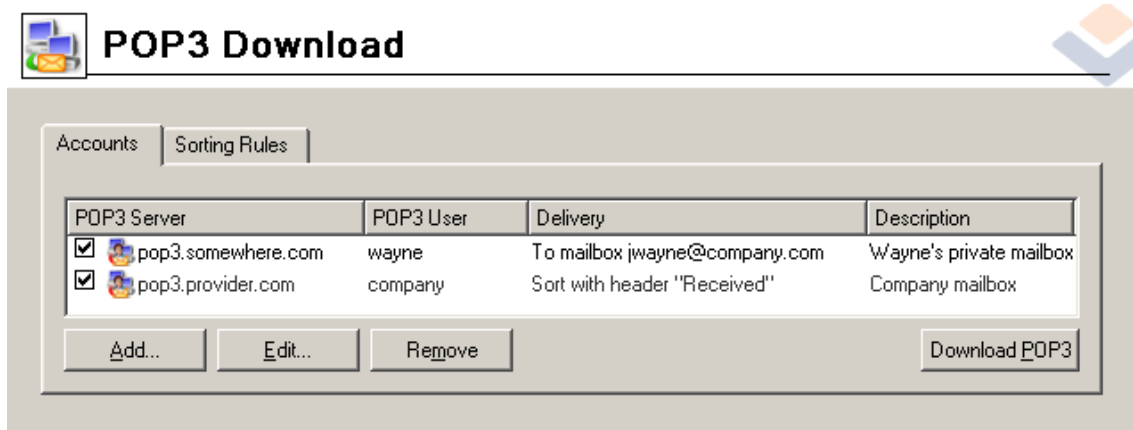


Figure 16.8 Remote POP3 download

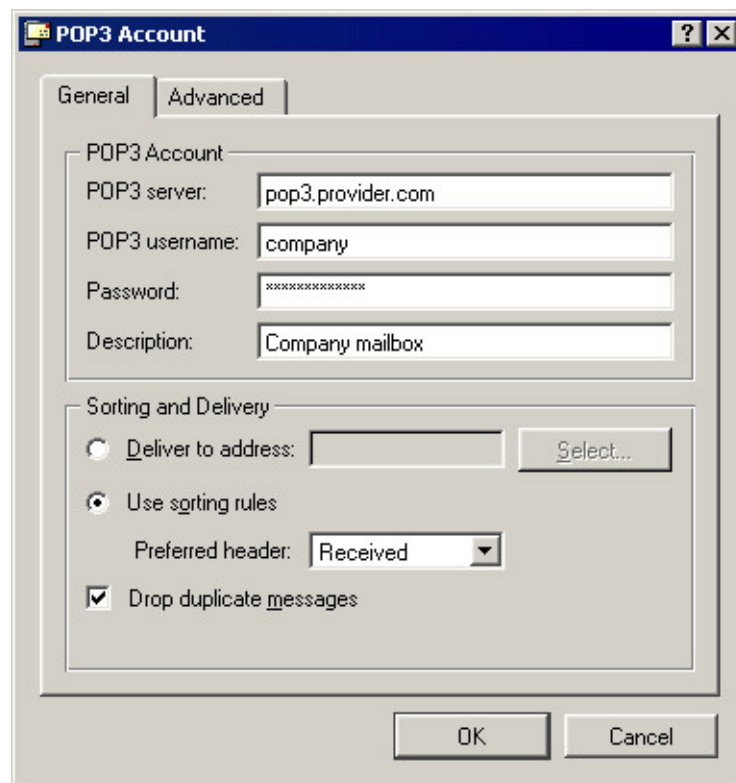


Figure 16.9 Defining Remote Mailboxes

Username and Password

The username and password for the mailbox

Description

Any text description of the POP3 account

Deliver to address

All messages from the mailbox will be sent to one address. Here you can enter a local user, a local group, an alias or an external email address. You can choose the local user or group from a list using the *Select* button.

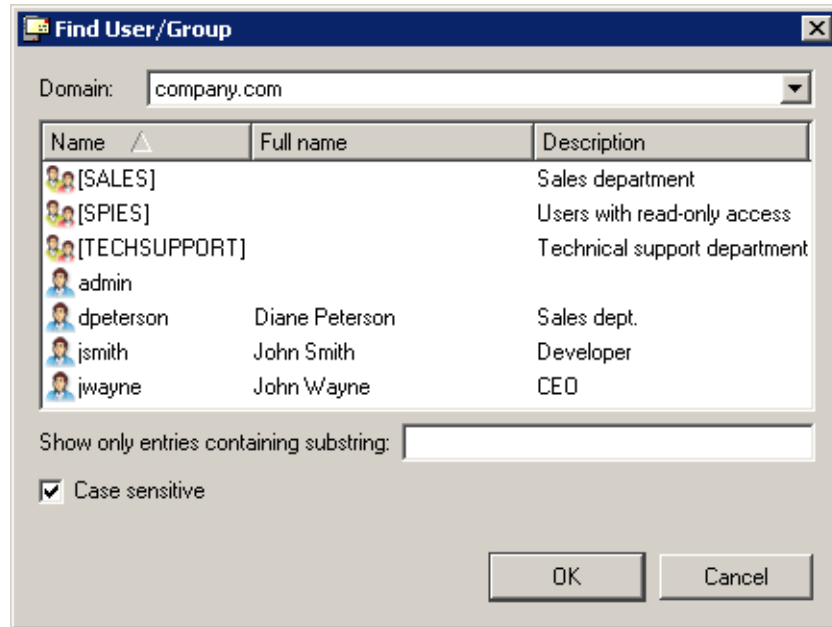


Figure 16.10 Find User/Group dialog

This dialog (see picture 16.10) allows to search for a specified string and specify the settings for the case-sensitivity. These options make the search faster, especially when searching through too many users and groups in the domain.

Use sorting rules

Messages from this mailbox will be sorted according to the sorting rules (see below).

Preferred header

The primary header entry that will be used for sorting. Here you can specify a header entry (the name of the header without a colon) or choose one from the list (*X-Envelope-To*, *Received* or *Delivered-To*). If the entry is not found in the mail header or no address complies with any rule, other header entries are searched — *Resent-To* and *Resent-Cc*, *To* and *Cc*. If an address is not found in these entries the message will be delivered according to an implicit rule (described below) or will be discarded.

Drop duplicate messages

If this option is enabled, and identical copies of one message are stored on a remote mailbox, only one copy will be downloaded (the others will be dropped).

Messages are duplicated when a message with more recipients (included in the domain) in the header is delivered into the domain mailbox. In such a case, the

message is delivered to the mailbox that many times how many recipients were originally specified. These messages differ only in their SMTP envelope. However, the envelope is cut out when the message is saved in the mailbox. All copies of a message stored in the mailbox will be identical. During standard POP3 sorting each recipient receives all the messages as his/her address is included (this means that each recipient receives the same number of copies as number of recipients). Dropping duplicate messages ensures that each recipient receives one of the copies only.

You can define the following parameters with the *Advanced* tab:

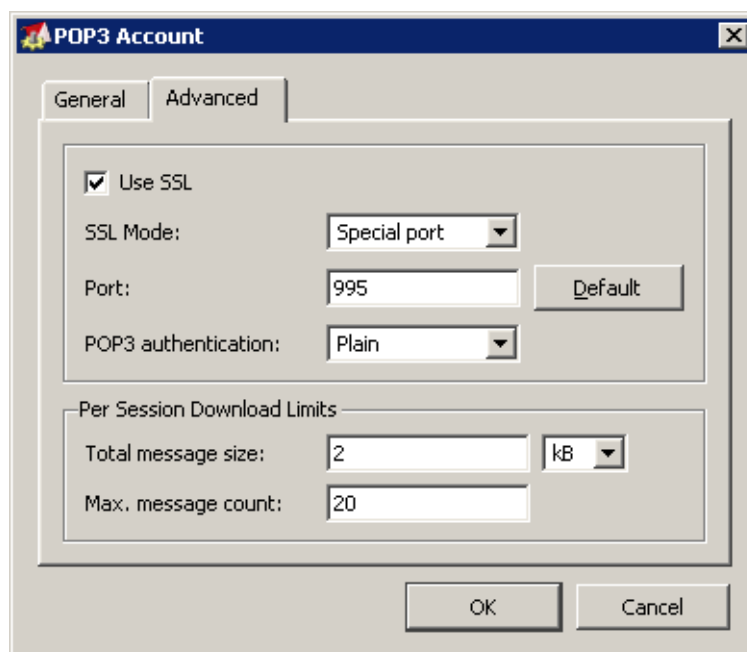


Figure 16.11 More detailed settings for downloading POP3 mailboxes

Use SSL

The connection with the POP3 server will be secured (encrypted) by SSL.

SSL Mode

The security method for communication with the POP3 server. Options: *Special port* (the SSL connection will be established on a port different from a standard POP3 port) or *STLS command* (first, a non-encrypted connection will be made and once it is established it will be switched to an encrypted mode using the STLS command). Contact the POP3 server administrator for more information about securing communication with the POP3 server.

POP3 authentication

The POP3 server authentication method: *Plain* (the password is sent in its normal form) or *APOP* (the password is encrypted to prevent tapping and misuse). Contact the POP3 server administrator for more information.

Per Session Download Limits

- *Total message size* — this entry enables specification of a maximal total size of messages downloaded within one POP3 session. The zero value means that no limit has been set.
- *Max message count* — The maximum number of messages that will be downloaded during one connection (if there are more messages at the server they will be downloaded in the next session). The zero value means that no limit has been set.

The total message size limit protects the user from repeated downloads of identical messages in cases where POP3 session was interrupted.

The main reason is the principle of POP3 protocol. On the server, messages to be deleted are not physically removed until a successful disconnection by the QUIT command. If the POP3 session is interrupted, messages are not removed and the server downloads them again within the following POP3 session. Setting of these limits therefore helps to control of data flowing in repeated sessions.

For temporary remove of appropriate rules use matching fields next to the rule definitions.

Sorting Rules

Sorting rules define how messages downloaded from a remote POP3 mailbox will be delivered to and divided between local users or forwarded to external email addresses. Use the *Sorting Rules* tab to define sorting rules.

Use the *Add* button to add a new sorting rule:

Sort Address

Email address that will be searched for in the selected message header entry. It must be complete; a substring is not acceptable.

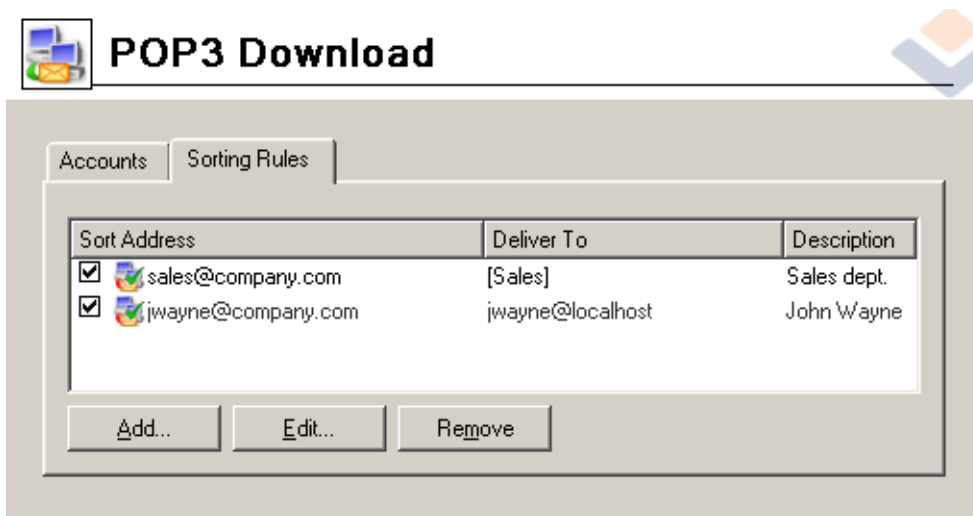


Figure 16.12 Sorting Rules

Deliver To

This entry defines the recipient of the message complying with the rule. Here you can specify:



Figure 16.13 Sorting Rule dialog

- local user or group of users — local users/groups of users can be selected using the *Select* button
- alias — enter an appropriate alias
- external email address — any address

TIP: To deliver messages to groups, you must assign addresses to these groups (or you can create an alias). For details refer to chapter 15.

Description

A commentary on a sorting rule (e.g. purpose explanation)

For temporary remove of appropriate rules use matching fields next to the rule definitions.

Special Sorting Rules

In sorting rules you can also define rules in this format:

- * → address (implicit rule) Email messages not complying with any rule will be delivered to this user (group). If this rule is not defined, such messages will be discarded.
- *@domain.com → *@anotherdomain.com All messages containing the specified domain will be forwarded to another specified domain.

No other usage of the asterisk character (e.g. for completing a part of an address) is allowed.

16.5 Receiving Email Using ETRN Command

In the *Configuration* → *ETRN Download* section you can define SMTP servers from which email will be downloaded using the ETRN command (usually these will be the domain's secondary or tertiary servers).

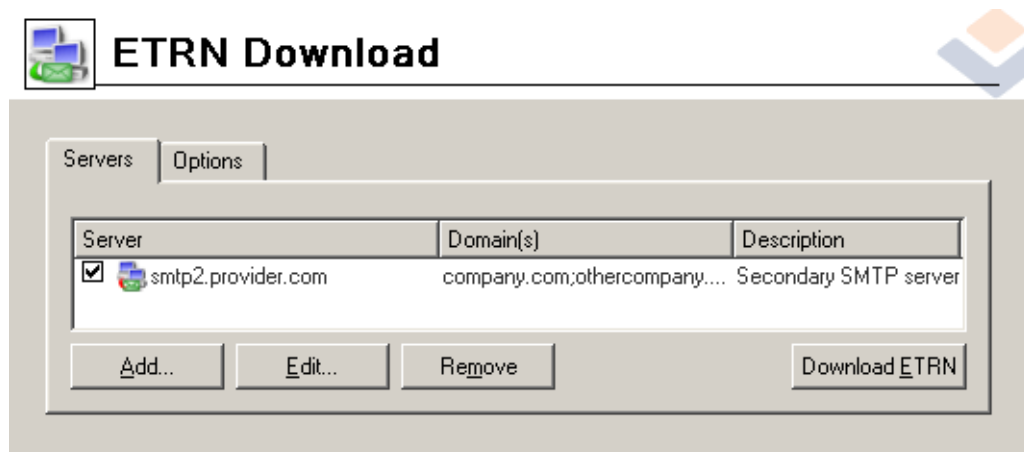


Figure 16.14 ETRN Download

Use the *Add* button to add a new server:

Server

The DNS name or IP address of the server

Domain(s)

A list of domains for which the server stores email. Separate individual domains using a semi-colon (;).

Figure 16.15 Setting parameters for accessing the server

Description

A commentary on the ETRN server definition. May be left blank.

Authentication is required

Enable this option if the server requires username/password authentication.

User, Password

Appropriate user name and password

Use the *Edit* button to change the settings for server access. Remove servers using the *Remove* button. For temporary removal of this server, use matching fields next to the server definition.

The *Options* tab allows users to set the maximum delay time of dial-up line response.

16.6 Advanced Options

In the *Configuration* → *Advanced Options* section you can set several advanced parameters for the mailserver.

Miscellaneous tab

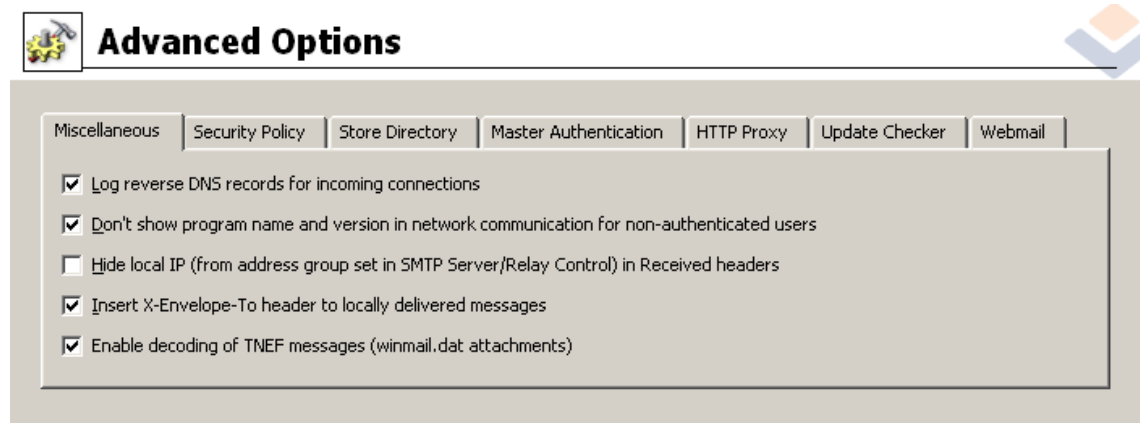


Figure 16.16 Miscellaneous tab

Log reverse DNS records...

Convert IP addresses of remote clients and servers connecting to *Kerio MailServer* to DNS names (using reverse DNS requests). This makes logs more comprehensible but it can also decrease the performance of *Kerio MailServer*.

Don't show program name and version...

Enable this option if you do not wish to reveal the version and name of the mailserver application for this domain.

Hide local IP in Received headers

Kerio MailServer will hide the local IP address (included in the IP address group defined in the *Relay Control* tab of *Configuration* → *SMTP server*) in the *Received* part of the message header.

Each SMTP server that the message passes through inserts an entry into this field, specifying where the message came from, where it is going and who received it. This implies that the first record in the *Received* header contains the sender's email and IP addresses. If the SMTP server is placed on a private network behind a firewall, the client's private IP address is inserted. This means that outgoing email messages can carry information about a private network that would normally be hidden from the Internet. This information could make it easier for a potential hacker to attack such networks. Only switch this option on if *Kerio MailServer* is installed on a private network behind a firewall (even if it runs on the same machine as the firewall).

There is a connection to relay control here so that the mailserver recognizes local IP addresses. In relay control, a group of local IP addresses is usually used to define addresses from which mail can be sent to any domain (see chapter 16.2).

Note: If relay control is disabled or no local IP address group is defined, this option will have no effect.

Insert X-Envelope-To header...

Defines if the X-Envelope-To entry will be inserted into the header of messages delivered locally. X-Envelope-To is the original recipient address based on the SMTP envelope. This option is useful especially if there is a domain mailbox in *Kerio MailServer*.

Enable decoding of TNEF messages

TNEF (Transport Neutral Encapsulation Format) is a *Microsoft's*, proprietary format used to send messages with format extensions from *MS Outlook*. The `winmail.dat` file is attached to any message sent in this format. It contains a complete copy of the message in RTF along with all attachments. This implies that if a user does not access their email via *MS Outlook* and an email message with an attachment in this format will be delivered to their mailbox, the attachment cannot be opened.

The TNEF decoder built-in *Kerio MailServer* decodes TNEF messages at the server's side in the standard MIME format and helps avoid `winmail.dat` attachment difficulties.

Use this option if users do not access their email only by *MS Outlook*.

Security Policy tab

Kerio MailServer allows setting of security policies, i.e. the minimum required security level. These settings can be established in the *Configuration* → *Advanced Options* section in the *Security policy* tab (see picture 16.17).

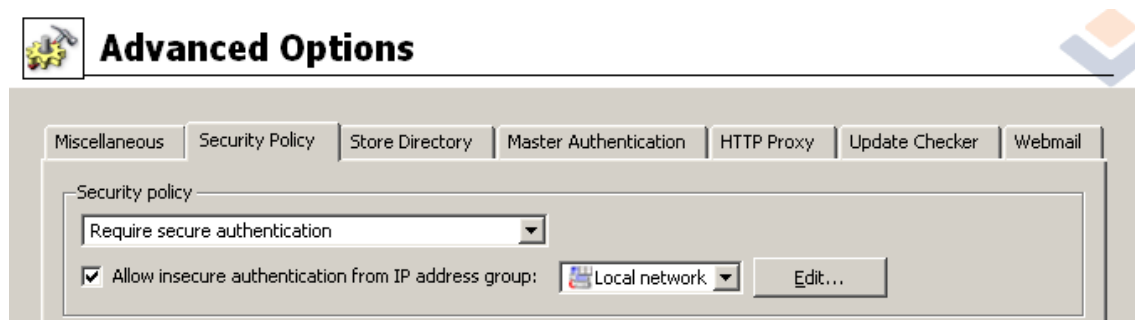


Figure 16.17 Security Policy tab

The menu at the top of the page allows you to choose from one of these policies:

No restrictions

Self explanatory.

Require secure authentication

Kerio MailServer will always require secure user authentication. This implies that the authentication must be performed by using one of these methods — CRAM-MD5, DIGEST-MD5, NTLM, or the user must use an SSL tunnel (by enabling SSL traffic in their email clients).

If users access their email by *Kerio WebMail* where no one of the authentication methods can be applied, the SSL-secured HTTP protocol is used automatically.

Once the secured authentication is set, it is possible to allow non-secured connections from a specified IP group. This group can be either selected from existing groups or a new one can be created. For details on IP groups definition, refer to chapter 13.1.

Warning: Do not apply this method if users use saving passwords on the server in SHA format.

Require encrypted connection

When this option is activated, client applications will be able to connect to any service using an encrypted connection (the communication cannot be tapped).

SSL traffic must be allowed to all protocols at all client stations. The secured connection is set automatically upon a successful connection to *Kerio WebMail*.

The only exception from this restriction is the SMTP protocol. Due to the plenty of SMTP servers which do not support SMTPS and STARTTLS, it is not possible to allow the secure version of the protocol only. To still provide sufficient security, the SMTP server requires secure password authentication for the SMTP protocol upon enabling the *Require encrypted connection* option. Name and password are still sent by one of the supported secure authentication methods.

After the security policy is defined, you can create an exception for a group of IP addresses for which the secured connection will not be required. For this purpose, either a new IP group can be created or an existing one can be selected. For information on IP address settings, see chapter 13.1.

If you decide for this communication protection method, make sure that all users have a valid authentication certificate installed on their client stations (for more information, see chapter 11).

Supported authentication methods

Kerio MailServer supports the following methods of user authentication:

- CRAM-MD5 — password authentication method (using MD5 digests). This method is quite common and many email clients provide support for it.
- DIGEST-MD5 — password authentication method (using MD5 digests).

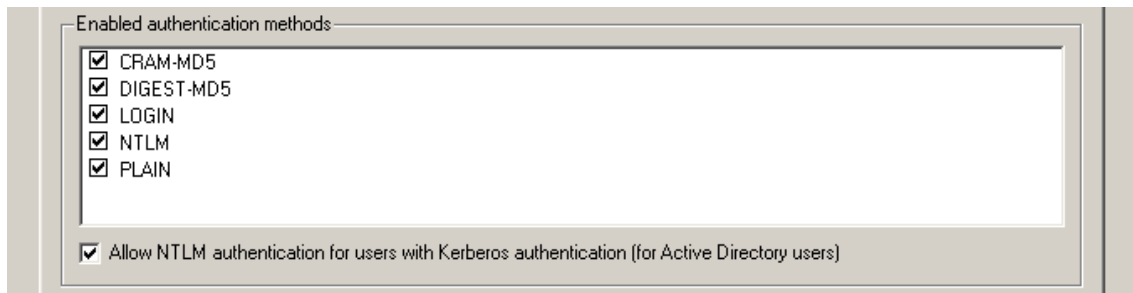


Figure 16.18 Authentication methods

- LOGIN — user passwords are completely unprotected during transfer. If this method is used, it is strongly recommended to enable SSL tunnel connection.
- NTLM — this method can be used only in case users are authenticated against an *Active Directory* domain. It is applicable only to the user accounts that were imported from *Active Directory*.
- PLAIN — user passwords are completely unprotected during transfer. If this method is used, it is strongly recommended to enable SSL tunnel connection.
- APOP — the authentication method is not displayed in the list, *Kerio MailServer* uses it automatically to download POP3 accounts.

The server provides all the above mentioned authentication methods. They are ordered the same way as in the table below (from CRAM-MD5). If the selected method is supported by the client, the other methods will not be used. However, a problem may occur if the password is stored in the secure format (SHA1). If this encryption method is used, only LOGIN and PLAIN authentication methods can be used. If you select the secure CRAM-MD5 and DIGEST-MD5 methods, the system selects one of the secure authentication methods and it will be impossible to log in to *Kerio MailServer*. If the password is stored in the SHA format, disable all methods but LOGIN and PLAIN.

Further recommendations:

- If a client authentication method fails, it is recommended to disable it in *Kerio MailServer* (uncheck it in the *Enabled authentication methods* list).
- For all authentication methods, it is recommended to enable SSL login to the mail clients.

Operational system	Authentication against Active Directory	User mailboxes are stored locally and passwords are secured by DES encryption	User mailboxes are stored locally and passwords are secured by SHA encryption
<i>MS Windows</i>	NTLM LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN
<i>LINUX</i>	LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN
<i>Mac OS X</i>	LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN

Table 16.2 Authentication methods

Check *Allow NTLM authentication for users with Kerberos authentication* to allow users from *Active Directory* to authenticate when attempting to log in to *Kerio MailServer*. In order for the NTLM authentication to be functional, both the computer as well as the user account have to be parts of the domain used for authentication. The NTLM (SPA) authentication must be also enabled in users' mail clients.

Warning:

- NTLM (SPA) can be used only on Windows operating systems. *Linux* and *Mac OS* operating systems do not support this type of authentication (see table 16.2).
- NTLM (SPA) authentication is not available if *MS Outlook* extended by the *Kerio Synchronization Plug-in* is used.

In the *Account lockout* section the following parameters can be defined (see figure 16.19):

Enable account lockout

When this option is selected, user accounts will be locked based on the following rules. These settings protect the user accounts from being misused.

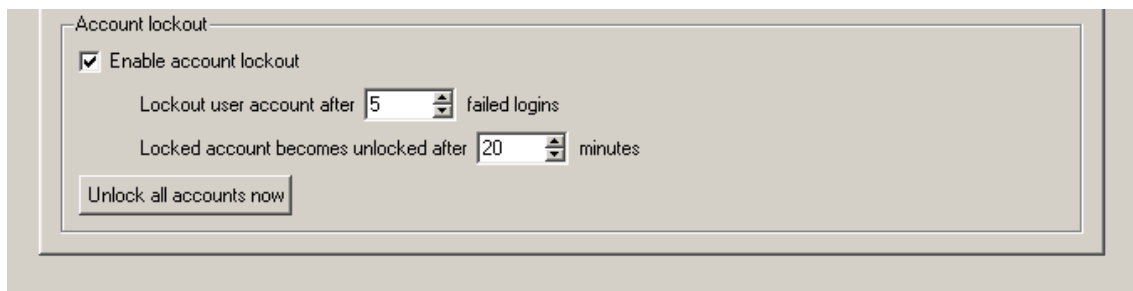


Figure 16.19 Account lockout

Lockout user account...

You can specify a number of failed logins from one IP address that will be allowed.

Locked account becomes unlocked...

This information defines when the account will be unlocked automatically.

Use *Unlock all accounts now* to unlock all accounts previously locked.

Store Directory tab

The *Store Directory* tab contains settings of directories for message storing (user and public folders) and backup. Information about private and public folders, logs, messages that are to be sent and files that are just being checked by antivirus are saved into the *Store Directory*.

Path to the store directory

Define the absolute path to the store directory (according to the operating system on which *Kerio MailServer* is running).

Watchdog Soft Limit

If the value specified is reached, *Kerio MailServer* will automatically warn users about this fact upon each login to the administration console. After the limit is reached, it will be recorded in the *Error* log (for more information, see chapter 23.6).

Watchdog Hard Limit

If this limit is reached, *Kerio MailServer Engine* and *Kerio MailServer Monitor* will be stopped. *Kerio Administration Console* can be run. Immediately after login, the critical limit error message is displayed. This information is also recorded into the *Error* log (for more information, see chapter 23.6).

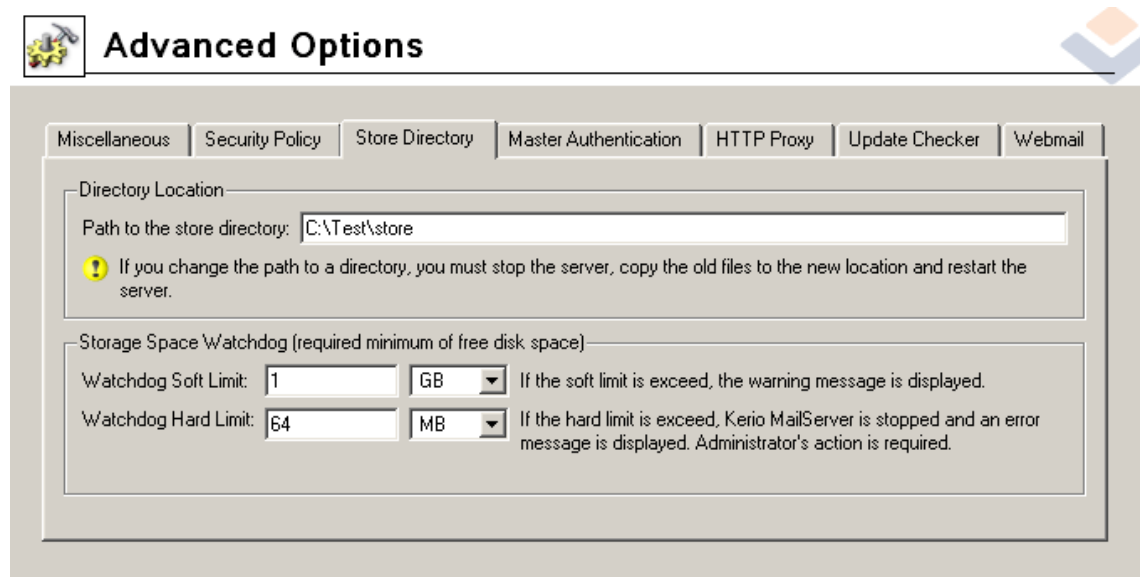


Figure 16.20 Store Directory tab

Warning: Do not set the hard limit for 0, otherwise an error message or warning will be displayed when a new mail is delivered.

Changes in the paths are effective only after restarting the *MailServer Engine*. If you don't change these settings immediately after the *Kerio MailServer* installation, you will need to first stop the *Engine* and then move files from the old location to the new one and then start the service again.

Master Authentication tab

Master authentication password is a special password. It can be used by specific applications to access *Kerio MailServer* accounts without knowing individual corresponding passwords.

A typical application using master authentication is the *Kerio Exchange Migration Tool*. This tool needs to access individual accounts to perform the migration. Correct settings of the master authentication enables the migration tool to access any accounts not having to specify passwords for individual accounts (more details in chapter 37).

Warning:

1. The *Master Password* cannot be used to access user accounts from email clients or via *Kerio WebMail*. It is not a versatile administrator password (it is not possible to use it for authentication to *Administration Console*).
2. Since *Kerio MailServer 6.0.5*, the *Master Password* is stored in the new SHA format. For this reason, the original password will not work after server configuration is transferred to an older version and it must be changed.

Master authentication settings can be defined in Configurations → *Advanced Options*.

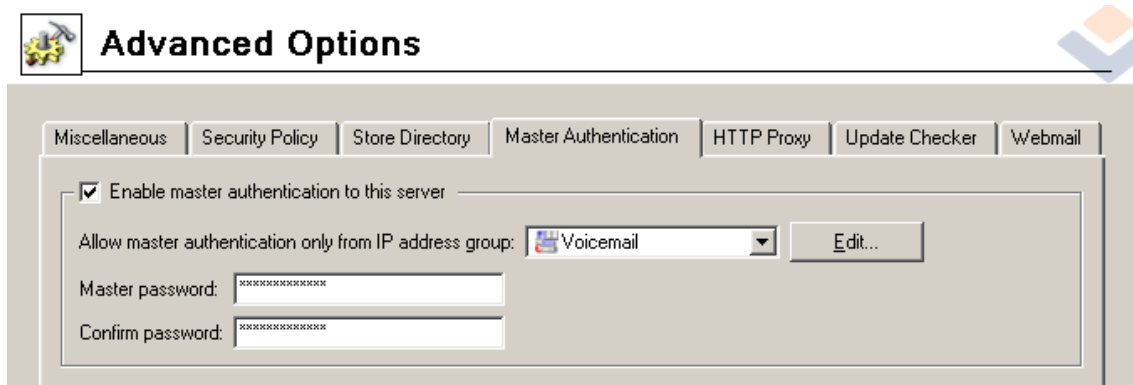


Figure 16.21 Master Authentication tab

Enable master authentication...

This option enables/disables *Kerio MailServer* master authentication. We recommend keeping this option disabled unless it is needed (e.g. by *Kerio Exchange Migration Tool*).

Allow master authentication only from IP address group

Select an IP address group where master authentication will be exclusively allowed. The group must be first defined in *Configurations* → *Definitions* → *IP address groups* (see chapter 13.1). For security reasons it is not possible to allow Master authentication from any IP address. You can simply add a new IP group using the *Add* button.

Master Password

Define a password that will be used for access to all accounts. This password should be known by as few persons as possible. If the *Master Password* arrives to an unauthorized person, privacy of all user accounts on the server can be broken!

Confirm password

The password confirmation is required to eliminate typos.

HTTP Proxy

If *Kerio MailServer* runs on a host behind a firewall, it can be connected to the Internet via a proxy server. This feature can be useful for example for upgrade downloads or/and for searching for new versions of *Kerio MailServer* or antivirus application.

Use HTTP proxy for ...

Insert HTTP proxy address and port on which the service is running.

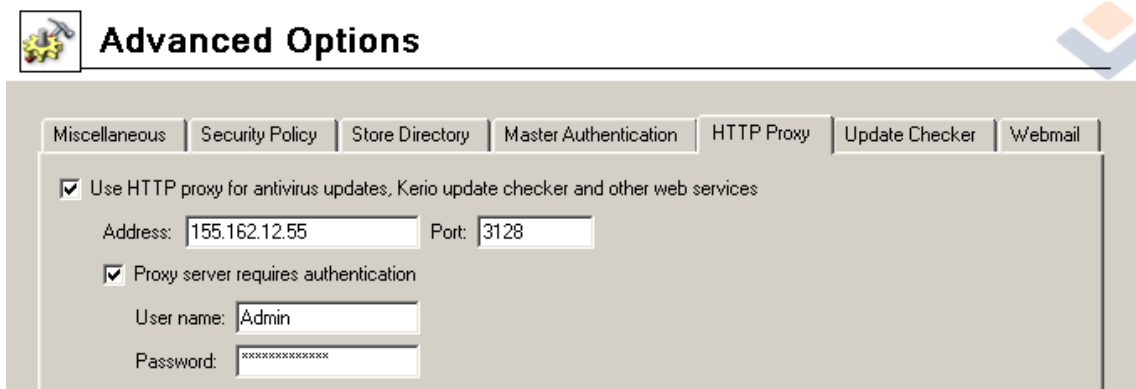


Figure 16.22 HTTP Proxy tab

Proxy server requires authentication

Username and password must be specified if the proxy server requires authentication.

Username

Insert your user name to connect to the particular proxy server.

Password

Correct password must be specified for a successful connection.

Update Checker tab

This tab enables users to perform administration of *Kerio MailServer* version updates.

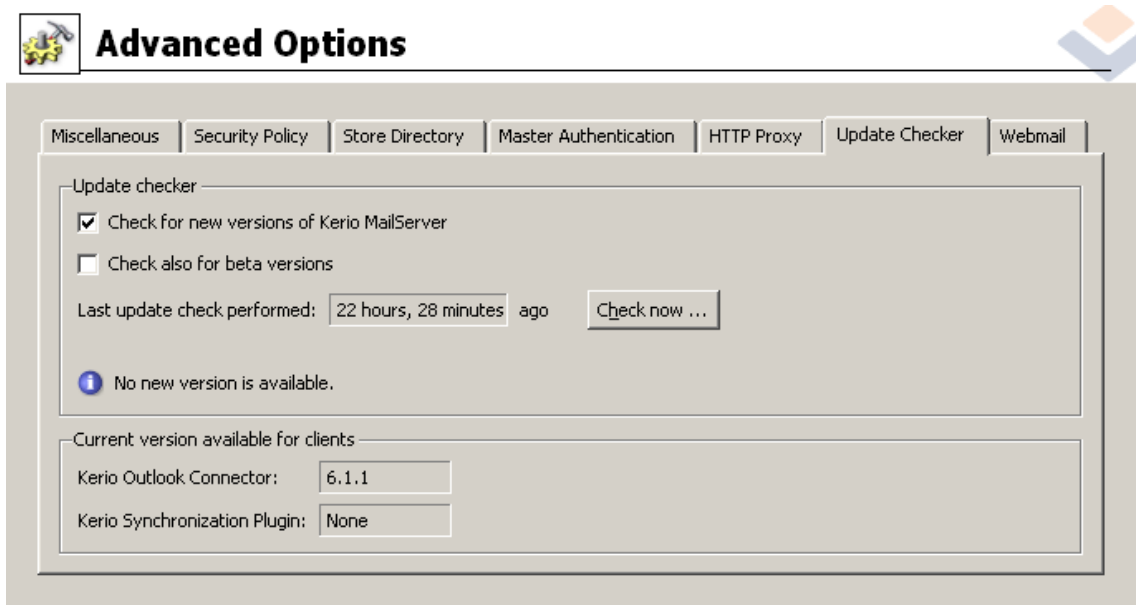


Figure 16.23 Update Checker tab

Check for new versions of...

Check this option to enable the automatic updates of *Kerio MailServer*. New versions of *Kerio MailServer* are stored in the `/store/temp` directory, where *Kerio MailServer* is installed.

Check also for beta versions

This option checks for new beta versions of *Kerio MailServer*.

Note: If you want to participate in beta version testing, enable the *Check also beta versions* option. If the *Kerio MailServer* is used in production, the beta versions are not recommended — do not enable this option.

Last update check performed ...

Time since the last update check. The system checks for new versions of the product every 24 hours.

Click the *Check now* button to check for the new version. When the new version is found, the user can download it. If no new version is available, the user is notified.

If a new version was released by *Kerio Technologies*, the *Update* tab will contain link to the download web page. The installation package also contains automatic installations of *Kerio Outlook Connector* and *Kerio Synchronization Plug-in*:

Kerio Outlook Connector is updated automatically. The *Current version available for clients* field displays the information about the version currently used.

New *Kerio Outlook Connector* versions are stored in the

`Kerio\MailServer\webmail\download`

Kerio Synchronization Plug-in is updated the same way as *Kerio Outlook Connector*. The *Current version available for clients* field displays the information about the version currently used.

New *Kerio Synchronization Plug-in* versions are stored in the directory

`Kerio\MailServer\webmail\download`

Warning:

- In order to perform an automatic upgrade of *Kerio Outlook Connector* and *Kerio Synchronization Plug-in*, the HTTP or HTTPS service must be running.
- If only HTTPS traffic is allowed in *Kerio MailServer* (e.g. for security reasons), it is necessary that a trustworthy *Kerio MailServer* certificate is installed in *Internet Explorer* of all clients (a self-signed certificate can be used). Otherwise, new versions will not be updated automatically.

WebMail

In *Kerio Administration Console*, several parameters for *Kerio WebMail* can be set (see figure 16.24):

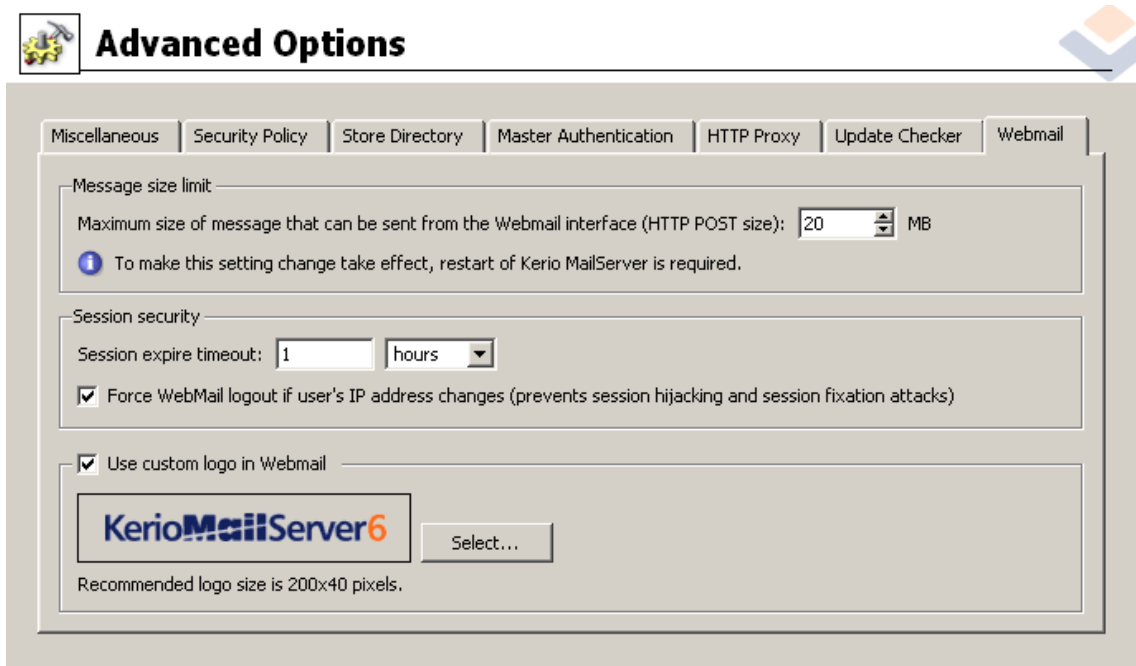


Figure 16.24 WebMail

Message size limit

Setting of maximal message size can be used for the following purposes:

- to limit size of attachments sent to *Kerio WebMail* by the an HTTP POST request,
- to set maximal size of memory allocated in *Kerio MailServer* to each HTTP POST request.

For better understanding of the limit, here is an explanation of how a message written in *Kerio WebMail* is sent to *Kerio MailServer*. Each new message composed in the web interface is sent by a browser via HTTP protocol using an HTTP POST request to *Kerio WebMail*. The interface receives the message and processes it so that *Kerio MailServer* can send it to the addressee by SMTP protocol.

Each HTTP POST request contains one message including a message body, all headers and attachments. The limit set by this option narrows size of any HTTP POST request directed to *Kerio WebMail*. This means that any limit set for requests also limits size of email messages.

Size limit set for HTTP POST requests is applied to any files sent from *Kerio WebMail* to *Kerio MailServer* and it is applied to all *Kerio MailServer* users. The default value

for maximal size of messages sent from *Kerio WebMail* is 20 MB. This limit should be generally satisfactory for these purposes.

The minimal value for the limit is 2 MB. If any lower limit is entered in the *Maximum size of messages that can be sent* entry, the 2 MB value is set automatically.

If a message includes any attachments, they are encrypted by the Base64 method. This type of encoding is able to increase the size of transmitted data even by one third (in case of binary data). This means that, for example, the minimal 2 MB limit might also allow just 1 — 1,5 MB attachments.

It is necessary that a memory allocation value is specified in *Kerio MailServer* for HTTP POST requests. The more bulky the request is the more memory must be allocated. This implies that the size of the allocated memory changes according to changes in the size limit.

Warning: Any time the limit is changed, it is necessary to restart *Kerio MailServer* since the memory allocation is changed as well.

Session security

Session security depends on methods and manners how users manage connection to *Kerio WebMail*. Users often simply close their browsers without logging out of *Kerio WebMail*. In such cases, the session is not interrupted and it can be misused more easily (the session is the more risky the longer it takes). For this reason, it is possible to set session timeout. If the user does not use the session over the timeout, connection to the server is interrupted automatically when this timeout runs out. By default, the timeout is set for one hour.

The *Force WebMail logout if user's IP address changes* option uses another method to protect the session. It might happen that a session of one user is hijacked by an attacker (especially if SSL-secured HTTP is not used) to access the server. Connection of an attacker to the session changes the client's IP address. If the *Force WebMail logout if user's IP address changes* option is enabled, *Kerio MailServer* detects change of the IP address and terminates the session.

Warning:

- The “anti-hijack” protection must be disabled if *Kerio MailServer* users share their accounts. The option disallows connection to a single account from multiple hosts (IP addresses) at a time.
- The “anti-hijack” protection also cannot be applied if your ISP changes IP addresses during the connection (e.g. in case of GPRS or WiFi connections).

Select a logo for Webmail

At the top of each page of *Kerio WebMail*, *Kerio Technologies* logo is displayed. However, you can use any other logo or image instead (for more information on logo configuration, refer to chapter 12.2). The image parameters are as follows:

- Format: GIF
- Size: 200x40 pixels

Click *Select* to browse to the logo file.

Chapter 17

Antispam

Antispam protection of SMTP server protects users from spam. The configuration of antispam protection can be set in *Configuration/Spam Filter*:

17.1 Spam Rating tab

Use the *Spam rating* tab to fight spam using *SpamEliminator*. This filter consists of two main parts. One of them is based on statistical filtering using the message's contents (keywords, etc.). Each incoming message is assigned a numeric score according to the number of characters significant for spam messages. A higher score indicates a higher probability of spam.

The other part of *SpamEliminator* is a so-called Bayesian filter, which is able to “learn” to recognize spam messages. This filter compares the individual spam characteristics with actual messages. This method, however, requires user input. Users have to reassign the incorrectly evaluated messages to correct types (spam / non-spam) so that the filter learns to recognize them in the future.

Note: *SpamEliminator* checks only messages which do not exceed the size of 128 kB since spam messages are mostly not so large and checking of large messages might overload or slow down the server's performance.

Since individual users must check the messages, the spam evaluation tools must be embedded in mail clients. By default, these tools include only *MS Outlook* with the *Kerio Outlook Connector* and the *Kerio WebMail* interface. Users can click special buttons in the toolbar to mark an incorrectly evaluated message as non-spam.

For email clients with IMAP accounts as well as for *MS Entourage* (for IMAP and Exchange accounts), there is another method of how to teach the Bayesian filter. These users can mark incorrectly classified messages by moving them to appropriate folders. If users want to mark a message as spam, they can move such messages to *Junk E-mail*. To mark a message as not spam, they can move it to *Inbox*.

TIP: To use this method as efficiently as possible, set users a spam rule (either when creating user accounts in *Kerio MailServer* or by defining a corresponding sieve rule for incoming mail). Any messages marked by *Kerio MailServer* as spam will be automatically moved to the *Junk E-Mail* folder. This will make the Bayesian filter learn about new spammers. Messages that are incorrectly marked as spam can be moved to *Inbox* by hand.

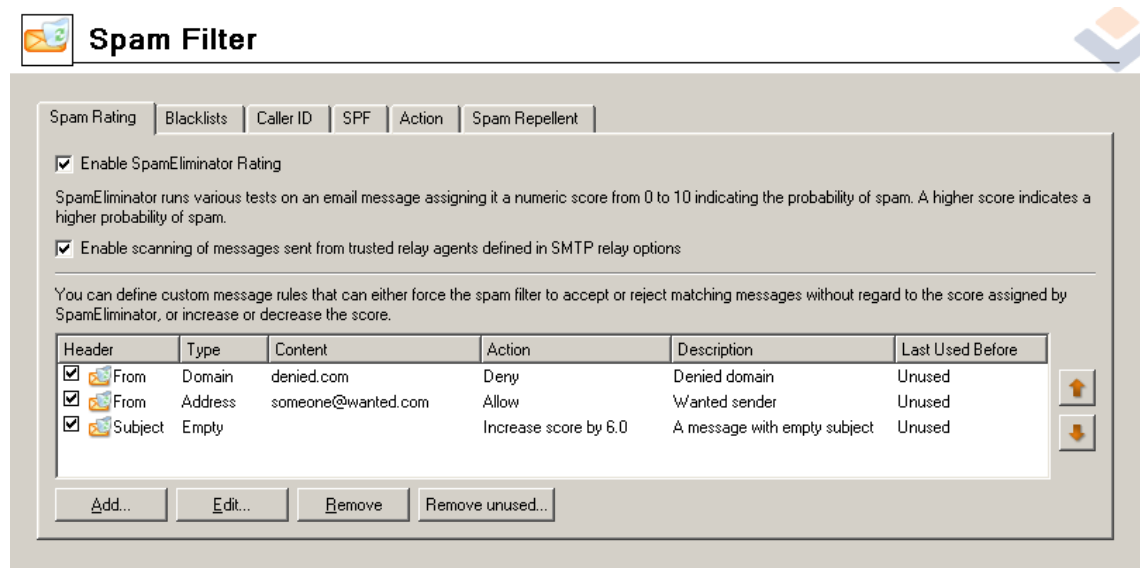


Figure 17.1 Spam Rating tab

Enable SpamEliminator Rating

SpamEliminator evaluates each incoming message using scale from 0.0 to 10.0 (this number includes various results of *SpamEliminator* evaluations). The higher the value, the more probable is that the message includes a spam.

Test results are stored in the X-Spam-Status header.

Enable scanning of relayed messages...

Turns the scanning of messages sent by local (authenticated) users on/off. Groups of trustworthy IP addresses can be defined in *Configuration* → *SMTP Server* → *Relay Control* (for detailed information, refer to chapter 16.2).

Defining email filtering rules

In addition to enabling *SpamEliminator*, the *Spam Rating* tab enables making a list of custom spam filtering rules. Each row stands for one filtering rule. Using matching fields on the left you can activate or disable individual rules. This way you can switch the rules temporarily on and off without the need to remove them and add them again. You can also use arrow buttons to reorder rules (the order takes no effect in their execution, it helps the administrator to keep the *Kerio MailServer* administration clearer and more comfortable).

Click the *Remove* and *Remove unused* buttons to delete rules from the list.

Use the *Add* button (or *Edit*) to open a dialog where rules can be defined or modified.

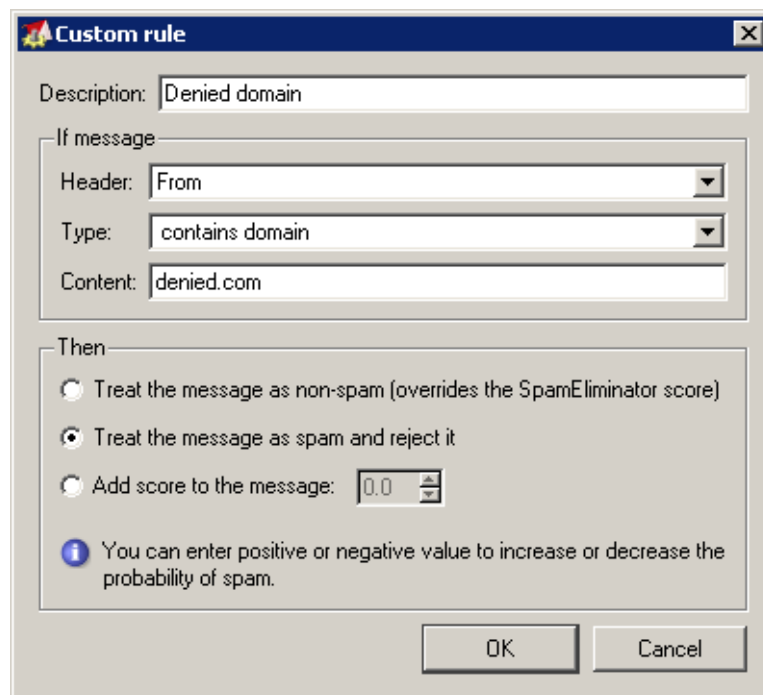


Figure 17.2 Defining rule

Filtering rules consist of the following items:

Description

Comment on the rule (for use of administrator).

Header

Tested part of email message header. You can choose from various predefined options (*From*, *To*, *Cc*, *Subject* and *Sender*) or create a custom one (i.e. X-Mailer). Do not use colons while defining header names.

The *From* and *To* items slightly differ from the other ones. These items are checked for the *From* and *To* headers in email and for headers included in SMTP envelopes. The *From* item is compared with MAIL FROM: and the *To* item is compared with RCPT TO:. Any other items are compared with headers included in the email itself only.

This implies that messages are checked by the *From* and *To* related rules even before they are added to the message queue, i.e. before they are accepted and received by *Kerio MailServer*. Rules for items included by email (e.g. *Subject* or *Cc*) are not tested until accepted in the message queue.

If a rule is created that includes *From* or *To* as a testing item and all messages meeting the rule are considered as spam (the *Treat the message spam and reject it* option), the rule does not apply to the *Action* tab setting (see chapter 17.4). These settings cannot be applied unless the corresponding message is accepted by *Kerio*

MailServer. Any message meeting the rule is rejected and marked with the 553 error code (this code means that it is a persistent error and the SMTP server will not retry to deliver it) and a DNS message is sent to the sender.

Type

Type of condition under which the entry will be tested. Available types:

- *Is empty* — the item is empty
- *Is missing* — the message does not contain the specified message header
- *Contains address* — the item contains a specific email address
- *Contains address with domain* — the item contains all email addresses from this domain. Enter the mail domain, i.e. the second part of the email address right from the @ character, in this field.
- *Contains substring* — the item contains specific string of characters (a word, a piece of text, a number, etc.).
- *Contains binary data* — using this condition, the above-mentioned specific characters as well as binary data that may be contained in spam messages can be recognized. Binary data are characters that have a different meaning in each character set (e.g. specific national characters).

Content

Required entry content (according to the selected type).

Once a rule is set, select one of the following actions:

Treat the message as non-spam

Messages treated as spam may be accepted as non-spam using this option.

Treat the message as spam and reject it

Any message meeting the rule will be marked as spam and action set on the *Action* tab (see chapter 17.4) will be applied to it, regardless of the spam filter.

Add this value to the message's spam score

Define score value for *SpamEliminator* (the higher the value, the lower is the possibility that a message passes through the filter). Value that you match with messages meeting this rule will be added to the corresponding *SpamEliminator* evaluation (negative values protect messages from being considered as spam). Settings defined on the *Action* tab will be applied to the rule (see chapter 17.4).

Examples:

1. Suppose that you want that the server blocks all email sent from `someone@undesirable.com`. Define a rule where the *From* entry will be tested. Choose the *contains address* condition type (particular email address) and specify the *Content* entry using the email address (`someone@undesirable.com`). In the *Score* entry specify a value — this should be equal or higher than the value set in the *Action* tab.

You can also use the *Treat the message as spam and reject it* option.

2. A user has demanded regular messages with current special offers. These messages are sent from the address `info@offer.com` and they are treated as spam by *SpamEliminator*. To override this denial, we will create the following custom rule:
 - *Header* — use the From selection
 - *Type* — select the *Contains address* option
 - *Content* — insert `info@offer.com`
 - *Add score to the message* — set a negative value that will decrease the total score. You can also use the *Treat the message as non-spam (overrides the SpamEliminator score)* option.

17.2 Blacklists tab

Kerio MailServer can also block incoming messages from servers that are considered as spam servers. For this purpose, it uses public databases of these servers located in the Internet or its proprietary database.

To define these parameters go to the *Blacklists* tab in *Configuration* → *Spam filter* section.

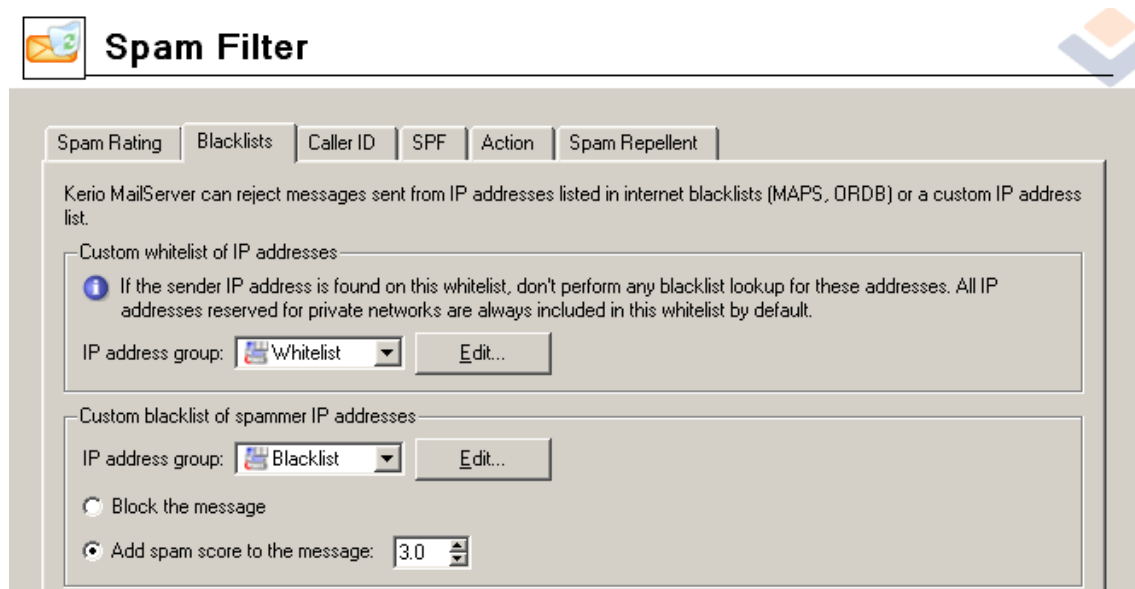


Figure 17.3 Blacklists tab

List of trustworthy IP addresses (whitelist)

So called blacklists, i.e. spammer databases, can occasionally include servers which send legitimate mail. This may occur for example when an SMTP server is not secure enough and it is misused for spam sending. Therefore, *Kerio MailServer* includes a list of trustworthy IP addresses (so called whitelist). In this list, IP addresses considered by the mailserver as spammers can be added. In future, these addresses will be considered as trustworthy, even though they may be included in a blacklist used by *Kerio MailServer*. Messages from the servers included in the whitelist are not checked by any spam filters and they are let in automatically.

To create a whitelist, a new IP group must be defined. To define a new IP group, click *Edit*. This opens a dialog, where a custom IP group of SMTP servers (or users) can be created.

Note: All IP ranges reserved for private networks are added to the whitelist automatically.

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

This applies to the following IP ranges: However, all IP addresses, though included in the whitelist, are verified in the blacklist (*Custom blacklist of spammer IP addresses*). This may be helpful when it is necessary to block any of these addresses.

Custom blacklist of spammer IP addresses

In this section, it is possible to define a custom group of IP addresses of SMTP servers (or users) known as spammers. Click *Edit* to edit the selected group or to create a new one.

Any messages sent from any SMTP server included in the blacklist can be blocked or its spam rating value can be increased. The specified value will be added to the *SpamEliminator* rating.

Internet databases

Kerio MailServer can use various spammer databases (free or paid) available in the Internet. These databases do not depend on each other and they can be used simultaneously. It is also possible to define other databases by using the another dialog which can be opened by the *Add* button:

DNS suffix

Insert the name of the corresponding domain.

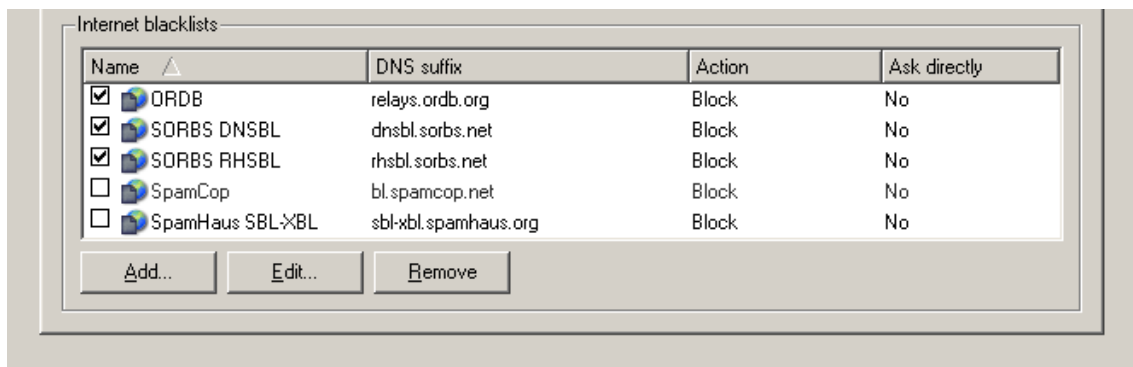


Figure 17.4 Internet databases

Description

Optional entry, for reference only.

Block the message

In this mode, connections from servers included in the blacklist will be blocked. Message(s) will be rejected by *Kerio MailServer*.

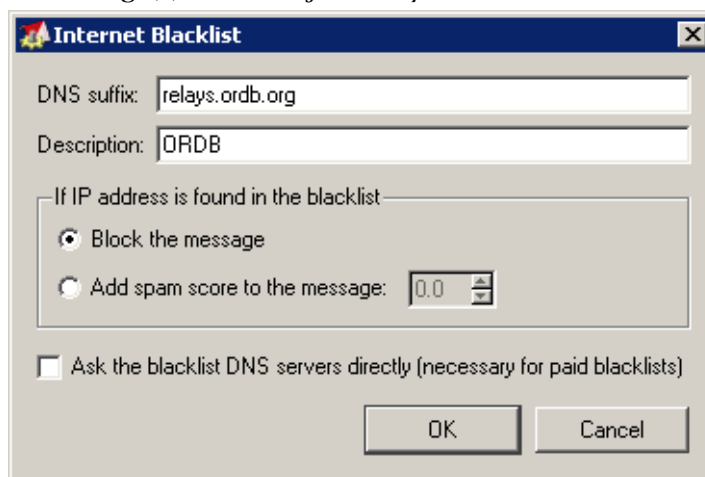


Figure 17.5 Database parameters

Add spam score to the message

The value set here will be added to any message accepted from any server included in the blacklist.

Ask the blacklist DNS servers...

using of this option is recommended in cases where *Kerio MailServer* uses a paidspammer database where the license is associated with a particular IP address. Queries are sent directly to the database, parent DNS servers will not be used for the delivery.

17.3 Email policy records check

Many spam emails are sent from a fake sender email address. Checking “email policy” records is used for filtering such messages.

The check verifies whether IP addresses of the remote SMTP server are authorized to send emails to the domain specified. Spammers thus have to use their real addresses and the unsolicited emails can be recognized quickly using different blacklists.

There are two similar technologies available for performing “email policy” records check in *Kerio MailServer*. The first one is *Caller ID* created by *Microsoft*, the other one is a project named SPF (Sender Policy Framework). Both technologies provide explicit verification of message senders. During this verification process, the IP addresses of SMTP servers that send mail from the specific domain are published. For each domain that supports at least one of the above technologies, a TXT record is stored in DNS with a list of IP addresses that send email from the specific domain. *Kerio MailServer* then compares the IP address of the SMTP server with IP addresses contained in this DNS record. This method guarantee verification of sender’s trustworthiness for each message. If the DNS record does not contain the IP address the message was sent from, such message has a falsified address and it is considered as spam. This way, it is quite easy to distinguish, whether the message is spam or not.

Messages received from server that has no IP address list in the DNS record will be always delivered. For the “email policy” purposes, these emails will not be considered.

To set *Caller ID* and SPF in *Kerio MailServer*, use the tabs in *Caller ID (Spam filter → Caller ID)* and *SPF (Spam filter → SPF)* menu.

Caller ID

For information about how to set a *Caller ID*, refer to the site <http://support.kerio.com/>.

The *Caller ID* tab enables users to configure basic settings:

Check the Caller ID of every incoming message

This option enables/disables *Caller ID*.

On the *Relay Control* tab in the *SMTP server* section, it is possible to define a group of trustworthy IP addresses. *Caller ID* will not be checked in case of messages sent from trustworthy IP addresses (for details, see chapter 16.2).



Figure 17.6 Caller ID tab

Only log this to the Security log

All messages of this type will be logged to the *Security* log. Messages with invalid *Caller ID* will be delivered to the addressee.

Reject the message

Messages with invalid *Caller ID* will be rejected (returned to sender).

Add this value to the message's spam score

The value in this field will be added to the spam score of *SpamEliminator* (see previous chapter).

Apply this policy also to testing Caller ID records

Currently the *Caller ID* technology has not been widely adopted. Therefore, it is often used by domains in testing mode only (the XML script's header in the corresponding DNS record includes the *testing* flag). For this reason, many domains use it only in a testing mode (headers of XML scripts in DNS records contain the *testing* item). Therefore, it is recommended to enable this option (otherwise, *Caller ID* will not function for most domains).

Warning: With this option enabled, do not set the *Block the message* option for messages with an invalid *Caller ID*.

Don't check Caller ID from...

Use this option especially for specifying backup servers. If a message is sent through a backup server, the IP address of the server does not match the ones allowed for the domain. Therefore the messages from these addresses should not be checked.

This is why messages sent from these addresses should not be checked.

Check my email policy DNS records

Click the link to *Kerio Technologies* web pages where the *email policy* DNS record for a domain can be checked.

Note: For detailed instructions on proper configuration of DNS entry settings for *Caller ID*, see the official *Microsoft* web pages.

SPF

SPF is an open source equivalent to *Caller ID* developed by *Microsoft*. Both technologies can be used simultaneously in *Kerio MailServer*.

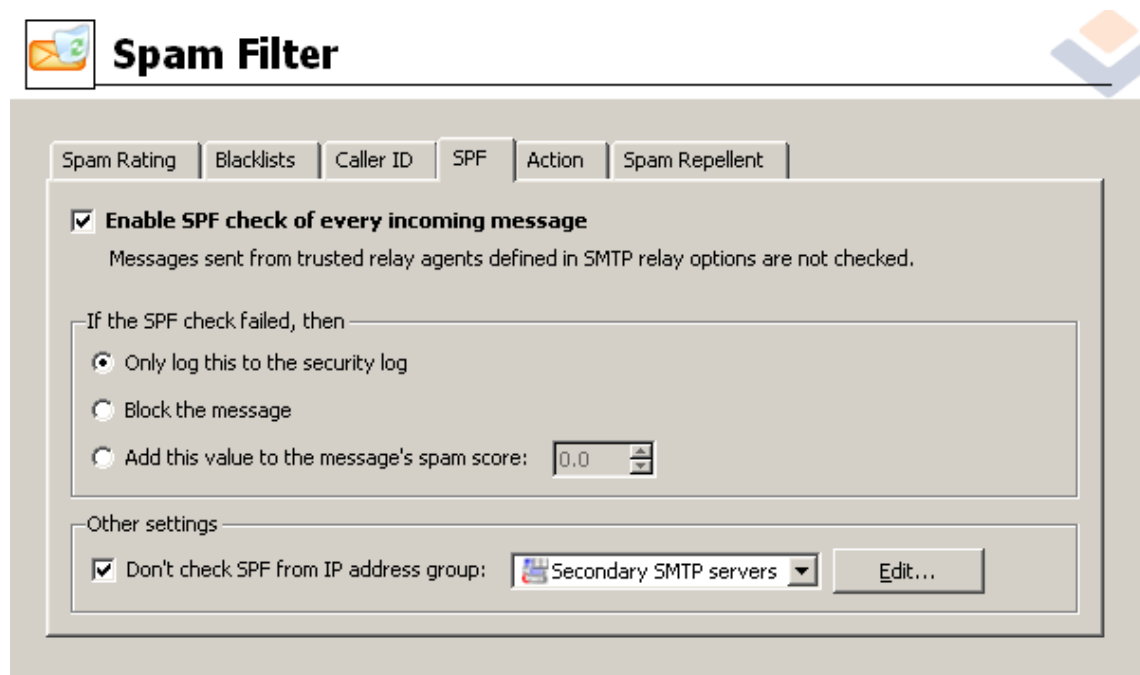


Figure 17.7 SPF

In the *SPF* tab, the following options are available:

Enable SPF check of every incoming message

Enable/disable use of *SPF*.

On the *Relay Control* tab in the *SMTP server* section, it is possible to define a group of trustworthy IP addresses. *SPF* check will not be applied to messages sent from trustworthy IP addresses (for details, see chapter 16.2).

Only log this to the security log

Messages with an invalid *SPF* record will be only added to the *Security* log.

Block the message

The message with an invalid *SPF* record will be blocked (returned to the sender).

Add this value to the message's spam score

The value in this field will be added to the spam score of *SpamEliminator* (see previous chapter).

Don't check SPF from this IP address group

Use this option especially for specifying backup servers. If a message is sent through a backup server, the IP address of the server does not match the ones allowed for the domain. Therefore the messages from these addresses should not be checked.

Warning: To ensure a full functionality of *SPF*, do not add any other servers than the backup servers to this group.

Note: Details about the *SPF* check are displayed in the *Debug* log, after the appropriate settings are specified (for more information, see chapter 23.8).

17.4 Action

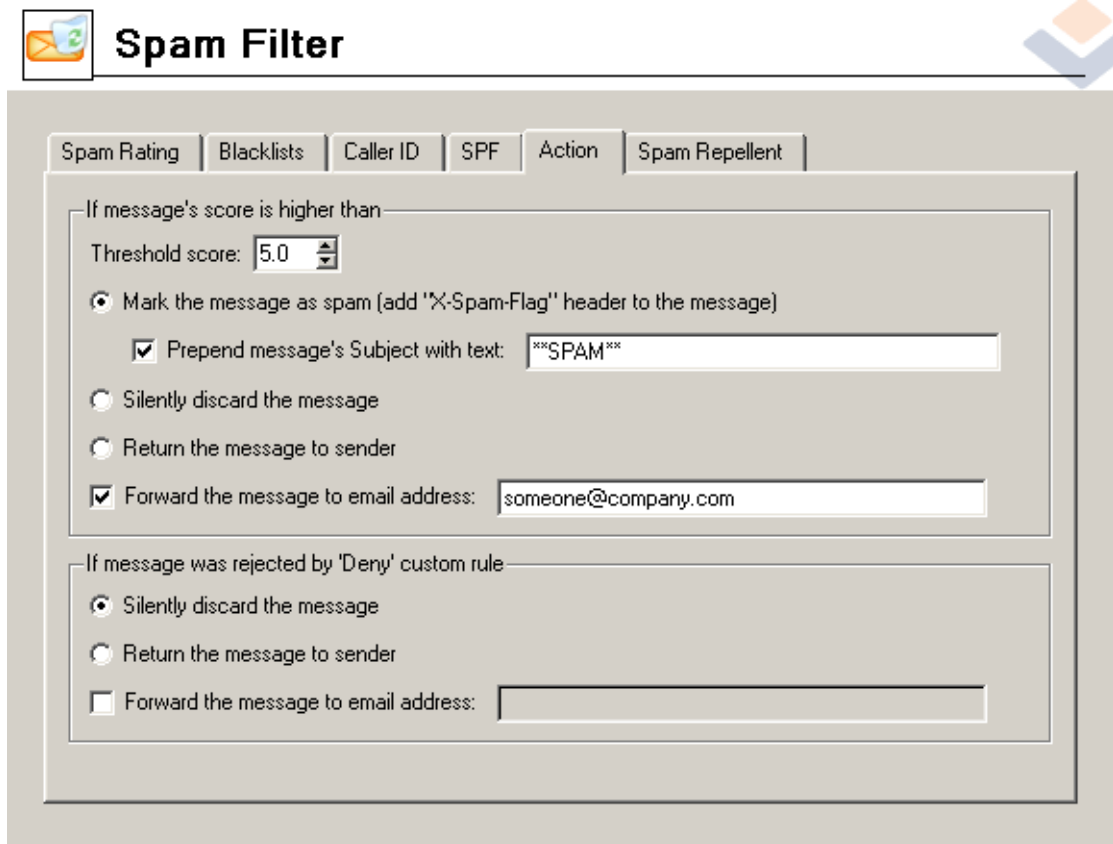
Using this tab you can define what happens with messages once considered as spam

If message score is higher than...

If the score of a message is higher than the defined score value, the message is considered as a spam. Insert a value from -20.0 to +20.0 (the lower the value, the less messages will pass the filter). The message will be tested according to total count of all rules that it meets (the *Spam Rating* tab) and to the *SpamEliminator* evaluation.

We recommend you to use the 5.0 value — statistics claim that 91.12 per cent of spam do not pass through this filter. However, the filter also blocks 0.62 per cent of correct mail. If you set the score higher (i.e. to 8.0), the probability that correct messages will be blocked is lower (0.04%) and the efficiency of spam filtering is also lower (74.36%).

Warning: If the value you set will be too low, every message will be considered as a spam.



The image shows a web-based configuration window titled "Spam Filter". At the top left is an icon of an envelope with a green checkmark. The title "Spam Filter" is in a large, bold font. Below the title is a horizontal tab bar with six tabs: "Spam Rating", "Blacklists", "Caller ID", "SPF", "Action", and "Spam Repellent". The "Action" tab is currently selected. The main content area is divided into two sections. The first section is titled "If message's score is higher than" and contains a "Threshold score:" label with a numeric input field set to "5.0". Below this are four radio button options: "Mark the message as spam (add 'X-Spam-Flag' header to the message)" (which is selected), "Silently discard the message", "Return the message to sender", and "Forward the message to email address:". The "Mark the message as spam" option has a checked checkbox and a text input field containing "**SPAM**". The "Forward the message to email address:" option also has a checked checkbox and a text input field containing "someone@company.com". The second section is titled "If message was rejected by 'Deny' custom rule" and contains three radio button options: "Silently discard the message" (selected), "Return the message to sender", and "Forward the message to email address:". The "Forward the message to email address:" option has an unchecked checkbox and an empty text input field.

Figure 17.8 Action

Mark the message as spam

Message will be marked as spam and delivered to the recipient. You can append a text that will indicate that the message is a spam into the *Prepend message's Subject with text* textfield.

TIP: If you use the [%s] referent for the *Prepend message's Subject with text* entry specification, the score evaluation (represented by asterisks) assigned by the antispam protection system is inserted into this textfield. This implies that users can define their custom antispam rules in their mail server or in the *Kerio WebMail* interface.

Discard the message

Message will be discarded without notification.

Return the message to the sender

Rejected message will be returned to the sender. These settings are not recommended, because the sender address usually does not exist. The messages are left in the queue and must be deleted manually.

Forward the message to an address

Enter an address to which spam will be forwarded (regardless of which action was selected).

If the message was rejected by 'Deny' custom rule...

Setting of these actions applies to the rules created on the *Spam Rating* tab (see chapter 17.1). The *Treat the message as spam and reject it* option must be enabled for the rule.

Silently discard the message

Rejected mail will be discarded silently. This action is not performed if the rule filters the From and To items (for details, see chapter 17.1).

Return the message to the sender

Rejected message will be returned to the sender.

Forward the message to an address

An email address to which rejected mail will be forwarded.

17.5 Spam repellent

Kerio MailServer is able to check the delay of reply to SMTP greeting.

Kerio MailServer requests communication according to RFC (see glossary) which defines SMTP traffic. Most of the spam distributing applications do not follow this RFC. Thus, *Kerio MailServer* is able to distinguish them from legitimate SMTP servers.

Kerio MailServer uses two SMTP connection errors to recognize spam servers. The server that initializes the SMTP communication should according to the corresponding RFC wait for the reply for at least 5 minutes. Applications that send spam automatically do not wait for that long since they need to send email messages as fast as possible to send as many spam messages as they can. It would hold these applications too much to keep waiting the whole period. Therefore, spammer servers behave in one of the following two predictable ways if *Kerio MailServer* does not answer to the SMTP greeting for a certain period (i.e. delay is set for answers). In one case, the spammer server gives up the connection to *Kerio MailServer* and tries elsewhere. In the other case, it starts to send email to *Kerio MailServer* immediately, without receiving the SMTP greeting (in such a case, *Kerio MailServer* interrupts the connection immediately).

Benefits of the SMTP delay are as follows:

1. Reception of spam by *Kerio MailServer* is eliminated by 60 — 70 per cent. This also decreases the load on the server since spam testing is very demanding.
2. The method has no so called false positives as there is no influence to the email which is delivered legitimately. Settings

SMTP delay settings

You can set either the SMTP greeting delay in the *Spam repellent* tab of *Kerio MailServer* (*Configuration* → *Content filtering* → *Spam filter*):

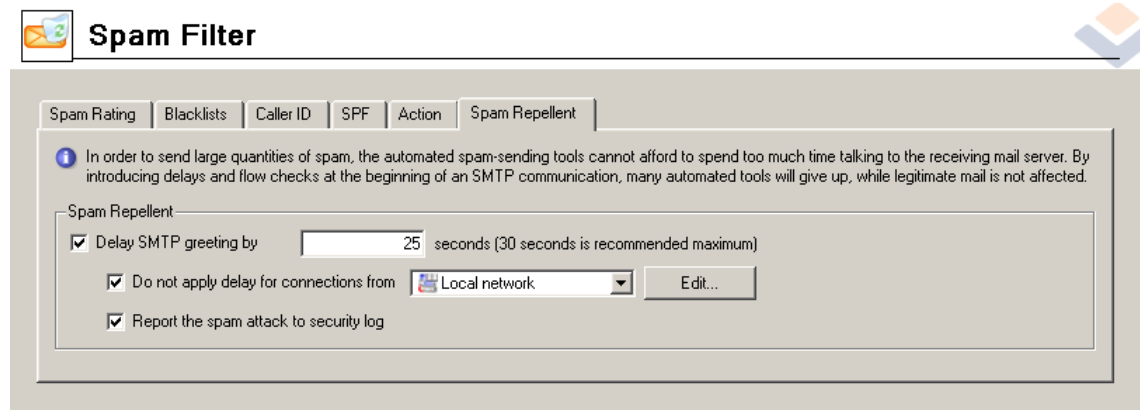


Figure 17.9 Spam repellent

Delay SMTP greeting by

Use this option to set the SMTP delay. The optimal delay value is between 25 and 30 seconds. Shorter delay might not be enough (the spam sending applications use 10-20 sec), longer time would impede the communication.

Do not apply delay for connections from...

Spam repellent settings apply to all incoming SMTP communication events, i.e. also to messages from local network, backup servers, e.t.c. It is therefore recommended to add all trustful IP addresses and networks to this IP address group, so that the communication is not blocked, if the messages are apparently non-spam.

Report the spam attack to security log

Check this option to record all recognized spam attacks to the *Security* log (for more information, see chapter 23.4).

If many emails go through *Kerio MailServer*, there are usually also many spam attack attempts, which can cause security log overflow. In such case, disable this setting.

Note: The settings in this tab apply only to the unsecured SMTP communication. The spam distributing programs do not use the secured SMTP protocol for communication.

Chapter 18

Antivirus Control of Email And Attachment Filtering

In *Kerio MailServer*, you can check all incoming emails for viruses. The control can be performed by using two combinable methods. For this purpose, you can use either the internal *McAfee* antivirus, or any of the external supported antiviruses.

Immediately after the installation of *Kerio MailServer*, the internal *McAfee* antivirus is started. It is possible to support it by enabling any other of the supported external antivirus applications. Both antivirus programs can run concurrently. This provides for reliable protection of your local network, since the virus databases updates will be performed faster (one of the antiviruses can react to a new virus occurrence a couple of hours sooner than the other). The update speed is a key element of the protection against new viruses.

Both antiviruses can be also switched off, but it is not recommended, because users are not protected against infected emails.

Kerio MailServer checks (independently of the antivirus) JPEG attachments for corruption and presence of GDI+ exploit (a malicious code, usually with a virus, that can run the exploit upon system breakdown). All messages with such attachment will be deleted automatically.

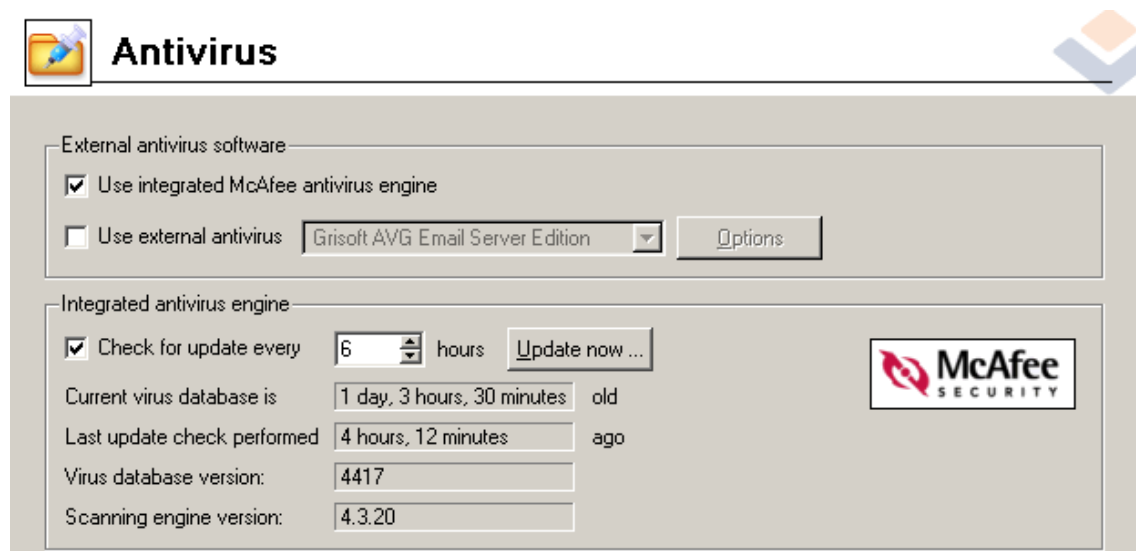


Figure 18.1 Antivirus

Besides cooperation with an antivirus program, *Kerio MailServer* allows you to filter certain file types from email attachments (using file extension or MIME type), regardless of whether they are infected by a virus or not. To specify these options, go to the *Configuration → Attachment filtering* section.

18.1 Integrated McAfee Anti-Virus

Check *Scan mail using McAfee Anti-virus engine* in the *Antivirus* tab of the internal version.

Note: The external *McAfee Anti-Virus* is not supported by *Kerio MailServer*.

Check for updates every

Interval for automatic update of the antivirus database and of the antivirus itself (in hours). Information about updates can be found in the *Security* log (see chapter 23.4).

Note: To enable automatic updates well-working connection to the Internet must be provided. Automated dialing is not supported. In case of dial-ups we recommend you to perform updates by hand (see below).

Virus definition updates are downloaded via HTTP. If the *Kerio MailServer* is behind a firewall you must allow for outbound communication over an appropriate TCP port (port 80 by default).

Click *Update now* to start the update of the virus database and antivirus software manually. When this button is pressed, the update progress window is displayed. Information about updates can be found in the *Security* log (see chapter 23.4).

Note: The update progress window can be closed anytime by pressing the *OK* button (it is not necessary to wait until the update is finished).

Current virus database is ...

Age of virus database (in minutes). This information represents the real age of the virus database, not the time elapsed from the last update attempt.

Last update check performed

The time elapsed from the last successful update attempt. If the time is significantly (several times) greater than the interval set for automatic update, then the automatic updates are not working correctly. In this case we recommend updating the database manually and to inspect the *Error* and *Security* logs for a failure explanation.

18.2 Choosing a Module for an Antivirus Program

Parameters for antivirus control are set in the *Configuration* → *Antivirus* section with the *Antivirus* tab. To use an external antivirus program, check *Use external antivirus*. This menu shows the antivirus software which can be used for email scanning. The antivirus software must be installed prior to making a selection (we recommend stopping the *MailServer Engine* before the antivirus installation).

The installed antivirus may not be run automatically. In such case, use the *Options* button to specify advanced settings of the external antivirus program.

Warning: If the external *Symantec Antivirus Scan Engine* is selected, it is necessary to define the IP address and port of the computer used by the antivirus in the *Options* dialog box.

The following conditions must be met so that the antivirus is properly run:

- The antivirus must be installed on the same computer where *Kerio MailServer* is running.
- The antivirus license must meet the conditions of the producer (usually the same or higher number of users of the licensed version of *Kerio MailServer* or a special server license).

The interface between *Kerio MailServer* and an antivirus program consists of special modules (one for each antivirus). The mailserver administrator must select the appropriate module for the antivirus to be used. If a module is selected and the corresponding antivirus is not installed or does not work properly, *Kerio MailServer* does not allow saving these settings. The message stating that the antivirus control is not functional appears in the *Error* log.

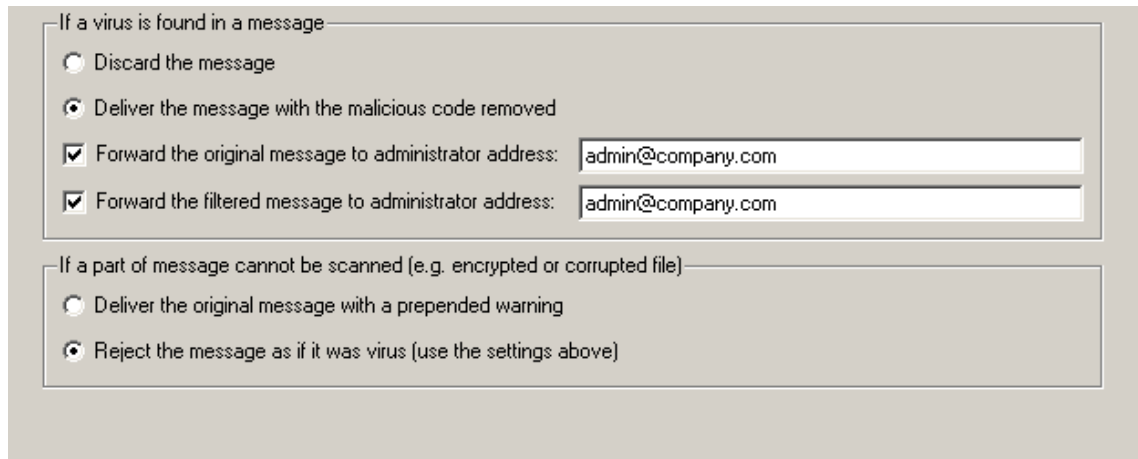
Note: There are two exceptions to this behavior: incorrectly transferred configuration of *Kerio MailServer* (for more information, see chapter 26.2), or less licenses of antivirus than the licenses of *Kerio MailServer*. In such cases, *Kerio MailServer* will work normally, but it will not be able to send messages. This is because *Kerio MailServer* wants to perform an antivirus check after receipt, but the antivirus does not work. The message stating that the antivirus control is not functional appears in the *Error* log.

In order for *Kerio MailServer* and antivirus program to cooperate properly, specify an exception for the *store* directory (or also for the **.eml* files in case of older versions of some antiviruses), so that the messages are not checked by the antivirus engine.

If the resident shield was set incorrectly, a dialog box is opened. The resident shield also detects the *eicar.com* file (a testing antivirus generated by *Kerio MailServer* to check for proper settings of an exception in the resident shield).

18.3 Server responses to detection of a virus or a forbidden attachment

The *Kerio MailServer* administrator can set a detailed course of action for the mailserver if a virus or a forbidden attachment is detected in an email. Use the *Action* tab to set this.



The screenshot shows the 'Action' tab in the Kerio MailServer configuration interface. It is divided into two sections. The first section, 'If a virus is found in a message', contains four options: 'Discard the message' (radio button), 'Deliver the message with the malicious code removed' (radio button), 'Forward the original message to administrator address:' (checkbox, with text input 'admin@company.com'), and 'Forward the filtered message to administrator address:' (checkbox, with text input 'admin@company.com'). The second section, 'If a part of message cannot be scanned (e.g. encrypted or corrupted file)', contains two options: 'Deliver the original message with a prepended warning' (radio button) and 'Reject the message as if it was virus (use the settings above)' (radio button).

Figure 18.2 Server responses to detection of a virus or a forbidden attachment

Discard the message

The message will be removed.

Deliver the message with the attachment removed

The message will be delivered to the recipient but without the attachment. Instead, a server message will be attached saying that the attachment has been removed.

Forward the message to the administrator address

The message will be forwarded (intact — with possibly infected or forbidden attachment) to the email address specified. It is not important whether the address is local or remote.

Forward the filtered message to administrator address

The message without an infected or prohibited attachment will be (apart from the actions selected below) forwarded to the specified email address as well. This can be used for verification of proper functionality of the antivirus and/or attachment filter.

If an attachment cannot be scanned ...

This section defines actions to be taken if one or multiple files attached to a message cannot be scanned for any reason (e.g. password-protected archives). The following actions can be taken:

- *Append a warning to the message* — the message (or attachment) will be delivered unchecked. The user will be warned that the message may still contain viruses.
- *Reject the message* — the system will react the same way as when a virus was detected (i.e. the message will be delivered without any attachment or rejected). This option is safe, but sending password-protected archives is virtually impossible.

Each message is evaluated first by an antispam system, then by antivirus. This saves computer time, since the antispam check is considerably less demanding than the antivirus check. If the messages marked as spam are set to be discarded automatically (in the *Spam filter* section), all spam messages containing viruses will be discarded as well.

18.4 Supported antivirus programs

Kerio MailServer supports several external antivirus programs for *Windows*, *Mac OS X* and *Linux* operating systems from different vendors (e.g. *NOD32*, *Grisoft*, *Sophos Antivirus*, etc.). For the most current list of supported antivirus vendors refer to the *Kerio Technologies* website at <http://www.kerio.com/>.

Here, you can find notes on peculiarities and possible configurations of external antivirus applications:

Symantec Scan Engine

One of the supported antivirus applications is *Symantec Scan Engine* by *Symantec*. Since *Kerio MailServer 6.1.2*, the traffic protocol for communication between *Kerio MailServer* and *Symantec Scan Engine* versions 4 and 5 has been changed. The applications now use ICAP instead of the Native protocol. For this reason, it is necessary to switch the protocol using the *Configuration* → *Protocol* → *ICAP* option in the SAVSE settings..

NOD 32 Antivirus System

Kerio MailServer also supports *Eset's NOD 32*. Edition *NOD32* for *Kerio MailServer* is supported.

Settings of *Kerio MailServer* and *NOD32* is simple in case that *NOD32* contains the license file. Simply set *NOD32* as the external antivirus in the *Kerio MailServer's* administration console.

If NOD32 does not include imported license file (e.g. in case of the trial version), a special supporting module must be installed at the server. This module can be downloaded at the *Kerio Technologies* website at <http://www.kerio.com/>.

NOD32 with the supporting file runs on API1 which implies that archives (ZIP, RAR, etc.) are not involved in the antivirus checks. The full version of NOD32 runs on API 2 which enables to apply the antivirus check also to archived attachments.

Note: To see whether your NOD32 uses API 1 or API 2, view the *Debug* log (for details, refer to chapter 23.8). To log communication between the antivirus and *Kerio MailServer*, enable the *Antivirus check processing* option. If logging is enabled, disable it, save settings and enable logging again. This ensures that relevant information is logged.

18.5 Filtering Email Attachments

The attachment filter can be set in the *Attachment Filter* tab. If the message is captured by this filter, it will be delivered to the recipient without the attachment.

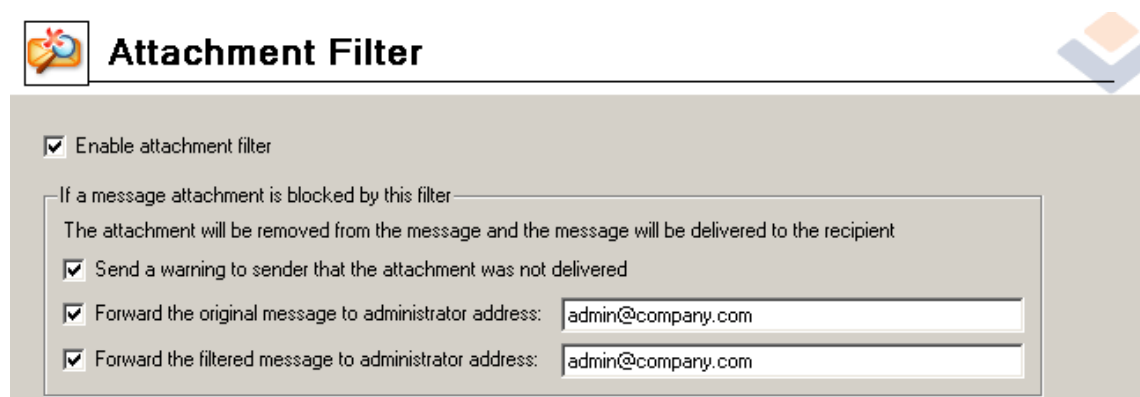


Figure 18.3 Attachment Filter tab

Enable attachment filter

Switches the attachment filter on or off.

Send a warning to sender ...

The sender will receive a warning from *Kerio MailServer*, that he/she has sent a message with a virus or blocked attachment.

Forward the original message to administrator address

The message will be forwarded (intact — with possibly infected or forbidden attachment) to the email address specified. It is not important whether the address is local or remote.

Forward the filtered message to administrator address

The message without an infected or prohibited attachment will be (apart from the actions selected below) forwarded to the specified email address as well. This can be used for verification of proper functionality of the antivirus and/or attachment filter.

List of filters

Displays individual filters. To the left of each filter there is a checkbox that you can use to enable or disable the filter. Use these checkboxes to switch filters off without the need to remove them.

After the *Kerio MailServer* installation, there is a list of several predefined filters. All filters are turned off and the administrator can choose to enable or remove them. This way for example executables (.com and .exe), Visual Basic scripts (.vbs), etc. can be filtered.

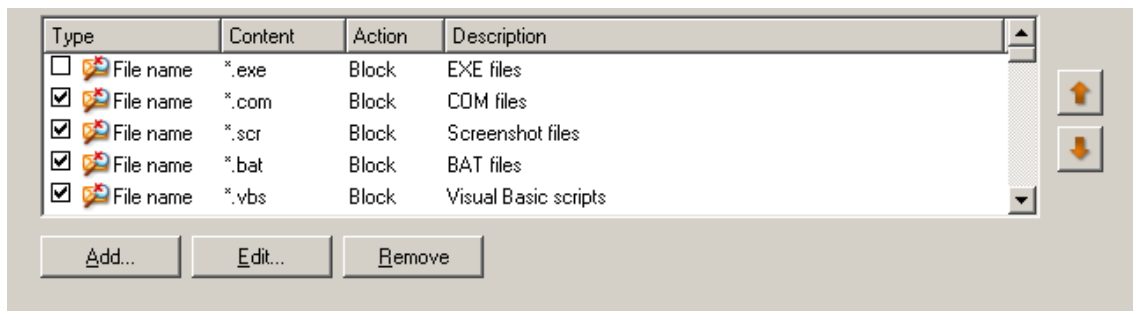


Figure 18.4 List of filters

Use the *Add* button to add a new filter:

Description

Text description of defined filter.

Filter type (MIME type/File name)

Defines if attachments will be filtered based on file names or MIME type (*Multipurpose Internet Mail Extension*).

Filename or filetype specification

Enter either the file name (you can use the asterisk convention for e.g. filtering files with a certain extension — e.g. *.exe) or the MIME type name (for example application/x-msdownload or application/*). You can also choose one of the pre-set or MIME types.

Block the attachment...

An action will be performed as defined above the list of disabled attachments (described above).

Accept the attachment

Attachments will not be removed from messages and no other rules will be applied.

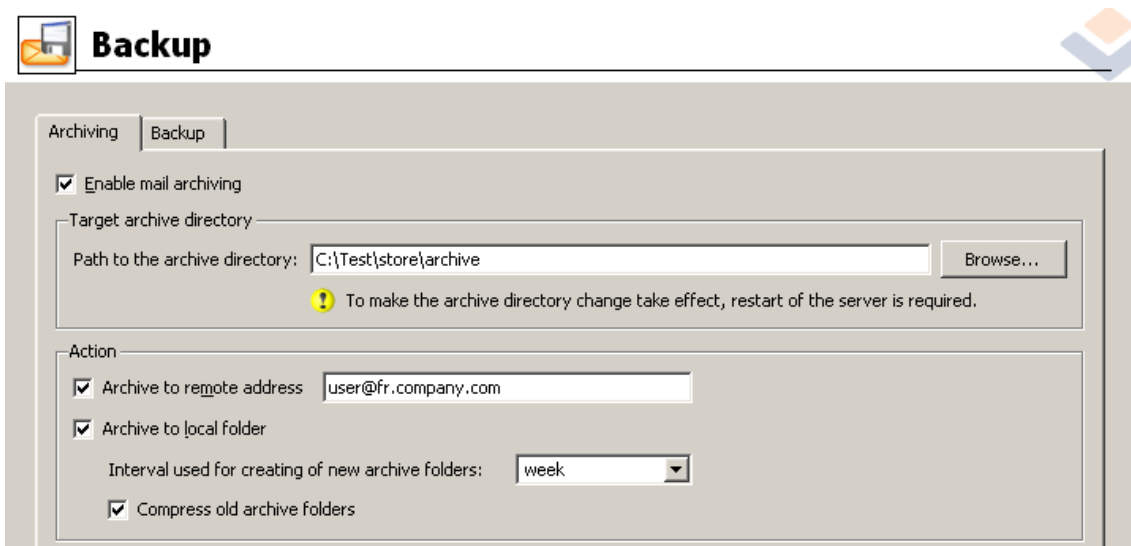
Email backup

19.1 Archiving

Kerio MailServer can store copies of all messages (or only messages sent to the Internet) in special archiving folders or re-send them to another SMTP server. This makes it possible to keep archived email for a situation where it would be necessary to look up a particular message or deleted messages (these can be reused by using so called email recovery which can be set in the domain settings — for details, see chapter 8.2).

The archive folders are displayed only to the users with the appropriate rights. By default, it is only the *Admin* user (for more information, see chapter 14.1). This user can grant the rights to archive folders to other users. Viewing archive folders as well as granting user rights for the particular folder to other users is possible only in *Kerio WebMail* or *MS Outlook* with *Kerio Outlook Connector* extension.

Set parameters for email archiving in the *Configuration* → *Archiving* section.



The screenshot displays the 'Backup' window with the 'Archiving' tab selected. The window has a title bar with a folder icon and the word 'Backup'. Inside, there are two tabs: 'Archiving' and 'Backup'. The 'Archiving' tab contains the following settings:


- ☒ Enable mail archiving
- Target archive directory:
 - Path to the archive directory:
 -  To make the archive directory change take effect, restart of the server is required.
- Action:
 - ☒ Archive to remote address
 - ☒ Archive to local folder
 - Interval used for creating of new archive folders:
 - ☒ Compress old archive folders

Figure 19.1 Archiving tab

Enable mail archiving

This option enables/disables mail archiving. If archiving is enabled and appropriate parameters are set on the *Archiving* tab, an archive folder with a name derived of the interval in which folders are created (daily, weekly, monthly) is created when the first message is delivered. The interval also can be set on the tab.

Anytime *Kerio MailServer* is restarted, a new archive folder is created (upon receiving the first message). Then, the archiving cycle follows settings defined on the *Archiving* section.

Path to the archive directory

The full path to the archive directory (in accordance with conventions of the operating system on which *Kerio MailServer* is running).

Archive to remote address

Email will be re-sent to this remote email address.

Archive to local folder

Copies of email messages will be stored in local folders, created automatically in the name space *#archive* (on the disk, it appears in the *mail_archive* folder in the directory where *Kerio MailServer* is installed) according to a defined format.

Interval used for creating...

A suitable interval for creating archive folders can be set in this option. The names of the archive folders reflect the interval settings:

2005-Jan — a monthly archive format. The name contains the year and month during which the messages were archived. Every thirty days, a new folder is created (upon reception of the first message after the server's midnight time).

2005-W03 — a weekly archive format. The name contains the year and week during which the messages were archived. Every seven days, a new folder is created (upon reception of the first message after the server's midnight time).

2005-Jan-12 — a daily archive format. The name contains the year, day and month during which the messages were archived. Every day, a new folder is created (upon reception of the first message after the server's midnight time).

Note: The interval for creating new archiving folders (implied from the name format) is up to the *Kerio MailServer* administrator. We recommend bearing in mind the number of messages passing through the MailServer (or the number of local users). A greater number of folders containing smaller numbers of messages are faster to access and easier to comprehend.

Compress old archive folders

Use this option to compress the archive except for the current folder (the last folder created). However, it is not possible to browse through the compressed folders via email clients.

The first compression of the archive folder is performed upon *Kerio MailServer's* startup. Each 24 hours since creation of a new folder, a new compression is performed.

Local messages (local sender, local recipient)

All local messages (messages sent from the local domain) will be archived.

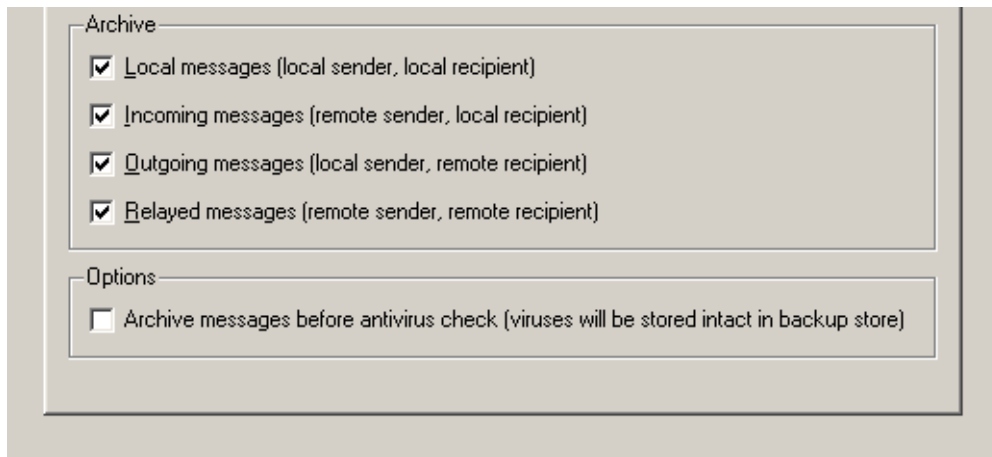


Figure 19.2 Selection of message types to be archived

Incoming messages (remote sender, local recipient)

All incoming messages will be archived (from remote senders to local recipients).

Outgoing messages (local sender, remote recipient)

All outgoing messages will be archived (from local senders to remote recipients).

Relayed messages (remote sender, remote recipient)

All messages forwarded to a relay server will be archived (from remote senders to remote recipients).

Archive messages before...

This option enables archiving of all messages before the antivirus check is started. All messages will be stored intact (including viruses) in these files.

By default, archive folders are available to the admin of the primary domain (see chapter 14.1). The Admin can also assign access rights to archive folders for other users. This may be done in *Kerio WebMail* (refer to the *Kerio WebMail* user guide) or in *MS Outlook* (see chapter 31.10) supported by the *Kerio Outlook Connector*. However, since messages of all users are archived, only a confidential administrator (or a tiny group of confidential persons) should be allowed to access these folders.

19.2 Backup of user folders

Kerio MailServer enables regular backups of user folders and configuration files on a corresponding media. For this purposes, any removable or network disk can be used.

Kerio MailServer makes a backup of the entire store data directory and of the `users.cfg` and `mailserver.cfg` configuration files.

Backups of user folders include various settings. To configure backups, go to the *Backup* tab under *Configuration* → *Backup*:

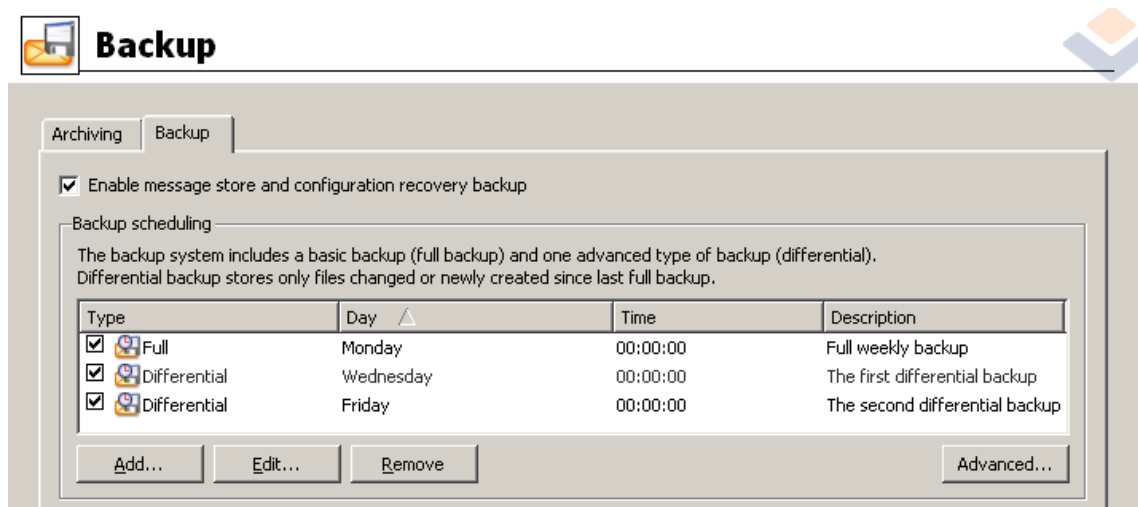


Figure 19.3 Backup of user folders

Enable message store and configuration recovery backup

Use this option to back up all user folders together with the current *Kerio MailServer* configuration. It applies to the whole store data directory and `users.cfg` a `mailserver.cfg` files.

Uncheck the option to disable archiving in *Kerio MailServer*. If archiving is enabled, the default exemplary archiving schedule will be used upon each restart of *Kerio MailServer*.

Warning:

- The backup system in *Kerio MailServer* does not include all configuration files of the server. If it is necessary to move the configuration and user folders to another server or to reinstall *Kerio MailServer*, manual backup must be performed for the `sslcert` (includes SSL certificates) and `license` (includes license files) directory, in addition to standard backup. For detailed information on this issue, see chapter 26.2.
- It is recommended to backup the `sslcert` and `license` directories immediately upon *Kerio MailServer*'s installation and registration and also everytime their content

changes (e.g. when number of user licenses is increased or when a new trustworthy certificate is imported).

Backup Schedule

On the *Backup* tab, backups can be scheduled in details. Two backup types can be scheduled:

- *Full backup* — full backup of all files.
- *Differential backup* — a partial backup, including all changed and new files. These backups are not so bulky. Typically, partial backups complement a full backup. If multiple differential backups in row are scheduled, the newest backup always rewrites the previous one. This means that at most one differential backup can be saved on the backup disk besides the full backup.

Note: If the method of differential backups is used, the most recent full and differential should be used in case that a backup recovery is performed.

The backup schedule is defined by backup tasks. Each task includes settings for time when the particular backup will be performed and selection of a backup type (see above). To add a new backup task to the schedule, click *Add*. A backup schedule definition window is opened (see figure 19.4) that includes the following setting options:

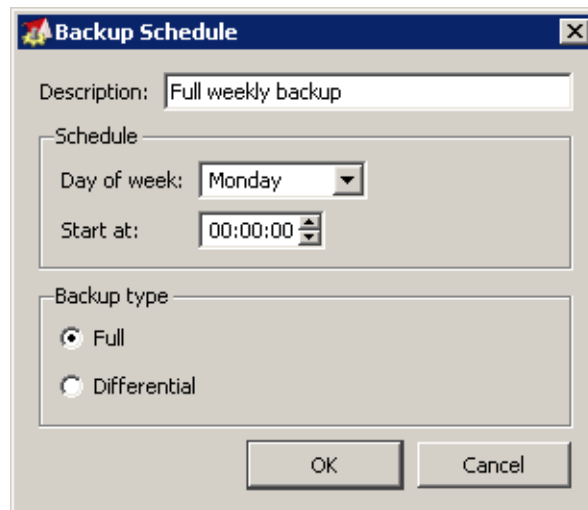


Figure 19.4 A backup task

Description

This is an optional item, it is used for better reference.

Schedule

The box includes two entries where day and time are selected for the backup. It is recommended to perform backups at night (especially full backups) since backups might overload the mailserver.

Backup type

Selection of either the full or differential backup type.

The *Add* button opens a definition of a new backup task. You can also click the *Edit* button to edit a corresponding task or *Remove* to remove a task from the schedule.

Both backup types can be combined by using multiple tasks. Any number of backup tasks can be defined. This depends on the user. Number of backup tasks may depend on:

1. Size of the data store which influences how long each backup takes and on its size. Both problems might be easily solved by using differential backups.
2. Importance of data which might be lost. This implies that backups are typically more frequent in companies where email communication and message storing is important. If backups are performed frequently, minimum of data is lost in case of the server's failure.

Click *Advanced* for advanced settings (see figure 19.5):

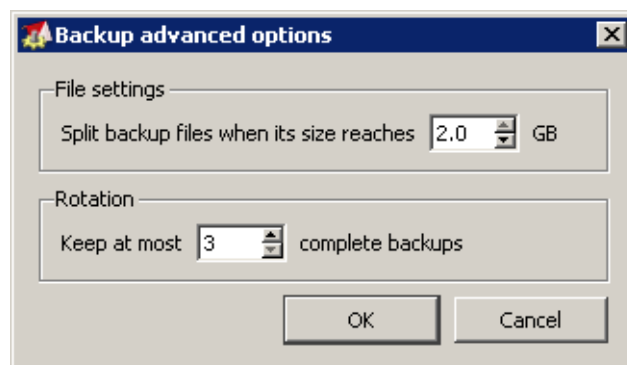


Figure 19.5 Backup advanced options

File settings

Backups are saved in compressed files (.zip) where the maximal size of 2 GB is allowed. This box enables you to split the backup to several files of smaller size. The maximal file size for splitting is set to 2 GB by default. If a file exceeds the value set in the dialog, the file is not backed up.

Rotation

Each backup of user folders is very space-demanding and it might be desirable to often remove these backups. It is possible to set rotation where old backups are removed automatically. Just specify number of backups to be kept in the *Keep at most ... complete backups*. Whenever the number is exceeded, the oldest backup is rewritten by the new one.

Other settings

Backup directory

Specification of the complete path to the backup directory (according to conventions of the operating system on which *Kerio MailServer* is installed). The default backup store is in the directory where *Kerio MailServer* is installed:

Kerio\MailServer\store\backup

Warning: It is recommended to change the backup directory by setting the path to the corresponding removable disk or another media where the backup will be stored if available.

Figure 19.6 Backup directory specification

Each archive consists of backup type and date when it was created:

- Full backup — F20060118T220007Z.zip
 - F — full backup
 - 2006 — year
 - 01 — month

- 18 — day
- Differential backup — I20060106T220006Z.zip
 - I — differential backup
 - 2006 — year
 - 01 — month
 - 06 — day
- Backup copy (manual back up startup) — C20060117T084217Z.zip
 - 2006 — year
 - 01 — month
 - 17 — day

Network disk authentication

In addition to saving backups to removable media it is also possible to store save backups to a network disk. If access to the disk is secured, authentication by user-name and password must be enabled (a user with access rights to the network location must be used).

Username and password for authentication to the network disk can be used only if *Kerio MailServer* is installed on *MS Windows*.



Figure 19.7 Network disk authentication

Notifications

Specify an email address where notifications about the backup status will be sent by *Kerio MailServer*.

In addition to backups set in the schedule, it is also possible to make so called backup copies. The copy is a kind of full backup. The copy can be enabled by the *Start now* button. The current status of the backup process appears next to the button. In case of a backup recovery, the copy is considered as a standard full backup and it is used for the recovery if it is the most recent copy performed.

Recovery

A special application called *Kerio MailServer Recover* is used for recovering of the backup data. This application performs decompression of the particular backup and saves it in the store directory.

To launch *Kerio MailServer Recover*, run the `kmsrecover` command from the directory where *Kerio MailServer* is installed.

Usage:

```
kmsrecover <directory_name>|<file_name>
```

You can also see these details and examples to individual attributes, by running the `kmsrecover` command.

Warning:

- It is necessary to stop the *Kerio MailServer Engine* prior to the recovery.
- Applying a full or copy backup will overwrite the existing store. Applying any backup will overwrite the existing configuration.

Backup recovery will be better understood through this simple example:

The recovery is performed on a host using *MS Windows*. The directory with configuration data is stored at the default location (as set as default during the installation), the store directory is located on a separate disk (RAID or a faster disk) of the same computer where the configuration directory, and the backup directory is located on an exchangeable disk. For backup recovery, use full backup.

Conditions:

1. The configuration data is stored under
C:\Program Files\Kerio\MailServer
2. The *store* directory is located in
D:\store
3. For security purposes, the backup directory is stored on the removable disc
E:\backup

Solution:

The command must be run from the directory where *Kerio MailServer* is installed. In this case, the directory is

`C:\Program Files\Kerio\MailServer`

At this point, two command formats can be used:

1. We want to recover the last complete backup (the most recent full and differential backups or the most recent backup copy). The command will be as follows:

```
kmsrecover E:\backup
```

2. To recover a particular backup (except the last one), use the following format:

```
kmsrecover E:\backup\F20051009T220008Z.zip
```

The `kmsrecover` detects the path to the store (`D:\store`) automatically in the *Kerio MailServer's* configuration file and uses it.

Warning: If the parameter contains a space in a directory name, it must be closed in quotes. For example:

```
kmsrecover "E:\backup 2"
```

Chapter 20

LDAP server

The built-in LDAP server enables access to public and private contacts (you can use either the secured or the unencrypted access — for detail see chapter 7) stored in KMS for email client programs supporting the LDAP protocol (*Lightweight Directory Access Protocol*). This protocol is supported by all commonly used email clients. This protocol is supported by all most common email clients.

These clients can enable users to search for users' data (typically email addresses) and automatic completion of email addresses when they are inserted.

20.1 LDAP server configuration

Usage of the *LDAP* service in *Kerio MailServer* is easy. Simply, the following two conditions must be met:

- At least one *LDAP* service or *Secure LDAP* must be run in *Kerio MailServer*.
- The user must have his/her contacts defined in the contacts folder or must have subscribed at least one public or shared contact. No contacts will be found unless this condition is met.

Note: If *Kerio MailServer* is protected by a firewall and the LDAP service is intended to be available, the appropriate ports must be open (389 for the *LDAP* service and 636 for *Secure LDAP*). You should use the encrypted *LDAP* version.

20.2 Configuring Email Clients

The following information should be considered to enable a mail client to access contacts stored in *Kerio MailServer* by the LDAP protocol.

LDAP server

DNS name (e.g. mail.company.com) or IP address (e.g.) of the host that *Kerio MailServer* is running on.

User name and password

This data is used by users to log into the LDAP server (equal to the name and password for user login to mailboxes). The LDAP server in *Kerio MailServer* does not support anonymous logins — the user login is always required.

Security, Port

Select, whether the secure or non-secure version of LDAP protocol should be used.

If you do not use standard port insert a corresponding port number.

Note: TLS is not supported.

Search base

If you want to access all private and subscribed shared and public folders, leave the entry blank or enter

`fn=ContactRoot`

Specify appropriate branch of the LDAP database in more details to limit access only to certain folders. To better understand various alternatives, read the following examples:

- `cn=jsmith@company.com,fn=ContactRoot`
 - it will be searched only through contact files of the user `john@company.com`
- `fn=personal,fn=ContactRoot` — it will be searched only through contact files of users that are logged into the LDAP server. This option is identical with the previous one, however, it is not necessary to specify username (or email address) of the user. This feature can be used for example for configuration of more clients, etc.
- `fn=public,fn=ContactRoot`
 - it will be searched only through public contact files
- `fn=Contacts,cn=jsmith@company.com,fn=ContactRoot`
 - it will be searched only through the `Contacts` folder of the user
- `fn=PublicContacts,fn=public,fn=ContactRoot`
 - it will be searched through the public `PublicContacts` folder only

Example of Configuration — Outlook Express

The client configuration for enabling the search of contacts through LDAP is explained in the following example using *Microsoft Outlook Express*.

The LDAP account is defined in the *Tools → Accounts → Directory Service* menu. New accounts can be added by wizards. However, only basic parameters can be defined there. Therefore, it is possible to set detailed parameters by selecting a corresponding account and clicking on *Properties*.

General folder:

Name of the account

Name of the account, used for reference only.

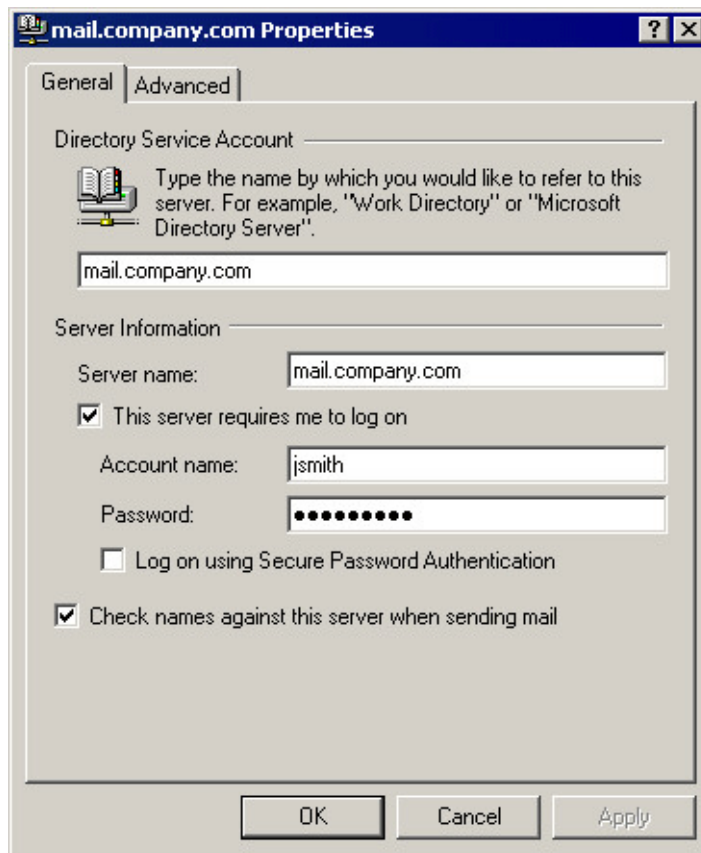


Figure 20.1 LDAP server settings — General tab

Server Name

DNS name or IP address of the host where *Kerio MailServer* is running (e.g. mail.company.com or 192.168.1.10).

This server requires me to log on

Check this option. The LDAP server in *Kerio MailServer* does not support for anonymous connections.

Account name, Password

Insert your username and your password for login to the server (identical with your name and password for login to your mailbox).

Log on using Secure Password Authentication

When this option is enabled, passwords will be sent securely through NT domain authentication (SPA/NTLM). This authentication method is not supported by the LDAP server in *Kerio MailServer* therefore it must be disabled.

Note: We recommend using the secure version of the *LDAP* service (SSL) for encrypted user authentication.

Check names against this server when sending mail

If this option is enabled, personal email addresses will be searched for automatically when a message is sent. This means that names can be used instead of full email addresses in the *To* field (or *Copy To* or *Blind Carbon Copy To*). The appropriate email addresses will be changed when the email is sent.

Note: If an inserted name cannot be found, the message will not be sent by *MS Outlook Express* and the user must correct the name or insert the full email address. If there are more addresses for one name, a dialog for user / address selection will be opened.

Advanced folder:

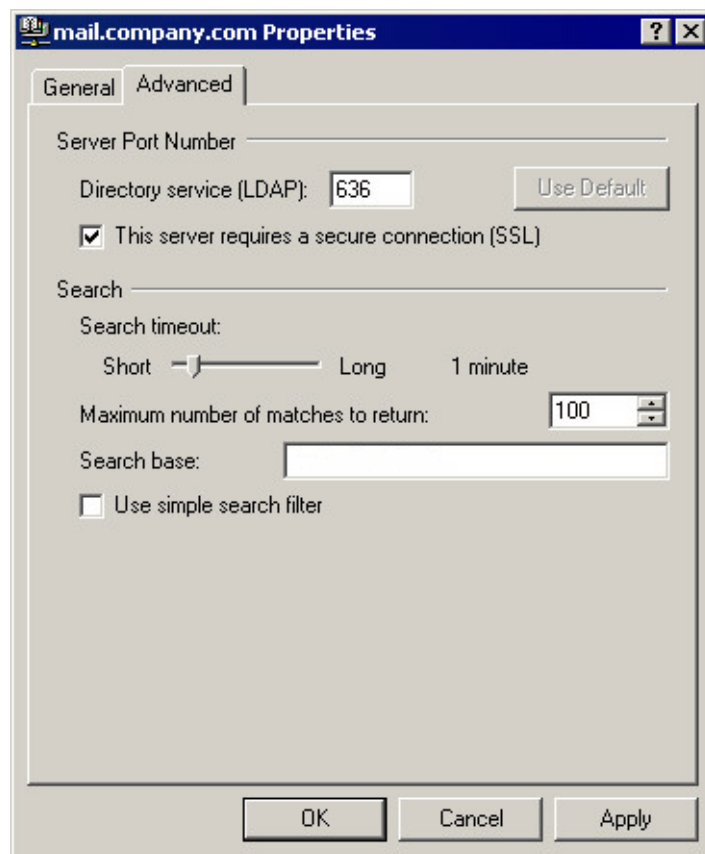


Figure 20.2 LDAP server settings — Advanced tab

Server Port Number

Port the LDAP service is running on. The *Use Default* button will set the standard port number (depending on the on/off mode of SSL — see below).

This server requires a secure connection (SSL)

A secure connection is activated or inactivated with this option. Set the SSL security system according to *Kerio MailServer* services configuration (for details, see chapter 7) or according to your security policy (see chapter 16.6).

Search timeout

If there is a large LDAP database or the connection is slow, the search can take a long time. This option defines the maximum length of time for searching through the database. When this time expires, the searching is stopped, regardless whether any record has been found or not.

Note: If the LDAP server is located within the same local network as the client, the search should take almost no time.

Maximum number of matches to return

If the specifications of the item searched are too broad (e.g. most of the recipient's name is not included), the search may result in many items found. Limiting the maximum number of matches can reduce the search time as well as line traffic. If a large number of items are returned, a new search should be performed using more narrowly defined specifications.

Search base

Specify a location of contacts in the LDAP database (see above). If you leave this entry blank, all subscribed folders will be scanned (public and shared).

Use simple search filter

This option reduces the number of database items that will be searched. This will make the search faster, however, the search potential will be reduced. *We recommend not to use this option.*

Chapter 21

Mailing lists

Kerio MailServer allows for any number of mailing lists to be defined within each local domain. However, the number is limited by user licenses, because each mailing list is considered to be one license by *Kerio MailServer*.

Mailing lists are based on an email address shared by all users included in the group — messages sent to the address are distributed to all members of the corresponding mailing list. In addition to functions of simple user group, the following functions are available in mailing lists:

- dynamic user logins and logouts to/from mailing lists
- mailing list moderating (moderators conduct users' subscription/unsubscription, participation and message postings)
- automatic modifications of message body or subject (by adding predefined text to each message)
- header substitution (hides sender's email address)
- disallowing messages that contain certain features (e.g. messages where subject is not defined)

All actions are executed by sending emails to special accounts. Mailing lists must be created in the *Kerio Administration Console*. All other actions may be taken by email sent and delivered via SMTP.

Warning: If POP3 access is used, it is not recommended to process messages from mailing lists. If you plan to run mailing lists, the MX record for your server is required.

21.1 User Classification

Users of mailing lists may have the following roles:

Administrator

User with *Kerio MailServer* administration rights (read/write access — see chapter 14.1). *Kerio Administration Console* administrators create all mailing lists and define their parameters (e.g. moderators, policies, etc.). For details, see chapter 21.2).

Moderator

Each mailing list should have at least one moderator. Moderators are allowed to take the following actions:

- confirm or refuse a user login (if required by the mailing list policy)
- allow or deny postings to the mailing list (if required by the mailing list policy)
- receive error reports (e.g. reports about emails that could not be delivered)
- can be addressed by
`<mailinglist_name>-owners@<domain>`

Member

Any user subscribed to the mailing list is a member. Their email addresses may belong to any domain — mailing lists are not limited only to the domain where they were created. Mailing list members have the following rights:

- subscribe/unsubscribe (if the member is subscribed, he/she receives all messages sent to the mailing list address)
- ask for help
- send messages to the mailing list (if required by the mailing list policy, each message sent to the mailing list must be approved by a moderator)

Note: Each user may have more than one role (e.g. a moderator can be a member as well, etc.)

21.2 Creating a Mailing List

Mailing lists are defined in *Domain Settings* → *Mailing Lists*. Only administrators (users with both read and write rights) are allowed to create new mailing lists.

Before adding a mailing list make sure you have selected the correct domain from the drop down menu at the top of the *Mailing Lists* dialog. Use the *Add* button to define a new mailing list.

Basic Parameters — General

Name

Name of the mailing list. This name will be used as the email address of this mailing list within the particular domain.

Example: There is a mailing list called `discussion` in the `company.com` domain which will have the address `discussion@company.com`.

Warning:

- Names of mailing lists should not include suffixes (expressions starting with a dash) because they are used for special functions (e.g. `-subscribe` as the

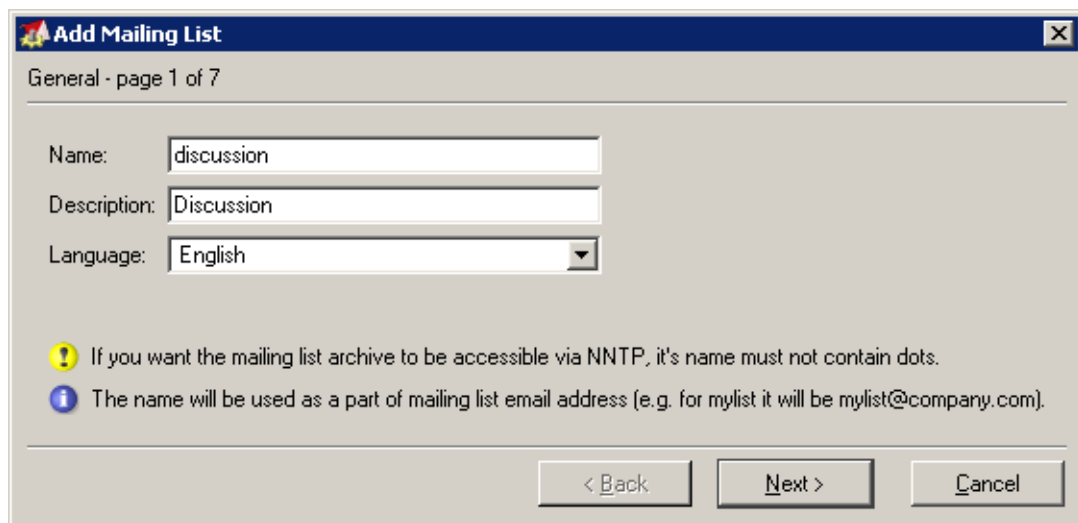


Figure 21.1 Creating a mailing list — basic parameters

suffix is used to subscribe mailing lists). For details, see chapter 21.7, section *Aliases within Mailing Lists*.

- The name of the mailing list must not include the . symbol (dot) since it is used for other purposes in NNTP mailing lists. Though such a mailing list can be created, it is not possible to read it using the NNTP service.
- The mailing list name must be different from the usernames or aliases in the same domain. Otherwise, the alias is preferred and the message will not be delivered to the mailing list.

Description

A commentary on the mailing list.

Language

Selection of a language that will be used for displaying informative and error reports related to the mailing list. Thanks to this option, it is possible to create mailing lists in various languages on one server. Message templates for individual languages are kept in the `reports` subdirectory where *Kerio MailServer* is installed. The UTF-8 encoding is used for the files. Administrator can modify individual reports or add a new language report version.

Comment

In this step you can enter a comment that will be sent to each new participant (upper field) and a text that will be added to the end of each message body sent to the mailing list (bottom field). These fields may be left blank.

Add Mailing List

Comment - page 2 of 7

This text will be automatically sent to each new member:

Welcome in Discussion Feel free to post anything here...

This text will be automatically appended to each email:

This message was posted to the mailing list discussion@company.com

< Back Next > Cancel

Figure 21.2 Creating a mailing list — comments

Note: A welcome message is sent only to those new members that have subscribed to the list via email (for details, see chapter 21.7). Members added to the mailing list through the *Kerio Administration Console* will not receive the welcome message.

Login

Rules for subscription of new members can be defined in this step.

Note: To see details about subscription go to chapter 21.7.

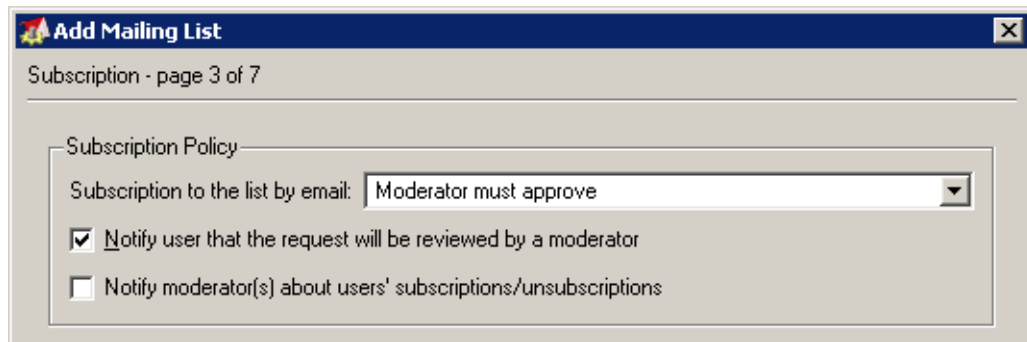


Figure 21.3 Creating a mailing list — subscription

Subscription to the list by email

New members can subscribe to the list by sending an email to a special account. The menu provides the following options to select from:

- *Allowed* — user that has sent an email to the subscription address will be subscribed automatically.
- *Moderator must approve* — a new member's subscription request is forwarded to the moderator(s) of the mailing list. The subscription must be confirmed by a moderator first. If the moderator denies the subscription or no moderator answers the request in seven days, the user will not be subscribed and will receive an informative message.
- *Denied* — subscription via email is not available. Members must be defined by the administrator within this dialog (see below).

Notify user that the request will be reviewed by a moderator

User requesting subscription will be informed that the request has been forwarded to the list moderator(s). This message will be delivered to them immediately after the request reception. If this option is disabled, the message will be delivered when the request is either accepted or denied.

Notify moderator about user subscription/unsubscription

If this option is enabled, moderators will be informed about each user subscription/unsubscription.

This can be especially helpful if automatic subscriptions are allowed (otherwise moderators receive a request). Since each unsubscription is automatic, this feature may provide moderators with important information.

Note: If a user is added to or removed from the list through the *Kerio Administration Console*, the moderators will not be informed of this fact.

21.3 Posting rules

In step 4, rules for posting messages to the mailing list and for automatic modifications of the messages can be defined.

The screenshot shows a window titled "Add Mailing List" with a close button in the top right corner. Below the title bar, it says "Posting - page 4 of 7". The window is divided into two main sections: "Posting Policy" and "Message".

Posting Policy section:

- "Member can post a message:" with a dropdown menu set to "Allowed".
- "Non-member can post a message:" with a dropdown menu set to "Allowed".
- "Moderator can post a message:" with a dropdown menu set to "Allowed".
- Two checked checkboxes:
 - ☒ Notify user that the posting will be reviewed by a moderator
 - ☒ Send delivery errors to moderators

Message section:

- "Reply-To:" with a dropdown menu set to "This list".
- "Add this prefix to each subject:" with a text field containing "[Discussion]".
- Two checkboxes:
 - ☐ Hide sender's address and replace it with an address of the list
 - ☒ Permit messages with an empty subject

At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 21.4 Creating a mailing list — posting rules

Member can post a message

This option specifies whether a member is allowed to post messages. You can select from the following options:

- *Allowed* — messages sent to the mailing list will be delivered to all members (including the sender) immediately.
- *Moderator must approve* — messages to the list address are forwarded to moderators for confirmation. The message is sent to other members only when approved by a moderator. If denied, the sender is informed.
- *Denied* — members cannot post messages to the mailing list.
- *Only Moderators* — only moderators are allowed to send messages to the mailing list.

Non-member can post a message

This option allows non-members send messages to the mailing list. This feature is customized by a pop-up menu providing the following options:

- *Allowed* — messages sent to the mailing list will be delivered to all members (including the sender) immediately.
- *Moderator must approve* — messages to the list address are forwarded to moderators for confirmation. The message is sent to other members only when approved by a moderator. If denied, the sender is informed.
- *Denied* — members cannot post messages to the mailing list.
- *Only Moderators* — only moderators are allowed to send messages to the mailing list.

Note: The message will not be sent to the sender as he/she is not a member of the list.

Moderator can post a message

This option defines whether and how moderators can send messages to the mailing list. It covers the following options:

- *Allowed* — use this option to deny members and non-members access for security reasons. Thus only moderators can send messages to the mailing list.
- *Moderator must approve* — this option has similar function as the previous one but it provides higher security. If a sender tries to break the denial rule by using the moderator's address, the message will not be sent into the mailing list but it will be forwarded to the moderator.
- *Use rules for members/non-members* — This option assigns the moderator rules for members/non-members (according to the fact whether the moderator is a member of the mailing list or not).

Notify server about sending...

Users that send messages to the list will be informed that their requests were forwarded to the list moderators. This message will be delivered to them immediately after the request reception. If this option is disabled, users will receive the report when the request is denied or when the timeout expires.

Send delivery errors to moderators

If this option is enabled, all error reports related to the mailing list will be delivered to moderators. Otherwise, only the sender of the email message will receive the error report. An example of such a report is a notification that an invalid request was sent or that an email account of a mailing list member has exceeded the disk quota set in *Kerio MailServer* and the message sent to the mailing list could not be delivered to the member's mailbox.

Reply-To

This item specifies which address will be used in the messages as the address for replies (the `Reply-To:` item in email headers):

- *Sender* — the address of the original sender will be kept in the header. Responses will be sent to the original sender only. If this alternative is chosen, the message sent to the list will not be modified.
- *This list* — the address of the original sender will be substituted by the list address. This means that the responses will be sent to all list members.
- *Other address* — the address of the original sender will be substituted by a user defined email address. Responses to the messages can be sent to a particular person, another mailing list, etc.

Add this prefix to each subject

Prefix that will be added to subjects of each message sent to this list. When a new list is opened, its name inserted in square brackets is entered to this item automatically. The item content can be edited and it can be left blank (if it is empty, there will be no prefix added to the subject).

Note: Prefix is not added to the subject if it is already included there — for example, in responses to mailing list messages, subject usually follows this pattern:

Re: [name of the mailing list] the original subject

— if this option is disabled, the [name of the mailing list] prefix would be doubled.

Hide sender's address and...

If this function is enabled, the sender's address (the `From` item) will be substituted for the list address in each email sent to the list. If the sender does not enter his/her name, the messages will be anonymous.

Note: If this option is enabled, the *This list* or *Other address* must be set in the *Reply-To* item.

Permit messages with an empty subject

If this option is disabled, only messages with a non-blank `Subject` are accepted. The decision whether to allow messages with blank subjects depends on the administrator.

21.4 Moderators and Members

In these two sections, moderators and mailing list members can be defined. Use the *Add* button to open the corresponding dialog box and specify an email address. The users in local domains can be selected by using the *Select* button. The *Full name* item is optional.

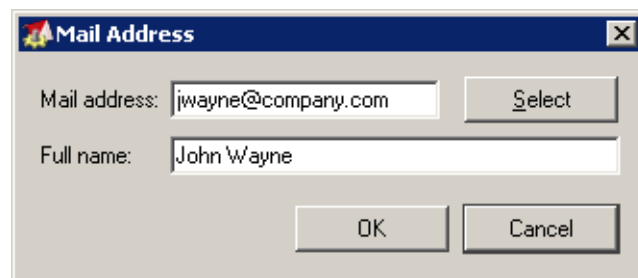


Figure 21.5 Creating a mailing list — add to e-mail address

Any user can be either a moderator or a mailing list member — the specified email address does not have to belong to any of the domains defined in *Kerio MailServer*. In this dialog box, only the administrator is allowed to appoint moderators. Mailing list members may be added either by the administrator or they can subscribe via email (if the list policy allows this option — see above).

21.5 Mailing list archiving

In the last step, the settings for message archiving can be defined. An archive is a special folder that can be accessed via NNTP.

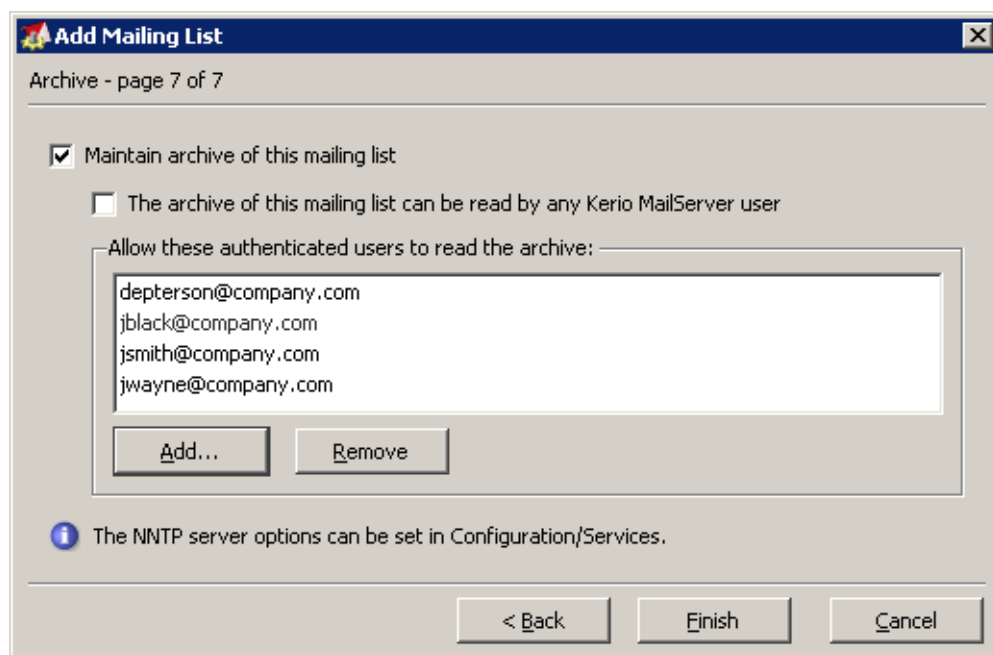


Figure 21.6 Creating a mailing list — maintain archiving

Maintain archive of this mailing list

Use this option to enable mailing list archiving. The archive of the conference can be accessed by all members of the corresponding mailing list

The archive of this mailing list can be read by any user of this server

If this option is enabled, all users with accounts in *Kerio MailServer* have read rights for the archive.

Allow these authenticated users to read the archive

The mailing list archive can be read only by users included in the list.

If an anonymous access is allowed for the NNTP service (see chapter 7), any user can read the archive (even if they have no account in *Kerio MailServer*).

21.6 Server Reports

In mailing lists, there are many automatically generated messages (informative messages, error reports, requests to moderators, etc.). In each list, language for these reports can be chosen (you can select from a few predefined language alternatives). Message templates are kept in the `reports` subdirectory where *Kerio MailServer* is installed. The `reports` directory includes other subdirectories according to languages (e.g., `en` for English, etc.). Language templates are included in these subdirectories.

Message templates may be edited in any editor that supports UTF-8 encoding. The *Kerio MailServer* administrator can modify these messages and reports or create a new language version following the guide that is included.

21.7 How to use Mailing Lists

Member Subscription/Unsubscription

If allowed by the list policy (see chapter 21.2), members may subscribe to the list via email. The subscription is done by sending any message (even with blank message body) to the list address of the following form:

`<name_mailinglist>-subscribe@<domain>`.

Example: A user wants to subscribe to a list called `discussion` in the `company.com` domain. He/she sends a message with an empty message body from his/her email account to the address

`discussion-subscribe@company.com`.

After sending this message the user will receive an email requesting confirmation of the subscription. Once the user sends a response to this message, the user's request will be accepted. This response system guarantees the authenticity of the user.

According to the mailing list policy, the user will be either subscribed or will have to wait for confirmation of a list moderator. If subscribed successfully, the new member will receive a welcome message.

Members can unsubscribe by email at any time. The unsubscription can be done by sending an email message with any content in the message body (it can be left empty) to the address of the following form:

`<name_mailinglist>-unsubscribe@<domain>.`

Example: A user intends to unsubscribe from the discussion mailing list in the company.com domain. He/she sends a message with an empty message body from his/her email account to the address

`discussion-unsubscribe@company.com.`

After sending this message the user will receive an email requesting confirmation of the unsubscription. Once the user sends a response to this message, the user's request will be accepted. After a response to the request is received, the user will receive a report regarding his/her unsubscription.

Message posting

If a user intends to send a message to the mailing list, he/she must send it to the list address (e.g. `discussion@company.com`). According to the policy, the message will be either delivered to each list member (including the sender if he/she belongs to list members) or forwarded to list moderators for approval. If the message is forwarded to a moderator, a report will be delivered to the sender (if defined — see chapter 21.2) and the message will be sent to the list when allowed by a moderator. If the message is denied or not allowed by a moderator within 7 days, the sender will receive a report as well.

Aliases within Mailing Lists

In each mailing list, special email addresses are generated automatically. These addresses are used for special functions, such as member login, contact addresses of the list moderators, etc. Each of these addresses has the following form:

`<mailinglist>-<suffix>@<domain>`

(e.g. to send a request to the discussion mailing list help within the company.com domain, users will send a message to: `discussion-help@company.com`)

Here the suffixes that can be used in the list address are listed:

- `subscribe` — a request for login to the mailing list
- `unsubscribe` — a request for logout from the mailing list

- `help` — a request for help for the mailing list usage
- `owner, owners` — sending a message to the list moderators (there is no need to know their email addresses)

Chapter 22

Status Information

Kerio MailServer allows the administrator (or any other person) to view its activities in great detail. Three kinds of information are available: status, logs and statistics.

- You can view the status of the mail queue, delivery tasks and connections to particular *Kerio MailServer* services.
- Logs are files where information about certain events (e.g. error and warning reports, debugging information, etc.) are recorded. For detailed information on logs, see chapter 23.
- Statistics contain detailed information about individual *Kerio MailServer* services usage such as received and refused messages, errors etc. *Kerio MailServer* can also show graphically the number of connections to individual services as well as the number of processed messages for a given period.

The following chapters describe what information can be viewed and how its viewing can be changed to accommodate the user's needs.

22.1 Messages in queue

All email processed by *Kerio MailServer* is stored in the mail queue. Physically, this is the folder `store/queue` in the directory where *Kerio MailServer* is installed. All messages are added to this queue as two files:

- The file with the `.eml` extension is the message itself
- The file with the `.env` extension is the message's SMTP envelope. This is used only for communication between SMTP servers and is discarded when the message is saved to the target mailbox.

Both files have identical names.

A message is sent from the mail queue either after it reaches the queue or in a time period defined in the scheduler — see chapter 9 for details. If the SMTP server sends messages straight to the target domains (i.e. no relay SMTP server is used) a situation can arise in which the message cannot be sent (no server for the target domain is available). In this case the message returns to the queue and is sent again later.

Note: If the server is in *Offline* mode, the message returns to the queue and the server attempts to send it again in a time specified in the scheduler (*Next Try* is only set in *Online* mode). If the server is in *Offline* mode (usually dial-up lines) then it is better to send messages via a relay SMTP server.

Viewing the Mail Queue

You may wish to check the mail queue if you suspect that messages are not leaving the server. Viewing the queue directly on the disk is not very easy, and is actually impossible if you administer *Kerio MailServer* remotely. For this reason it is possible to view the mail queue directly in the *Kerio Administration Console* in the *Status* → *Mail Queue* section.

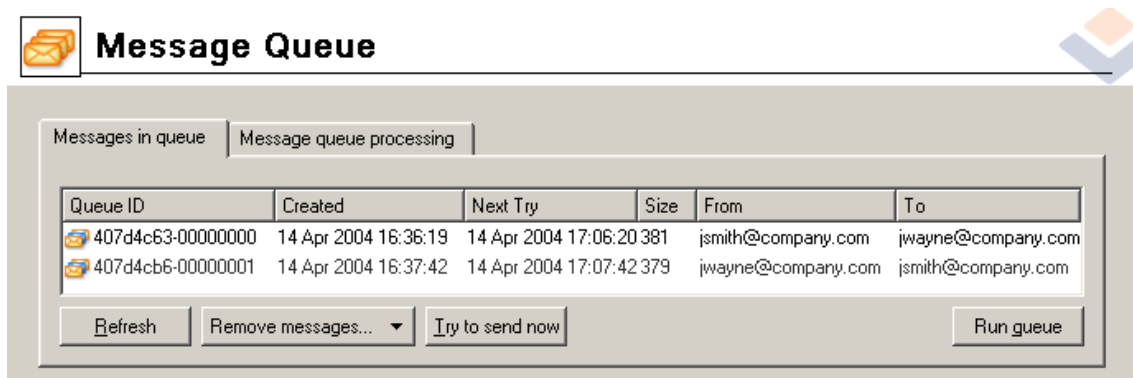


Figure 22.1 Messages in queue

Each line of this window contains information about one message in the queue. The columns contain the following information:

ID

Unique message identifier. This identifier also represents the file names under which the message is saved in the `mail/queue` folder.

Created

Date and time when the message entered the queue.

Next Try

Date and time of the next attempt to send the message (you can set the attempts interval and the number of attempts in the *Configuration* → *SMTP Properties* section — see chapter 16.2). *ASAP* stands for *As Soon As Possible*. This way sending messages that are queued for the first time — in the *Online* mode they are sent immediately, in the *Offline* they are queued and they are sent in scheduled time.

Size

The size of the message (excluding the envelope).

From, To

The sender's and recipient's email addresses. If the *From* field is empty, it is a DSN message sent by *Kerio MailServer*.

Status

Status of the message (reason why the message has not been sent) is described in this column.

Manipulating Messages in the Mail Queue

You can take the following actions using the buttons under the *Mail Queue* window:

Refresh

The *Mail Queue* window is refreshed whenever a change occurs in the queue. You can also use the *Refresh* button to do this manually.

Remove messages

Removes the selected message from the queue. Click this button to display a menu to select messages to be deleted from the queue. You can delete only selected messages, all messages or messages that meet specific criteria.

Try to send now

Attempts to send the selected message immediately.

Run Queue

Starts sending messages from the queue.

22.2 Message queue processing

When processing the *Mail Queue* *Kerio MailServer* creates a new process for each message that reports all actions (delivery to a local mailbox or a remote SMTP server, antivirus control, etc.) and then terminates. Several such processes can run simultaneously — that means that *Kerio MailServer* can send more messages at one time. The maximum number of delivery tasks can be set in the *Configuration/SMTP Properties* section, the *Options* tab, *Maximum number of delivery tasks* parameter (the default value is 8).

In the *Status* → *Message Queue* section on the *Message Queue Processing* tab you can view the active processes (when the process was created, which message is being processed, which SMTP server it is being sent to, etc.) and check their status (antivirus control, sending, local delivery, etc.).

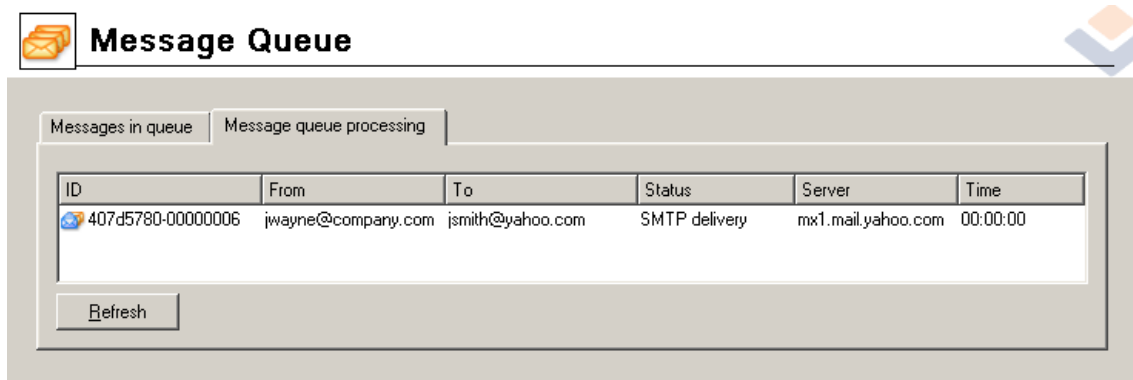


Figure 22.2 Message queue processing

The individual columns in the *Delivery Tasks* window have the following meaning:

ID

A unique message identifier (corresponds with the message ID in the mail queue and the filename in the `mail/#queue` directory)

Size

The size of the message (in bytes)

From, To

The sender's and recipient's email addresses

Status

The process status: *Executing*, *Backup*, *Content filtering* (checking for forbidden attachment types), *Antivirus control*, *Local delivery* (if the message is saved to a local mailbox), *SMTP delivery* (if the message is sent to a different SMTP server), *Terminating* (end phase, terminating the process). The process does not need to pass all the above listed phases — if, for example, mail backup is disabled the *Backup* phase will be skipped.

Server

The SMTP server, to which the message is sent (in the *SMTP delivery* phase only)

Time

The time of the whole process (the length of time from the process start to its termination)

Percent

Information about the delivery process (displays percentage that has already been sent).

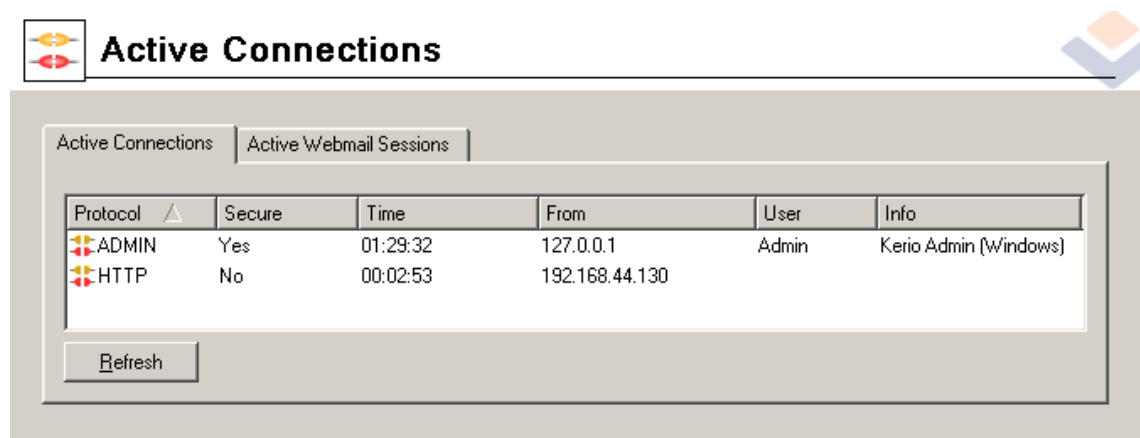
The information in the *Delivery Tasks* window is updated automatically. You can also update the information manually by clicking on the *Refresh* button.

22.3 Active Connections

In the *Status* → *Active Connections* section you can view all network connections established with *Kerio MailServer* including all its services (SMTP, POP3, etc.) and the *Administration Console*.

Active Connections

Each line of this tab contains information about one connection. These are network connections, not user connections (each client program can establish more than one connection at one time in order to receive or send more messages at once). The columns contain the following information:



Protocol	Secure	Time	From	User	Info
ADMIN	Yes	01:29:32	127.0.0.1	Admin	Kerio Admin (Windows)
HTTP	No	00:02:53	192.168.44.130		

Figure 22.3 Active Connections

Protocol

The protocol type that the client is using (or service to which it is connected). Names correspond with the names of services in the *Configuration/Services* section. *ADMIN* means connection to the *Kerio Administration Console* program.

Secure

Defines whether or not the connection will be secured by SSL (technical note: remote administration allows secured connection only).

Time

How long the client has been connected. The timeout is used for certain services (i.e. if there is no data flowing through the connection for a certain period of time, the connection is terminated).

From

IP address from which the client is connected. The DNS name of the client can be displayed here if the option *Enable reverse DNS lookup for incoming connection* is enabled in the *Configuration → Advanced Options* section (see chapter 16.6). We recommend you to enable this option only if you intend to monitor where clients connect from since reverse DNS queries slow down traffic on the server.

User

The name of the connected user. In some cases the name is not displayed (for example connections to the SMTP server — if user authentication is not required, the user remains anonymous).

Info

More information about the connection (e.g. IMAP folder, administration program version, etc.).

Information in the *Connections* window is refreshed automatically or can be refreshed manually using the *Refresh* button.

Active connection to WebMail interface

The table on this tab lists all users connected to the *Kerio WebMail* interface. Each row of the table contains information about a user (his/her email address), IP address used for connection to *Kerio MailServer* and the time when the connection ends.

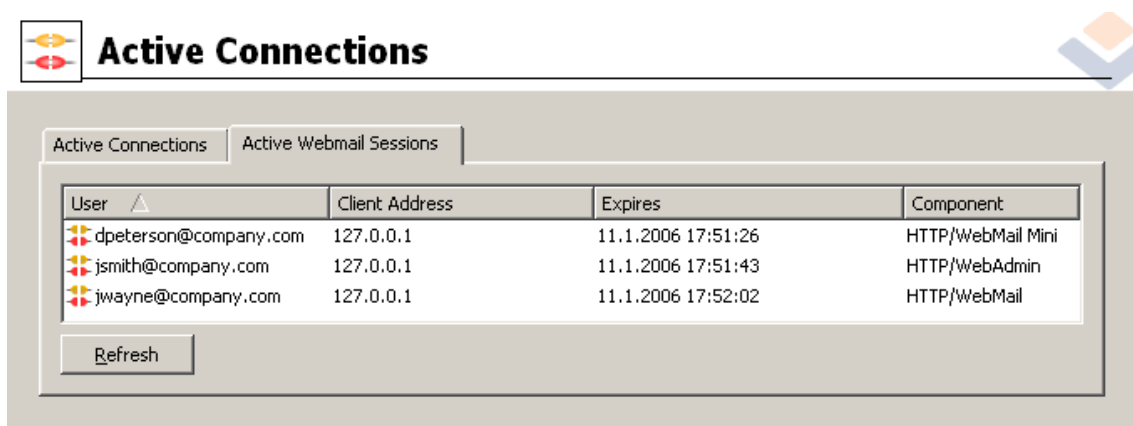


Figure 22.4 Active Webmail Sessions

User

A user connected via *Kerio WebMail* to *Kerio MailServer*.

Client address

IP address of the computer used for connecting to *Kerio MailServer*.

Expires

After a certain time of inactivity (1 hour), *Kerio WebMail* logs out users automatically for security reasons.

Components

Three different components can be used to connect to the server: *Kerio WebMail* (HTTP/WebMail), *Kerio WebMail Mini* (HTTP/WebMail Mini) and *Kerio Web Administration* (HTTP/WebAdmin).

22.4 Traffic Charts

In the *Status* → *Traffic Charts* section you can view (in graphical format) the number of connections to individual services of *Kerio MailServer* and the number of processed messages (both incoming and outgoing) for a given period.

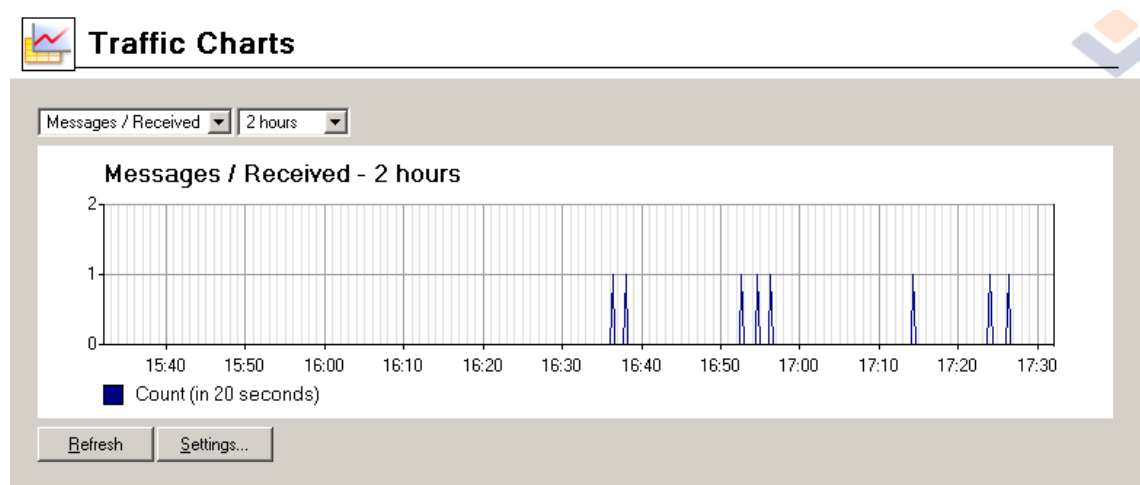


Figure 22.5 Traffic Charts

The graph allows the following parameter settings:

Monitored parameter

Use the first field to choose the monitored parameter:

- *Connections/IMAP* — the number of connections to the *IMAP* service
- *Connections/POP3* — the number of connections to the *POP3* service

- *Connections/SMTP* — the number of connections to the *SMTP* service
- *Messages/Received* — the number of messages processed by the MailServer (the total of outgoing and incoming SMTP messages and messages downloaded from remote POP3 mailboxes)

Time range

In the second field you can choose the time range you wish to monitor (the range can be from 2 hours to 30 days). The selected time range is always understood as the time until now (“last 2 hours”, “last 30 days”, etc.)

The legend below the graph shows the sampling interval (i.e. the time for which a sum of connections or messages is counted and is displayed in the graph).

Example: If *2 hours* is selected as the time range the sampling frequency is 20 seconds. This means that a number of connections and/or messages is counted for the last 20 seconds and is written into the graph.

The *Settings* button opens the dialog where the detailed settings of a chart can be defined.

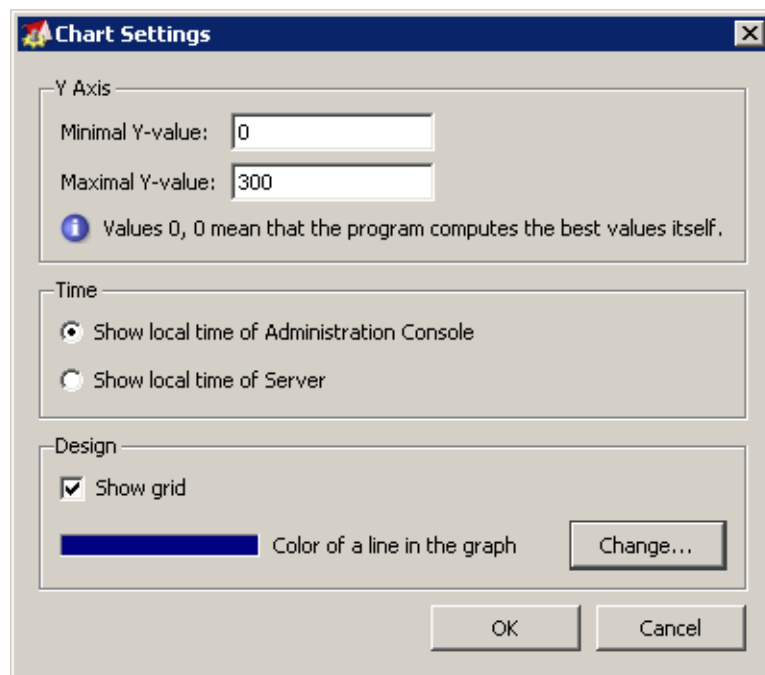


Figure 22.6 Chart Settings

Y Axis

Definition of the minimum and maximum values for the y axis.

Note: The scale of the x axis is determined by the time range that has been selected.

Time

This option defines which time type will be displayed in the chart (either the server time or the local time of the host the *Kerio Administration Console* is running on). The following rules are applied:

- If *Kerio Administration Console* is run on the same host where *Kerio MailServer* is installed, both time types are equal.
- The same rule is applied if the times on both hosts are synchronized (e.g. by the NTP protocol or in Windows NT domain).
- If the times are not synchronized and both hosts are in the same time zone, we recommend to use the server time.
- If the hosts are in different time zones, any of the two time types can be selected according to your needs.

Show grid

Grid can be showed or hidden in the graph.

Color of the line in the graph

Select a line that will be used in the graph. Click *Change* to select a color.

22.5 Statistics

Statistical data is displayed using the *Status* → *Statistics* section. Statistics are divided into groups for better readability (e.g. “Storage Occupied”, “Messages sent to parent SMTP server”, “Client POP3 statistics”, etc.). The *Refresh* button updates displayed data.

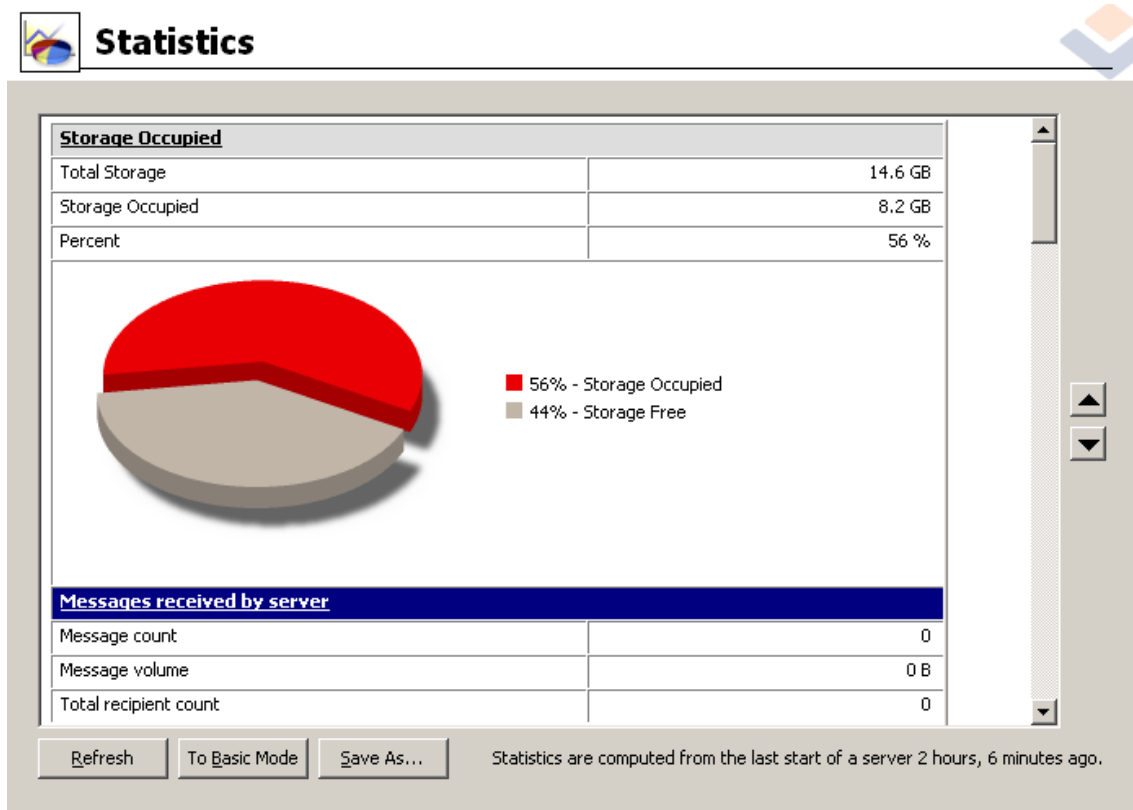


Figure 22.7 Statistics

Chapter 23

Logs

Logs are files where information about certain events (e.g. error and warning reports, debugging information, etc.) are recorded. Each item is represented by one row starting with a timestamp (date and time of the event). Events reported are in English only (they are generated by the *Kerio MailServer Engine*).

23.1 Log settings

When you right-click inside any log window, a context menu will be displayed where you can choose several functions or change the log's parameters (view, logged information).

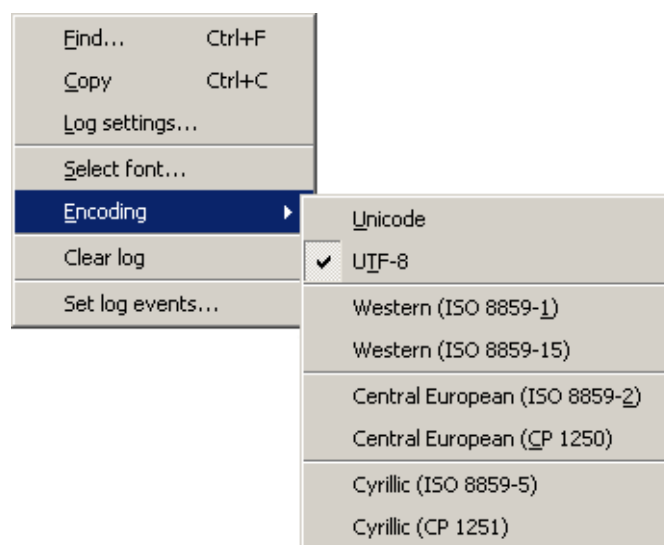


Figure 23.1 Context menu

Copy

Copies the selected text onto the clipboard. You can use the operating system hotkeys to do this (e.g. *Ctrl+C* or *Ctrl+Insert* in Windows).

Find

Use this option to find a particular log row. Insert search criteria into the *Find* entry (words, numerals, characters). Use the *Direction* parameter to define in which direction the logs will be read through (*Up*, *Down*).

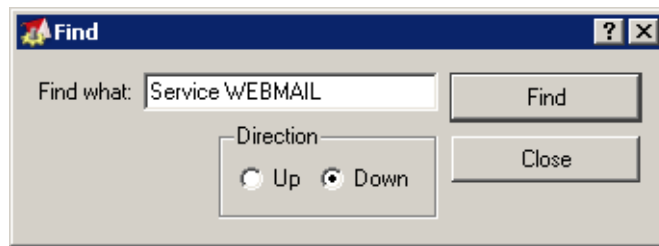


Figure 23.2 Search

Highlighting

Kerio MailServer enables to highlight any part of text in logs. This function is used for better reference.

Click *Highlighting* to open a dialog box where highlighting can be added, changed and removed by using the typical *Add*, *Edit* and *Remove* buttons.

New highlighting can be set in the *Add highlighting* dialog box:

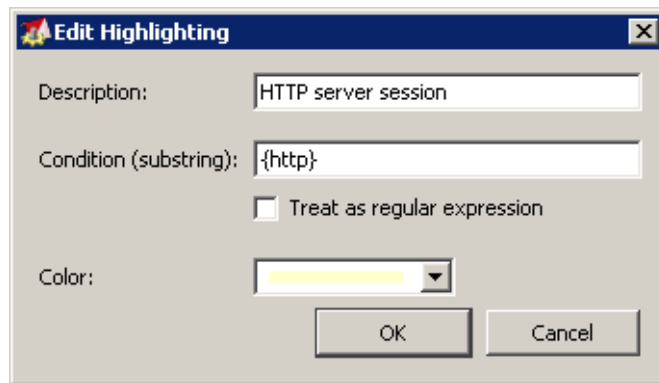


Figure 23.3 Highlighting

- *Description* — description used for better reference.
- *Condition (substring)* — every line containing the substring specified will be highlighted according to the parameters set in this dialog.

If *Treat as regular expression* is enabled, any regular expression can be entered (for advanced users).

Regular expressions are special POSIX expression for a string description. They are created by various flexible patterns that are compared with strings.

- *Color* — select a color used for the highlighting.

Every highlighting is applied to all log types. All lines meeting the condition are highlighted.

Select font

This option opens a standard dialog box for selection of size, style and font for the log.

Encoding

Select encoding for the log.

Log debug

Select this option to open the *Log debug* dialog where you can set parameters for clearing or saving logs.

The File Logging tab

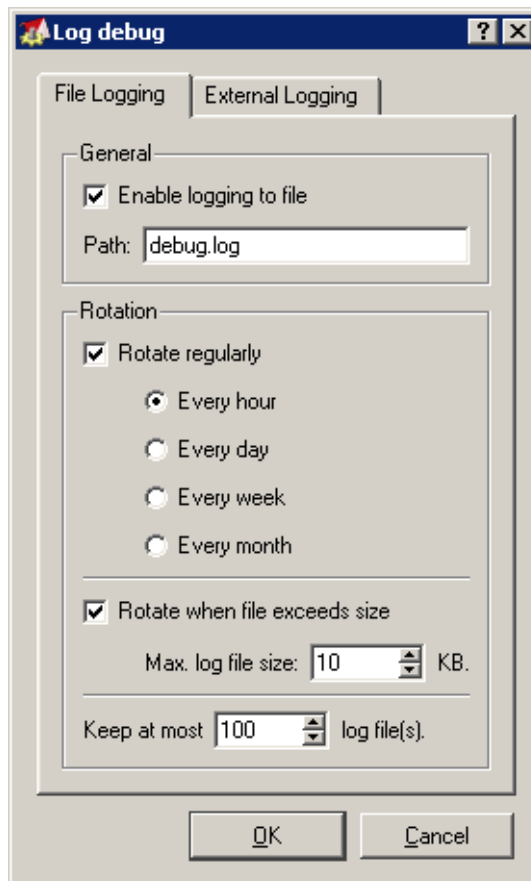


Figure 23.4 File Logging

- *Enable logging to file* — enables logging to a specified file. Use the *File name* entry to specify a path where logs will be saved.
- *Rotate regularly*— select one of the following options:
 - *Every hour* — log is saved once an hour and a new log file is started.
 - *Every day* — log is rotated once a 24 hours.
 - *Every week* — log is rotated once a week.
 - *Every month* — log is rotated once a month.

- *Rotate when file exceeds size* — set maximum log file size (in KBs) in *Max log file size*.
- *Keep at most ... log file(s)* — define how many log files will be stored. The oldest file will be cleared after each rotation.

The External Logging tab

Open the *External Logging* dialog to set logging to a *Syslog* server or to a file. The three options can be combined.

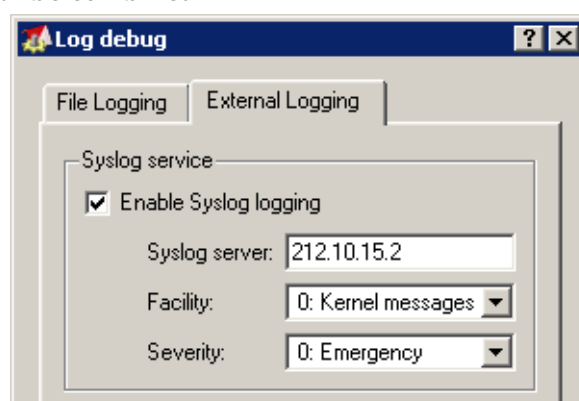


Figure 23.5 Storing logs on Syslog server

- *Enable Syslog logging* — use this option to enable logging to a Syslog server
- *Syslog server* — DNS name or IP address of the particular *Syslog* server
- *Facility* — this entry helps *Kerio MailServer* recognize where a log came from (*Syslog* server can receive logs from various sources)
- *Severity* — set how important the log is (*Syslog* enables filtering of logs with respect to their severity)

Clear log

Clears the log window (information is also removed from the appropriate file).

Messages

Advanced parameters for the logs can be set using this option (for details see below). Available only in the *Debug* section.

23.2 Config

The *Config* log stores the complete history of communication between *Kerio Administration Console* and *Kerio MailServer Engine*. It is possible to determine what administration tasks were performed by a specific user.

The *Config* window contains three log types:

Information about logging in to *Kerio MailServer* administration

Example:

[30/Jun/2004 09:09:18] Admin - session opened for host 127.0.0.1

- [30/Jun/2004 09:09:18] — the date and time of the log creation
- Admin — the name of the user logged in for *Kerio MailServer* administration.
- session opened for host 127.0.0.1 — information about session opening and IP address of the user logged in

Changes in the configuration database

Changes performed in *Kerio Administration Console*. Let's take new user account creation as an example:

[30/Jun/2004 13:09:48] Admin - insert User set Name='jwayne', Domain='company.com', Account_enabled='1', Auth_type='0', Password=xxxxxx PIN='NUL:4444', Rights='1', ForwardMode='0', Qstorage='10485760', Qmessage='5000'

- [30/Jun/2004 13:09:48] — the date and time when the log was created
- Admin — the name of the user logged in for *Kerio MailServer* administration.
- insert User set Name='jwayne'... — parameters that were specified for the new account

Other changes in configuration

A typical example is the backup cycle. After the *Use* button in *Configuration / Backup* section is pressed, the time and date of each backup is inserted into the *Config* log.

[30/Jun/2004 09:29:08] Admin - Store backup started

- [30/Jun/2004 09:29:08] — date and time when the backup was started
- Admin — the name of the user logged in for *Kerio MailServer* administration.
- Store backup started — information that the backup was started

23.3 Mail

The *Mail* log contains information about individual messages processed by *Kerio MailServer*. The log includes all message types:

- incoming messages,
- outgoing messages,
- mailing list messages,
- DSN (Delivery Status Notification) — messages generated automatically by the server (system messages — e.g. information that the message is undeliverable, that it could not be delivered in the defined time, that the user sent a virus-infected message, etc.).

Incoming and outgoing messages

All messages received via SMTP or HTTP protocols or downloaded via POP3. Here is an example of two log lines associated with one message as well as description of individual items:

```
[30/Nov/2005 17:57:14] Recv: Queue-ID: 438dd9ea-00000000,
Service: SMTP, From: <jwayne@company.com>,
To: <thenry@company.com>, Size: 1229, User: jwayne@company.com,
Sender-Host: 195.39.55.2, SSL: yes
[30/Nov/2005 17:57:15] Sent: Queue-ID: 438dd9ea-00000000,
Recipient: <thenry@company.com>, Result: delivered,
Status: 2.0.0
```

- [30/Nov/2005 17:57:14] — the date and time when the message was delivered or sent.
- Recv/Sent — this section provides information whether the server has already received the message or the message is just being sent. The status can therefore be Sent or Recv (i.e. Recieved).
- Queue-ID: 438d6fb6-00000003 — the number generated by the server in the queue of outgoing messages. It is an identifier which uses identical numbers for all log lines associated with one messages. Each message is first received by the server, then it is sent. This implies that at least two log lines must belong to each message (for reception and sending). Moreover, each message can be delivered to multiple users (each addressee has a special log line).
- Service: HTTP — protocol, that has been used by the server to receive the message (HTTP, SMTP). This information is included in incoming messages only. The information is not displayed for outgoing messages, it would be meaningless. All outgoing messages are sent by SMTP.
- From: <jwayne@company.com> — email address of the sender
- To: <jwayne@company.com> — email address of the recipient
- Size: 378 — size of the message in bytes
- User: jwayne@company.com — user account from which the message was sent.
- Sender-Host: 195.39.55.2 — IP address of the computer from which the message has been sent
- SSL: yes — informs whether the connection is SSL-secured (displayed for SMTP only)
- Recipient: <thenry@company.com> — email address of the addressee.
- Result: delivered — information about the result of the delivery process.
- Status: 2.0.0 — code of the SMTP response (for detailed information, see RFC 821). If the code starts with the 2 digit, the message was delivered successfully. If the code starts with the 4 or the 5 digit, the message delivery failed.

Server-generated messages

Messages of this type are usually generated by *Kerio MailServer*. If the delivery fails, the sender receives a delivery status notification (DSN).

[30/Nov/2005 15:31:40] Recv: Queue-ID: 438db7cc-00000000,
Service: DSN, From: <>, To: <dbeckham@company.com>,
Size: 1650, Report: failed

- [30/Nov/2005 15:31:40] — the date and time when the message was generated
- Recv: — this section provides information whether the server has already received the message or the message is just being sent. The status can therefore be Sent or Received.
- Queue-ID: 438db7cc-00000000 — the number generated by the server in the queue of outgoing messages.
- Service: DSN — *Delivery Status Notification*; messages generated by *Kerio MailServer*.
- From: <> — this item is empty because the message was generated by the mail server
- To: <jwayne@company.com> — email address of the recipient
- Size: 1650 — message size in bytes
- Report: failed — the type of notification

Mailing list messages

The *Mail* log contains all mailing list messages. The individual postings, as well as mailing list control messages are logged

[30/Nov/2005 19:09:11] Recv: Queue-ID: 438deac7-00000009,
Service: List, From: <Discussion@company.com>,
To: <jwayne@company.com>, Size: 3302,
Answer: subscribe response

- [30/Nov/2005 19:09:11] — date and time when the message was received
- Recv: — this section provides information whether the server has already received the message or the message is just being sent. The status can therefore be Sent or Received.
- Queue-ID: 438deac7-00000009
- Service: List — mailing list flag
- <discussion@company.com> — email address of the sender
- To: <jwayne@company.com> — email address of the recipient
- Size: 1397 — size of the message in bytes
- Answer: subscribe response — type of message

Sieve

Messages generated by a user filter (e.g. autoreply).

23.4 Security

The *Security* log contains information related to *Kerio MailServer's* security. It also contains records about all messages that failed to be delivered. The security log contains the following types of events:

Viruses and forbidden attachments detected

Example: a message that contains a virus:

```
[16/Jun/2004 18:37:17] Found virus in mail from
<missgold18@hotmail.com> to <support@kerio.com>:
W32/Netsky.p@MM
```

- [16/Jun/2004 18:37:17] — the date and time when the virus was detected
- Found virus in mail — action performed (information that the virus was found)
- from <missgold18@hotmail.com> — email address of the sender
- to <support@kerio.com> — email address of the recipient
- W32/Netsky.p@MM — the type of virus contained in the message

Messages rejected by spam filter

A message with high spam score:

```
[16/Jun/2004 18:37:17] Message from
<missgold18@hotmail.com> to <support@kerio.com>
rejected by spam filter: score 9.74, threshold 5.00
```

- [16/Jun/2004 18:37:17] — the date and time when the message was rejected
- from <missgold18@hotmail.com> — email address of the sender
- to <support@kerio.com> — email address of the recipient
- rejected by spam filter — action performed (rejection by spam filter)
- score 9.74, threshold 5.00 — *SpamEliminator* evaluation

Failed login attempts

This log contains information about invalid login attempts. These are usually caused by an invalid username/password or blocked IP address. The reason for a specific failed login can be found also in the *Warning* log (see chapter 23.5).

```
[13/Apr/2004 17:35:49] Failed IMAP login from 192.168.36.139,
missing parameter in AUTHENTICATE header
```

- [13/Apr/2004 17:35:49] — the date and time of the failed login
- Failed IMAP login — action performed (failed login attempt)
- from 192.168.36.139 — IP address of the computer used for login attempt

There are several possible reasons for login failure:

- missing parameter in AUTHENTICATE header — an incorrect or invalid header with login data has been sent
- authentication method PLAIN is disabled — the authentication method is disabled in *Kerio MailServer*
- authentication method CRAM_MD5 is invalid or unknown — *Kerio MailServer* is unable to perform authentication using this method
- error during authentication with method CRAM-MD5 — an error occurred during authentication, e.g. during communication with the authentication server
- authentication with method CRAM-MD5 cancelled by user — the authentication was cancelled by the user (client)
- (Failed IMAP login from 127.0.0.1), authentication method PLAIN — the authentication of the user failed (the user does not exist, the password is incorrect, the user account in *Kerio MailServer* is disabled or the authentication couldn't be performed due to the lack of authentication data in *Active Directory*)

Server misuse attempts (relaying)

An example of relaying attempt:

[11/Jun/2004 00:36:07] Relay attempt from IP address
61.216.46.197, mail from <wgiwknovry@hotmail.com>
to <fodder@falls.igs.net> rejected

- [11/Jun/2004 00:36:07] — the date and time
- Relay attempt — action performed (failed relaying attempt)
- 61.216.46.197 — IP address of the computer used for relaying attempt
- from <wgiwknovry@hotmail.com> — email address of the sender
- to <fodder@falls.igs.net> — email address of the recipient
- rejected — action performed (the message was rejected)

Antibombing

Server overload protection — see chapter 16.2, section *Security Options*.

[16/Jun/2004 18:53:43] Directory harvest attack from
213.7.0.87 detected

- [16/Jun/2004 18:53:43] — the date and time of the failed attack
- Directory harvest attack — type of attack
- from 213.7.0.87 — IP address of the computer used for the attempt
- detected — action performed (detected and blocked)

If the sender was found in databases of blacklisted servers

The sender was found in a blacklist database (*ORDB*, own IP address group)

[13/Apr/2004 17:44:02] IP address 212.76.71.93
found in DNS blacklist *ORDB*, mail from

- `<emily.macdonald@nmc-uk.org> to <support@kerio.com>`
- `[13/Apr/2004 17:44:02]` — the date and time when the message was received
- `212.76.71.93` — IP address used for sending the message
- `found in DNS blacklist ORDB` — type of action (the address was found in a database of blacklisted servers)
- `from <emily.macdonald@nmc-uk.org>` — email address of the sender
- `to <support@kerio.com>` — email address of the recipient

23.5 Warning

The *Warning* log displays warning messages about errors of little significance. Typical examples of such warnings are messages stating that a user with administrator rights has a blank password, that a user account of a given name does not exist or that a remote POP3 server is unavailable.

Events causing display of warning messages in this log do not greatly affect *Kerio MailServer's* operation. They can, however, indicate certain (or possible) problems. The *Warning* log can help if for example a user is complaining that certain services are not working.

23.6 Error

In contrast to the *Warning* log, the *Error* log displays errors of great significance that usually affect the MailServer's operation. The *Kerio MailServer* administrator should check this log regularly and try to eliminate problems found here. If this is not done, users are in danger of not being able to use certain (or even all) services. They may also lose their messages or security problems may occur (the MailServer can for example be misused to send spam email or virus-infected email).

Typical error messages displayed in the *Error* log pertain to: service initiation (usually due to port conflicts), disk space allocation, antivirus check initialization, improper authentication of users, etc.

23.7 Spam

The *Spam* log displays information about all spam emails stored in *Kerio MailServer*. Information about individual spam messages are displayed in rows. The logs differ according to the mode of spam detection. The *Spam* log lists also messages that have been marked as spam by *Kerio MailServer*, but the user marked them as regular messages.

Spam message detected by filter

The message was marked as spam by *Kerio MailServer* filter:

[06/Sep/2004 08:43:17] Message marked as
spam with score: 8.00, To: dbeckham@company.com,
Message size: 342, From: thenry@company.com, Subject:

- [06/Sep/2004 08:43:17] — date and time when the spam was detected
- Message marked as spam with score: 8.00 — type of action (the message was marked as spam because the score evaluated by spam filter was too high)
- To: jwayne@company.com — email address of the recipient
- Message size: 342 — message size in bytes
- From: jsmith@company.com — email address of the sender
- Subject: — the subject of the message (empty in this case)

Spam message detected by user

The message was marked as spam by user:

[06/Sep/2004 08:40:39] User thenry@company.com marked a
message as spam, Folder: ~thenry@company.com/INBOX,
Size: 462, From: "Daniel Beckham" <dbeckham@company.com>,
Subject: Hallo

- [06/Sep/2004 08:40:39] — date and time when the message was marked as spam
- User jwayne@company.com — email address of the recipient
- marked a message as spam — type of action (the message was marked as spam by user)
- Folder: ~jwayne@company.com/INBOX — the folder where the message is stored
- Size: 462 — message size in bytes
- From: "John Smith" <jsmith@company.com> — email address of the sender
- Subject: Hallo — the subject of the message

The message is not spam

The message was marked as not spam by a user:

marked a message as not spam, Folder:
~dbeckham@company.com/Junk E-mail, Size: 500,
From: "Thomas Henry" <thenry@company.com>, Subject: *SPAM*

- [06/Sep/2004 08:43:32] — date and time when the message was marked as not spam
- User: jwayne@company.com — email address of the recipient
- marked a message as not spam — type of action (the message was marked as not spam by user)
- Folder: ~jwayne@company.com/Junk E-mail — the folder where the message is stored (in this case, the folder for spam messages is required)
- Size: 500 — message size in bytes
- From: "John Smith" <jsmith@company.com> — email address of the sender

- Subject: ****SPAM**** — the subject of the message

23.8 Debug

Debug (debug information) is a special log which can be used to monitor certain kinds of information, especially for problem-solving. As default, it displays information relating to starting and stopping of *Kerio MailServer*, lists the services and the addresses and ports used for connection. Other information relates to services and processes used to operate the server.

The other information describe services and processes which handle the server. Too much information could be confusing and impractical if displayed all at the same time. Usually, you only need to display information relating to a particular service or function.

Warning: Displaying a vast amount of information also reduces *Kerio MailServers* speed. We recommend that you only display information that you are interested in and only when necessary.

Debug log settings

For the above reasons the *Debug* log allows you to define what information it will display. This can be done using the *Set log events* option in the context menu of the *Debug* window.

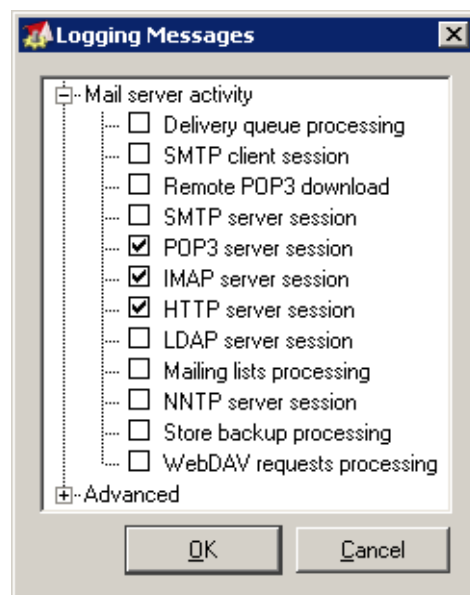


Figure 23.6 Debug log settings

Mail server activity section:

Delivery queue processing

Processing of the Mail Queue (sending and receiving messages, re-scheduling, etc.)

SMTP client session

Sending outgoing mail (communication between *Kerio MailServer* and the relay SMTP server or the target domain's MailServer). The log includes commands and responses of the client and the server ordered by time when individual events happened. Therefore, this log can be very helpful for resolving problems regarding email sending.

Remote POP3 download

Retrieval of remote POP3 mailboxes (*Kerio MailServer* in the role of a POP3 client) and sorting rules (when a message is received or downloaded from a remote POP3 mailbox). The *Remote POP3 download* log together with *Alias processing* can be helpful when you experience problems with domain mailbox.

SMTP server session

Detailed information about communication between clients and the SMTP server. This log can be helpful when you experience problems with MX records.

POP3 server session

Detailed information about communication between clients and the POP3 server. Together with *IMAP server session* and *HTTP server session*) helps to solve problems with retrieving email from the mailboxes.

IMAP server session

Detailed information about communication between clients and the IMAP server. The log also provides information on communication via the MAPI interface.

HTTP server session

Communication between clients and *Kerio MailServer* using the *Kerio WebMail* interface

LDAP server session

Detailed monitoring of communication between clients and the LDAP server, and search for contacts in the database.

Mailing list processing

Mailing lists monitoring (logins, logouts, message sending, moderators performance, etc.).

NNTP server session

A detailed report on communication with the news server.

Store backup processing

The report lists the backup process, browsing and backing up of all folders. Use this report to be sure if the backup process is correct and if it was not interrupted. Should an error occur while performing backup, a record will be entered in the *Error* log (see chapter 23.6).

WebDAV requests processing

The log lists all actions of the WebDAV interface. It is useful especially for solving communication issues between *Kerio MailServer* and *MS Entourage*.

Advanced section:

Mail folder operations

Operations with user and public folders (opening, saving messages, closing) This log can be used to resolve problems regarding mapping of public folders.

Alias processing

Processing of aliases (during reception of a message or its download from a remote POP3 mailbox). The *Alias processing* log is used together with *Remote POP3 download* to solve problems with domain mailbox sorting.

Antivirus check processing

Communication with the antivirus program, processing of individual message attachments. This log can be used if the infected messages are not detected by an antivirus program and are delivered to users.

Sieve filter processing

Filtering messages according to user filters

DNS resolver

Finding target domain SMTP servers through DNS MX record lookup

Authentication modules

External authentication of users (NT domain, Kerberos, PAM)

Network connections and SSL

Establishing connections to remote servers (on the TCP level), DNS requests, SSL encrypting, etc.

Directory service lookup

Queries to the internal user database (*Active Directory*). This log can be used in case of problems with import of users from local domains.

Contacts processing

Detailed information on contact processing provided in the *vCard* format.

Spam filter processing

Logs the messages with high *SpamEliminator* rating.

Update checker activity

Reports any communication with *update.kerio.com*, where all new versions of *Kerio MailServer* are available. From this server, updates of the *Kerio Outlook Connector* are also downloaded.

SyncML synchronization

This option reports any activity that occurred between *Kerio MailServer* and *Kerio Synchronization Plug-in* during synchronization.

SPF check

This option reports all information about SPF queries to SMTP servers. It can be used for solving problems with SPF check.

PHP engine messages

This option records *Kerio WebMail* information. This information is an extension to the *Error* log and it can be used for troubleshooting of *Kerio WebMail* issues.

23.9 Performance Monitor (under Windows)

If *Kerio MailServer* is installed under the Windows 2003, 2000, or XP operating system, the optional component *Performance Monitor* can be installed (for details, see chapter 3.3). *Performance Monitor* is a plug-in for the *Performance* system tool that is included in *Administrative Tools*.

In *Performance Monitor*, open the *System Monitor* section. To add new objects for monitoring, open the dialog window by clicking on the + button.

In *Performance object* select the *Kerio MailServer* item. In the left button at the bottom select statistics that you want to monitor. You can use any of the statistics offered by *Kerio MailServer* (see chapter 22.5, or the *Status/Statistics* section in *Kerio Administration Console*). Click on the *Explain* button to get more information about the selected object.

Notes:

- If the *Kerio MailServer* item is not displayed in the *Performance object* field in the object list, the *Performance Monitor* plug-in is not installed or it is incomplete. We recommend running the *Kerio MailServer* installation program again (see chapter 3.3).
- For detailed information about *Performance Monitor* see Help in Windows.

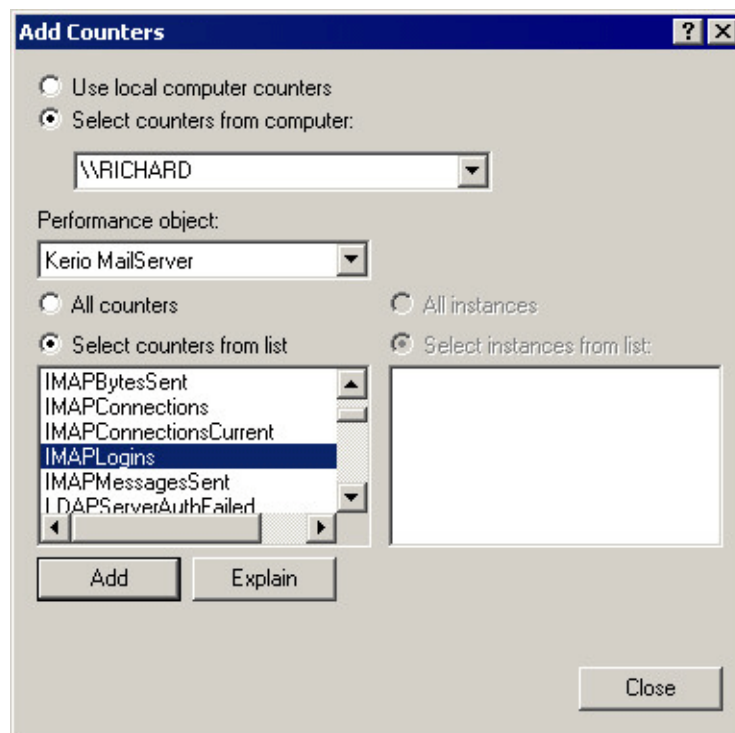


Figure 23.7 Performance Monitor

Chapter 24

Kerio MailServer Environment

24.1 Configuring Email Clients

This chapter contains basic information about how to set email clients (i.e. programs used to read and write email messages). It does not focus on particular client software but gives you general advice that you should follow in order for the client to work properly with *Kerio MailServer*.

Configuring an Email Account

An email account is a group of parameters describing the incoming and outgoing mail servers and the conditions for their use. Most email clients allow switching between multiple accounts. Let's create a new account that will be used for retrieving and sending messages via *Kerio MailServer*.

Note: The following description of settings was created using the *Microsoft Outlook Express 6.0* email client. However, basic account settings are very similar in all email clients.

Outgoing (personal) email address

This address should consist of the name of the user and the domain as it is set in *Kerio MailServer*, e.g. `smith@ourcompany.com`.

Name of the user

This can be anything as it is only displayed in the message header. Using special characters (typically in non-English versions) might cause problems.

It does not relate to the full name or description in *Kerio MailServer*. A decent user sends messages using his/her own name!

Outgoing mail server (SMTP)

IP address or the DNS name of the host on which *Kerio MailServer* is running (e.g. `192.168.1.1` or `mail.ourcompany.com`).

Incoming mail server

IP address or the DNS name of the host on which *Kerio MailServer* is running (e.g. `192.168.1.1` or `mail.ourcompany.com`).

Incoming mail server type

POP3 or IMAP. If both services run on *Kerio MailServer* the user can choose whichever suits him/her best. The protocol type cannot be altered later. It is important to realize that if the user accessed the account using the IMAP protocol and now he/she wishes to use POP3, he/she will only be able to download messages from the *INBOX* folder.

User name and password

The name and password for the *Kerio MailServer* user account. If the account is not in the primary domain a full email address must be used for the user name.

Authentication on the outgoing (SMTP) server

This needs to be set if anti-spam protection is enabled in *Kerio MailServer* (see chapter 17) as well as relay control — sending email to any domain is not permitted from the client's IP address (see chapter 17). If this is not set the user will only be able to send email within the local domains.

Server requires secure communication

These options define whether a non-encrypted or an SSL-encrypted connection should be used during sending or receiving of email. With *Kerio MailServer* you can use a secured connection in both cases (if appropriate services are running), which is recommended.

Secure password authentication (SPA/NTLM)

This function can be used if a user logs into an NT domain and the user's account in the *Kerio MailServer* is set to authenticate the user in the NT domain. This allows the client software to use the same authentication credentials as the ones for logging into a domain.

Directory Service

You can use the *Kerio MailServer* LDAP server as a directory service (for details refer to chapter 20)

IMAP Folders Administration

After creating a mail account using the IMAP protocol the client will download a list of folders from the server and display it. The user can choose the folders that are to be displayed (this can be changed later). In the client software the user can create, rename or delete folders in the same way as in the *Kerio WebMail* interface. It is important to note that these folders are stored at the server and not locally as with POP3 protocol.

It is important to ensure that the email client and the *Kerio WebMail* interface use the same folder names for sent mail (*Sent Items*) and draft messages (*Drafts*).

The email client can set synchronization for each folder. If a folder is synchronized with the server, each new message will be immediately displayed in the client software. This requires a permanent connection to the server. If the client is connected using a dial-up line, synchronization can only be performed manually or in defined time intervals.

24.2 Web browsers

Recommended browsers for the full version of *Kerio WebMail* are as follows:

- *Microsoft Internet Explorer* 6.0 or higher
- *Safari* 1.2 or higher
- *Firefox* version 1.0 or higher
- *Mozilla* 1.7 or higher

From technical reasons, in older versions of the browsers and the types not listed, it is not possible to run the full version of *Kerio WebMail*. However, it is possible to use its simplified version, *Kerio WebMail Mini*. *Kerio WebMail Mini* is run automatically in older versions of browsers, in text-based browsers such as *Lynx* or *Links*, on PDA devices, on cellular phones, etc. *Kerio WebMail Mini* does not use CSS and JavaScript.

To use the secured access to the *Kerio WebMail* interface (by HTTPS protocol), the browser must support SSL encryption. If this can be configured (e.g. in MS Internet Explorer) we recommend enabling support for SSL 3.0 and TLS 1.0.

24.3 Firewall

Quite often, *Kerio MailServer* is installed on a local network protected by a firewall or directly on the firewall host. To assure connectivity the system administrator then has to set several settings.

Ports

If the MailServer is to be accessible from the Internet, certain ports have to be opened (mapped) in the firewall. Generally, any open port means a security hole; therefore, the less mapped ports you have the better.

When mapping ports for *Kerio MailServer* the following rules should be followed:

- Port 25 must be mapped if you would like the SMTP server to be accessible from the Internet. This must be done if an MX record for the given domain (or more domains) points to the MailServer. In this case it is necessary to enable antispam protection (see chapter 17) and relay control (see chapter 16.2), so that the MailServer cannot be misused. Any SMTP server on the Internet can connect to your SMTP server to send email to one of the local domains. For this reason access must not be restricted to a selected IP address group.

If all incoming mail is to be downloaded from remote POP3 mailboxes, port 25 does not need to be opened.

- Ports for other services (POP3, IMAP, HTTP, LDAP and Secure LDAP) need to be opened if clients wish to access their mailboxes from locations other than the protected local network (typically notebook users). In this case we strongly recommend using only secure versions of all services and opening only the appropriate ports on the firewall (i.e. 663, 443, 993 and 995).
- If subnets or IP address ranges from which remote clients connect can be defined, we recommend allowing access to ports only from these addresses. This is not possible if the user travels world-wide and connects to the Internet randomly using many different ISPs.

Dial-up Connection

If *Kerio MailServer* and a firewall run on the same machine that is connected to the Internet via a dial-up line, a request may arise asking that the MailServer use a different dial-up connection (e.g. via a different ISP) than the firewall for accessing the Internet. The firewall then has to know both of these connections or it will block the packets going through the connection used by the MailServer (no unknown packet is allowed to pass the firewall — neither outgoing or incoming).

Chapter 25

Deployment Examples

This chapter shows how to set *Kerio MailServer* in different conditions. Each example is essentially an applied *Quick Checklist* (see chapter 1) for a given situation. These examples should help you set up *Kerio MailServer* quickly and easily for your company.

25.1 Leased Line

Information and Requirements

1. The company has the domain `ourcompany.com` and a primary MX record points to the computer where *Kerio MailServer* will be installed (the name of the computer in DNS is `mail.ourcompany.com`)
2. The computer is connected to the Internet via a leased line
3. There is no relay SMTP server
4. The company uses the NT domain DOMAIN and users will be authenticated in this domain
5. The production department will have an address `production@ourcompany.com` and the sales department will have the address `sales@ourcompany.com`
6. Some users would like *Kerio MailServer* to download messages from their mailboxes on the Internet and deliver them to their local mailboxes
7. AVG 7.0 antivirus program will be used for checking mail for viruses and no EXE, COM, BAT and VBS attachments can be sent
8. Remote administration of *Kerio MailServer* will only be allowed from the IP address `67.34.112.2` (external administrator)

Implementation

1. In the *Configuration → Domains* section, create the primary local domain `ourcompany.com` and enter the server's DNS name `mail.ourcompany.com`. In the *Authentication* tab enter the name of the NT domain `DOMAIN`.
2. In the *Domain Settings → Users* section, use the *Import* button to import all users from the domain. This way the users will not have to be added manually.
3. In the *Domain Settings → Groups* section, create the groups *Production* and *Sales* and add appropriate users to them.
4. In the *Domain Settings → Aliases* section, define the aliases `production` and `sales` to be delivered to the corresponding user groups.
5. The Internet connection is permanent. In the *Configuration → Internet Connection* section, select the *Online* option.
6. Outgoing mail will be sent directly to the target domains. In the *Configuration → SMTP Properties* section, select the *Deliver directly using DNS MX records* option.
7. In the *Configuration → POP3 Download* section, define retrieval of email from requested external mailboxes. For each mailbox, select a user to whom messages from the mailbox will be delivered.
8. Set up scheduling for downloading of mail from the remote mailboxes. The leased line is fast and is connected permanently so messages from the mailboxes can be downloaded quite often. Set scheduling every 10 minutes (*Every 00:10*). Outgoing mail is sent immediately and no mail is received using ETRN — only tick *Receive POP3 mailboxes*.
9. In the *Configuration → Antivirus* section, enable antivirus control and choose the *AVG 7.0* module. In the *Attachment Filter* tab enable filtering and set the names of forbidden files — i.e., `*.exe`, `*.com`, `*.bat` and `*.vbs`.
10. In the *Configuration → Definitions → IP Address Groups* section, create a group named `Remote administration` and assign it a single IP address (host) `67.34.112.2`.
11. In the *Configuration → Remote Administration* section, tick *Enable administration from network* and *Only from this IP address group*. Choose the created group *Remote administration* here.

25.2 Dial-up Line + Domain Mailbox

Information and Requirements

1. The company uses the domain `othercompany.com` and all messages sent to this address are stored in a domain mailbox entitled `other company` at the server `pop3.isp.com` with the username `othercompany` and password `password`
2. Internet connection is via a dial-up line
3. The ISP enables sending outgoing email via their server `smtp.isp.com`,
if the user authenticates by username and password (the same situation as in case of POP3).
4. During working hours (Mon-Fri 8:00-17:00) mail will be downloaded every hour and after working hours at 20:00, 0:00 and 5:00

Implementation

1. In the *Configuration → Domains* section, create the primary local domain `othercompany.com` and set the Internet name of the server `mail.othercompany.com` (this is more or less fictitious but it contains the domain name). The domain is defined as local, which means that mail sent between local users will not be sent to the Internet and downloaded back again.
2. In the *Domain Settings → Users* section, create user accounts for all local users.
3. The server will connect to the Internet using a dial-up connection (that already exists in the system). In the *Configuration → Internet Connection* section, choose the *Offline* option, tick the field *Use RAS to connect to Internet*, choose the requested RAS connection and enter the appropriate username and password.
4. All outgoing mail will be sent to a relay SMTP server. In the *Configuration → SMTP Properties* section, select *Use relay SMTP server* and enter its name — `smtp.isp.com`. The server requires authentication — enable the option *Relay server requires authentication* and fill in the appropriate username and password. Set the authentication type to *SMTP AUTH Command*.
5. In the *Configuration → POP3 Download* section, *Accounts* tab, define downloading of the domain mailbox `othercompany` at the server `pop3.isp.com`. Mail from this

mailbox will be delivered using sorting rules — select *Use sorting rules*. It is recommended to consult selection of a preferred header with the administrator of the server where the mailbox is located. The default *Received* header should be suitable in most of situations.

6. In the *Configuration → POP3 Download* section, *Sorting Rules* tab, set sorting rules for individual users' email addresses.
7. In the *Configuration → Definitions/Time Ranges* section, create a time interval *Working hours*, containing the range 8:00:00-17:00:00 valid from Monday through Friday, to be used in scheduling.
8. Set up scheduling for message retrieval from the POP3 box and sending of messages from the mail queue. Add scheduling for every hour (*Every 1:00*) valid at the time interval *Working hours* and three schedulings for certain times (*At*) that will be valid all the time. For all schedulings tick the *Receive POP3 mailboxes* but also *Send mail in mail queue*.

25.3 Dial-up Line + ETRN

Information and Requirements

1. The company uses the domain `thirdcompany.com` and the primary MX record points to the computer where *Kerio MailServer* is installed (its DNS name is `mail.thirdcompany.com`)
2. The secondary MX record is directed to the SMTP server.
`etrn.isp.com`,
which supports the ETRN command and requires authentication by username and password.
3. The computer is connected to the Internet via a dial-up line (a static IP is assigned, to which the DNS name `mail.thirdcompany.com` is assigned)
4. The ISP enables sending outgoing email via their server
`smtp.isp.com`,
if the user authenticates by username and password.
5. During working hours (Mon-Fri 8:00-17:00) mail will be downloaded every hour and after working hours at 20:00, 0:00 and 5:00

Implementation

1. In the *Configuration → Domains* section, create the primary local domain `thirdcompany.com` and enter the DNS name of the server `mail.thirdcompany.com`. When the line is up *Kerio MailServer* will function as the primary server for this domain. While the line is down email will be sent to a secondary server.
2. In the *Domain Settings → Users* section, create user accounts for all local users.
3. The server will connect to the Internet using a dial-up connection (that already exists in the system). In the *Configuration → Internet Connection* section, select *Offline* and tick *Use RAS to connect to the Internet*. Choose the requested dial-up connection and fill in the appropriate username and password.
4. All outgoing mail will be sent to a relay SMTP server. In the *Configuration → SMTP Properties* section, select *Use relay SMTP server* and enter its name — `smtp.isp.com`. The server requires authentication — enable the option *Relay server requires authentication* and fill in the appropriate username and password. Set the authentication type to *SMTP AUTH Command*.
5. Under *Configuration → ETRN Download*, define the following information:
server: `etrn.isp.com`,
domain: `thethirdparty.com`,
Server requires authentication, enter username and password.
6. In the *Configuration/Definitions/Time Ranges* section, create a time interval *Working hours*, containing the range 8:00:00-17:00:00 valid from Monday through Friday, to be used in scheduling.
7. Set up scheduling for sending and downloading of messages. Add scheduling for every hour (*Every 1:00*) valid at the time interval *Working hours* and three schedulings for certain times (*At*) that will be valid all the time. For all schedulings tick the *On-demand mail relay* option (i.e. receiving mail using ETRN) but also *Send mail in mail queue*.

Note: To keep the example as simple as possible, suppose that users `boss` and `secretary` work in the headquarters and users `technician` and `programmer` work in the branch office. The following description is focused on these special requirements — it does not include detailed configuration of the SMTP server, remote administration, etc.

Implementation

Headquarters (configuration at the primary server mail.company.com)

1. In the company's headquarters (at the primary server `mail.company.com`) in *Kerio MailServer*, set the `company.com` domain as the local primary domain.
2. In this domain, accounts of local users are defined (of those who work in the headquarters).
3. If *Kerio MailServer* is behind the firewall, it is necessary to make port 25 available for the SMTP service.
4. Create the `ldn.company.com` domain where no users and aliases will be defined. Set the *Forwarding* tab under *Domains* in a way that email for the `ldn.company.com` domain is forwarded to the `mail-ldn.company.com` server of the branch office.

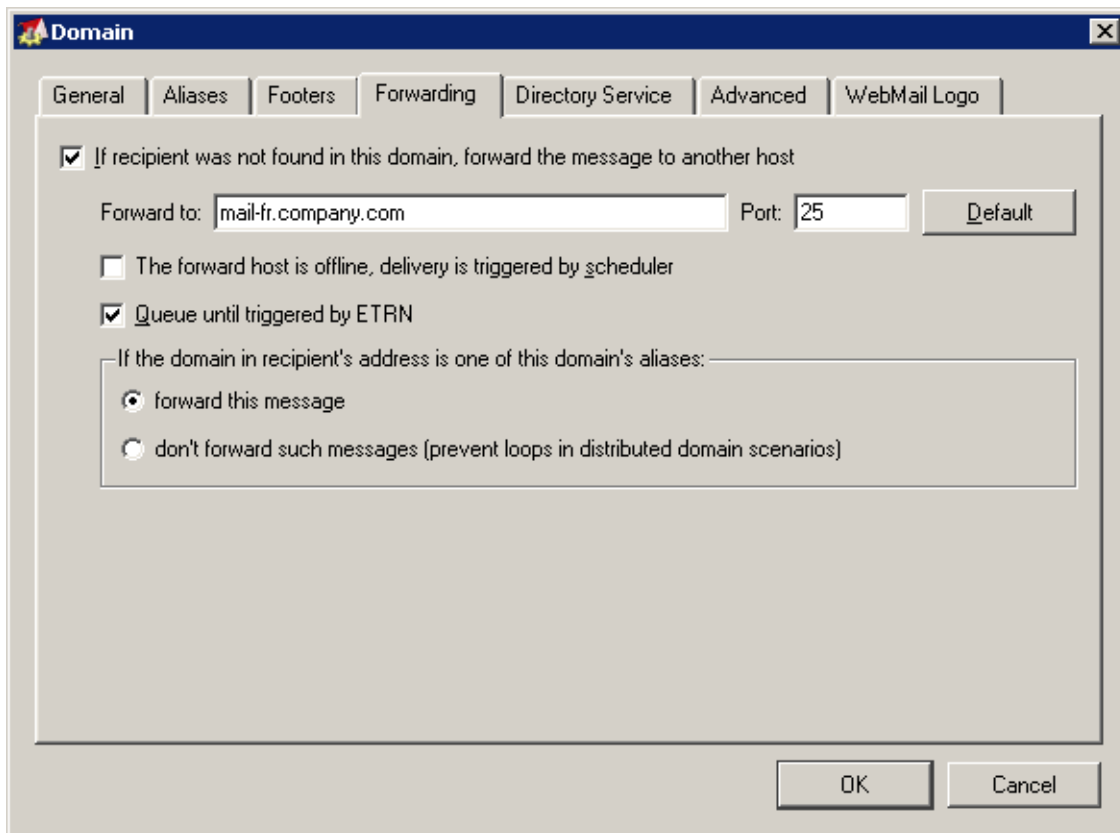


Figure 25.2 Forwarding settings

5. Next, set aliases for all users at the branch office (*Domain Settings* → *Aliases*), in this case for the users `technician` and `programmer`. These aliases provide that email for corresponding users is delivered to domain `ldn.company.com`.

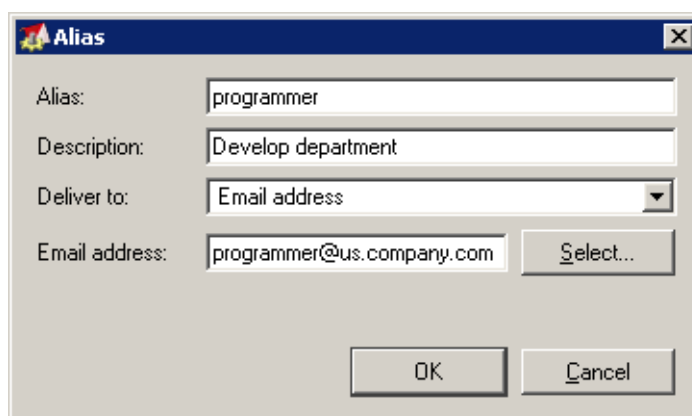


Figure 25.3 Alias settings

Branch office (configuration at the server mail-ldn.company.com)

1. Create a local primary domain company.com with the alias ldn.company.com.
2. In the local primary domain, create accounts for all users in this branch office (for those who will have local mailboxes at the filial).
3. Set that email addressed to the domain company.com is forwarded to the headquarters' server mail.company.com, while messages with the domain alias in the recipient's address are not forwarded. This option guarantees that messages where username or its alias is not specified correctly in the recipient's address are caught.

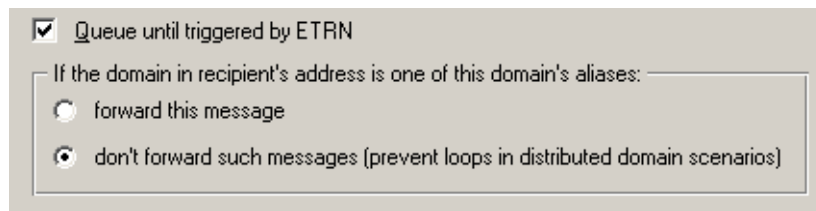


Figure 25.4 Anti-Loop settings

Warning: The wildcard alias should not be used in branch office's server's, otherwise the email for the headquarters will not be forwarded.

Recommendation: Set a secondary DNS MX record for the filial's server. This will help you avoid problems in case of the headquarters' primary server's failure.

Notes:

- If users want to access their email remotely (e.g. using *Kerio WebMail*), they will always connect to the server where their local accounts are created (i.e. users in the headquarters will connect to mail.company.com and users in the branch office connect to the server mail-ldn.company.com).
- The *Free/Busy* calendar will display only information regarding local users of the particular server.

For a detailed example of configuration of a company with multiple branch offices, read the *Multiple servers managing one domain* article in the *Kerio Technologies* knowledge base at <http://support.kerio.com/>.

25.5 Setting up the backup mail server

Information and Requirements

1. A company has own `company.com` domain, the primary MX record points to the computer where primary mailserver is installed. The primary mail server's DNS name is `mail1.company.com`.
2. Create the backup server for the primary mailserver (its DNS name will be `mail2.company.com`). A basic version of *Kerio MailServer* can be used, because in this case there is no need to create user accounts.

Implementation

1. Create the secondary MX record (with lower priority) in DNS for the `company.com` mail domain for (`mail2.company.com`) backup server.
2. After the backup of *Kerio MailServer* is installed, create a primary domain in the configuration wizard and assign it the same name as the primary mailserver, i.e. `company.com`.
3. No user accounts are set up in this domain.
4. In *Configuration* → *Domains* section of the *Kerio MailServer* administration console (chapter 8.5), specify message forwarding to the `mail1.company.com` primary mailserver (see picture 25.5).

There are multiple ways of forwarding messages:

- The best way of setting up forwarding from the backup server is to set the primary server in the way that it queries the secondary server regularly using the ETRN command. This procedure saves time because the servers are not connected to an unavailable primary server. The primary server must support the ETRN command.

Kerio MailServer supports using the ETRN command for requesting emails (see chapter 16.5). If you use *Kerio MailServer* as a primary mailserver, we recommend this option. *Kerio MailServer* also sends the ETRN command to different servers upon each server startup and thus all mail is downloaded to the server in the shortest possible time after failure.

If you wish to use this method of forwarding emails, enable the *Queue until triggered by ETRN* option for the `company.com` domain (*Configuration* → *Domains*).

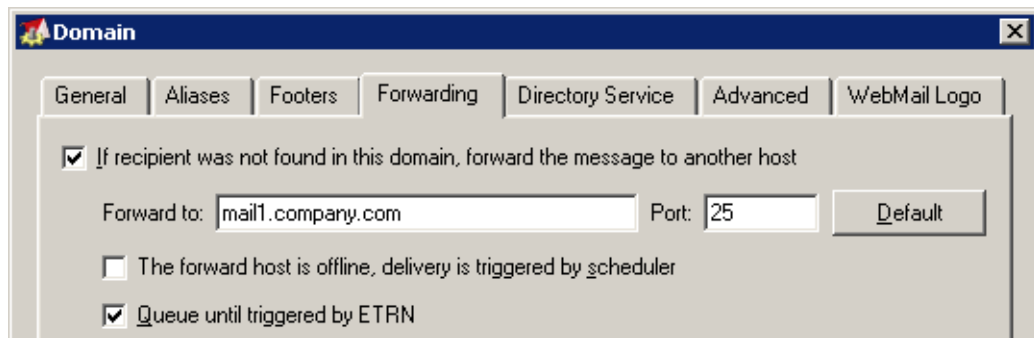


Figure 25.5 Setting up the backup server — the ETRN command

It is also necessary to enable using the ETRN command in the primary mailserver (see chapter 16.5) and schedule sending the ETRN command (see chapter 10).

- Another possibility is setting up the rules for outgoing messages (see chapter 16.2). However, in case of unavailability of the primary server, the server will repeatedly attempt to deliver emails, until the primary server is up and running again, which can occasionally cause overloading of the primary server.

If you prefer this method of setting the secondary SMTP server, we recommend to extend the interval for message resending. This can be set in *Configuration* → *SMTP Server*, on the *Queue Options* tab.

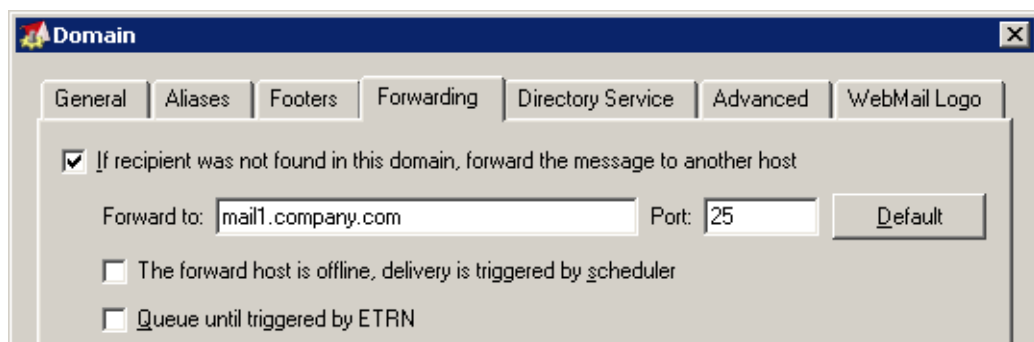


Figure 25.6 Setting up the backup server — mail delivery follows rules for queue of outgoing messages

In the configuration dialog, only name or address of the primary server and port are obligatory entries (see figure 25.6).

- The last method is to set up the scheduler so that it adjusts the intervals for sending emails. This setting is similar to the previous one, because the server again uses the rules for the outgoing message queue. However, in this case, the interval is adjusted by a scheduler, where more convenient schedule can be set.

In the *Configuration* → *Domains* menu, the *Forwarding* tab of the domain *company.com*, you must enable the option *The forward host is offline, delivery is triggered by scheduler*.

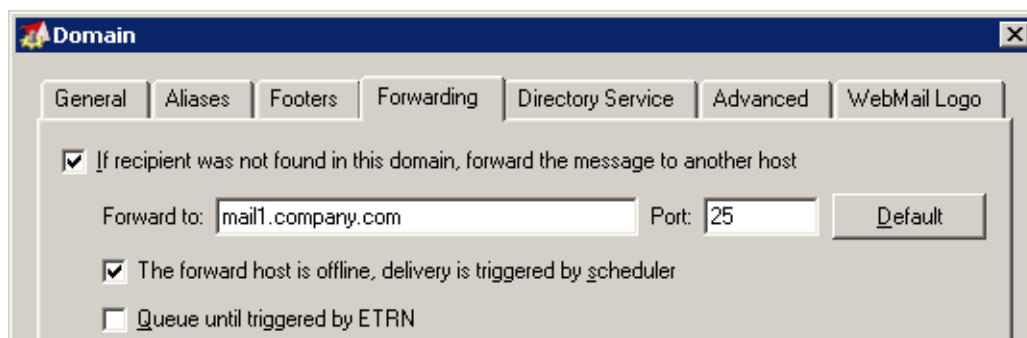


Figure 25.7 Setting up the backup server — mail delivery is controlled by the scheduler

5. If *Kerio MailServer* is used as a primary mailserver, we recommend to add the server address to the list of ignored servers that are not restricted by the settings in the *Configuration* → *SMTP server* menu of the *Security options* tab (for more information, see chapter 16.2).

Troubleshooting in Kerio MailServer

26.1 Reindexing mail folders

Problem description

User's folder or even his/her entire mailbox is not displayed correctly. The damaged folder seems to be empty or some messages are missing.

This problem might be caused by discrepancies between the `index.fld` special file and the `#msgs` directory in a *Kerio MailServer*'s mail folder.

For better understanding, let us explain how *Kerio MailServer* handles messages. Email messages, contacts, events and tasks are saved to a store in a form of folder tree. This store is represented by the `\store` directory which is further divided to domains, user mailboxes and folders included in these mailboxes. Each folder contains several directories and files where email messages as well as information regarding these messages are stored.

We will focus on the `#msgs` directory where messages in the format of `.eml` files are stored and on the `index.fld` special file which is used by *Kerio MailServer* to orientate in the `#msgs` directory while communicating with email clients. This file is created for each mail folder upon the first startup of *Kerio MailServer*.

The `index.fld` file includes list of messages contained in the folder as well as specific information regarding these messages. Each line of the file represents record of one email message stored in the folder. The `#msgs` directory is saved in the same directory as the `index.fld` file.

Under specific conditions (e.g. when checked by a resident module or when *Kerio MailServer* fails), *Kerio MailServer* makes a change in the folder (e.g. it adds/removes a message, it flags a message, etc.). However, it cannot modify the `index.fld` file so that the file and the `#msgs` directory collide (their information on messages in the email folder differ).

Solution

The solution might be easy:

1. Stop the *Kerio MailServer Engine*
2. Delete or rename the damaged `index.fld` file in the corresponding email folder
3. Run the *Kerio MailServer Engine*

Upon the next startup of *Kerio MailServer*, the file is created automatically, in accordance with the status of the folder.

However, this solution is not perfect, because it clears any information regarding the messages saved in the file. This information is called flags — the mail client uses them to find out for example whether the message was not marked as deleted or whether it has been forwarded or not.

Upon starting *Kerio MailServer*, the following record is written in the *Error* log:

```
[23/Jun/2005 12:12:47] mail_folder.cpp: Folder  
~dbeckham@company.com/Contacts has corrupted  
status and index files, going to restore them.  
Some flag information may be lost
```

The following solution is more difficult and it can be used only if the `index.fld` file includes more records than the real number of messages included in the folder (this typically happens when a residential module removes a message upon detecting a virus, but the event is not recorded in the `index.fld` file). However, flags are kept intact. To use this solution, follow these instructions:

1. Stop the *Kerio MailServer Engine*
2. Look up the problematic folder (e.g. INBOX) and the damaged `index.fld` file
3. The `#msgs` directory where messages in the `.eml` format are stored can be found in the same folder
4. Compare the `#msgs` directory with records in the `index.fld` file
5. Look up the redundant record and remove it from the `index.fld` file
6. Save `index.fld` and run the *Kerio MailServer Engine*

26.2 Configuration Backup and Transfer

All *Kerio MailServer* settings are independent of the operating system and are stored in two files placed in the directory where *Kerio MailServer* is installed:

users.cfg and users.cfg.bak

Information about user accounts, groups and aliases. If the file is corrupt and *Kerio MailServer* is unable to read it, it can be replaced by the `users.cfg.bak` backup file. Simply rename the file to `users.cfg`.

mailserver.cfg and mailserver.cfg.bak

All other configuration parameters. If the file is corrupt and *Kerio MailServer* is unable to read it, it can be replaced by the `mailserver.cfg.bak` backup file. Simply rename the file to `mailserver.cfg`.

Information on these two files are saved in the XML format. They can be therefore modified by hand or re-generated by your applications. Backups or transfers of these files can be easily performed by simple copying.

Before configuration transfer, we recommend to also backup the `sslcert` and `license` directories (stored in the directory where *Kerio MailServer* is installed by default). The `license` directory contains the `license.key` file with the *Kerio MailServer* license key. If you forget to make a copy of the backup, you can download the license key from *Kerio Technologies* product web. To download the license key, simply enter the product registration number on the <https://secure.kerio.com/reg> page. However, it is not recommended to use this procedure too often, because the number of license key downloads is limited.

The `sslcert` directory contains an information about a SSL certificate currently in use. If you fail to backup this directory before the configuration transfer, you will not be able to run any of the secured services in the new installation. In such case, call the *Kerio Technologies* customer support (the contact information is listed in chapter 38.1).

Warning: We recommend that *Kerio MailServer Engine* be stopped prior to any manipulation with the configuration files! Information contained within these files is loaded and saved only upon starting or stopping the MailServer. All changes to the configuration performed while the *Engine* is running are only stored in memory. Changes to configuration files performed while the *Engine* is running will be rewritten with the configuration stored in memory after the engine is stopped.

Configuration backup recovery

To use an archived backup configuration of *Kerio MailServer* (typically when transferring the application to another computer or after reinstallation of the operating system), follow these instructions:

1. Install *Kerio MailServer* on the computer (refer to chapter 3.3)
2. Stop the *Kerio MailServer Engine*
3. Copy the archived `mailserver.cfg` and `users.cfg` files (and optionally also the `sslcert` and `license` directories) into the *Kerio MailServer* installation directory.
4. Run the *Kerio MailServer Engine*

Chapter 27

KMS Web Administration

KMS Web Administration is a web interface for administration of local user accounts, groups and aliases. Using this interface, multiple users can administer user accounts, but they cannot access the whole *Kerio MailServer* administration.

KMS Web Administration was developed especially for ISPs and their customers. These customers are able to access their user account, groups and aliases settings in their domains and add, edit or delete them as needed.

Warning: Accounts mapped to *Kerio MailServer* from the LDAP database will be available in *KMS Web Administration* just for reading.

Note: *KMS Web Administration* is available in English version only.

27.1 Web browsers

New versions of all commonly used browsers that support JavaScript and cascading stylesheets (CSS) can be used to access *KMS Web Administration*. The following browsers are supported:

- *Microsoft Internet Explorer* version 5.5 or higher
- *Mozilla* version 1.6 or higher
- *Safari* version 1.1 or higher
- *Firefox* version 0.6.1 or higher

To use the secured access to the *Kerio WebMail* interface (by HTTPS protocol), the browser must support SSL encryption. If it can be configured (e.g. in *Microsoft Internet Explorer*), it is recommend to enable support for SSL 3.0 and TLS 1.0 versions.

Pop-up killers

If any *Pop-up* killer is installed and running, specify an exception for *KMS Web Administration*.

27.2 Setting access rights to the web interface

Special access rights set in *Kerio MailServer* are required to access the *KMS Web Administration*. Users can access *KMS Web Administration* and manage all accounts and groups of the given domain with other than administrator rights.

Warning: Users and groups with full administration rights for *Kerio MailServer* will not be shown in the interface, therefore it will not be possible to edit them through Web Administration.

Users and groups with administrator rights to *Kerio MailServer* will automatically have access to the *KMS Web Administration*. Users and groups with Web Administration rights will also not appear in the

27.3 Settings that enable web administration

To make the administration via the web interface working smoothly, the following settings must be done in the *Kerio Administration Console*:

1. The HTTP service or the HTTPS service (see chapter 7) must be running in *Kerio MailServer*.
2. In the administration console, in the *Configuration → Remote Administration* section, administration via the web interface must be enabled. To keep the server as safe as possible, it is also possible to allow this administration for a specific IP group only (see chapter 13.3).
3. Web administration rights must be assigned to the user. For higher security, it is possible to allow the administration for a certain IP address group only (refer to chapter 13.3). Access rights for web administration must be set for a specific user in the *Configuration → Domain Settings → User Accounts*. In the dialog where the user's parameters are defined, it is necessary to enable the *User can administer aliases, users and groups for their own domain* option on the *Rights* tab (refer to chapter 14.2).

The same right may be assigned also to a user group (*Configuration → Domain Settings → Groups*).

4. *Kerio MailServer* enables limiting of number of users within a domain. Users with administration rights cannot break this limit. The limit can be set under *Configuration → Domains*. In the last configuration window for a domain, it is necessary to enable the *User count limit* option on the *General* tab (see chapter 8.2).

27.4 Users logged in

To access the HTTP service using a web browser, insert the IP address (or the name if it is contained in DNS) of the computer where *Kerio MailServer* is running. A protocol has to be specified in the URL — either HTTP for non-secured access or HTTPS for SSL-encrypted access. The URL can have the following form: `http://192.168.1.1/admin` or `https://mail.company.com/admin`. It is recommended to use the HTTPS protocol for remote access to the service (simple HTTP can be tapped and the user login data can be misused). By default, the *HTTP* and *HTTPS* services use the standard ports (80 and 443). If the standard ports are changed, specify the port number in the URL address, like `http://192.168.1.1:8000/admin` or `https://mail.company.com:8080/admin`. If the URL has been entered correctly, a login page will be displayed in the browser. Enter the username and password on this page (if the user does not belong to the primary domain, a complete email address is required).

The image shows the login page for Kerio MailServer 6 Administration. At the top, the text "KerioMailServer6™ Administration" is displayed in blue and orange. Below this, a message says "Enter your Username and Password below to login to administration:". There are two input fields: "Username:" with the text "jsmith" and "Password:" with masked characters "••••••••". A "Log In" button is located below the password field.

Figure 27.1 Web Administration Login

Log out

It is recommended to log out after finishing work in *Web Administration*. To log out, click the *Logout* button in the upper right corner. After logout, users get disconnected from *Kerio MailServer*, which prevents misuse of such connection.

27.5 Page header

In the *KMS Web Administration* header, name and logo of the company is displayed. Click on the logo to open the *Kerio Technologies* product website.

By default, the *Kerio Technologies* logo is used as the header. However, it is possible to use any other logo or image by changing it in the *Kerio MailServer's* administration console.

In the top right corner of the header, information about the user connected and domain he or she can administer is provided.

27.6 Welcome page

After a successful login to *KMS Web Administration*, the main *Kerio MailServer* administration window is opened. This page is divided into two parts:

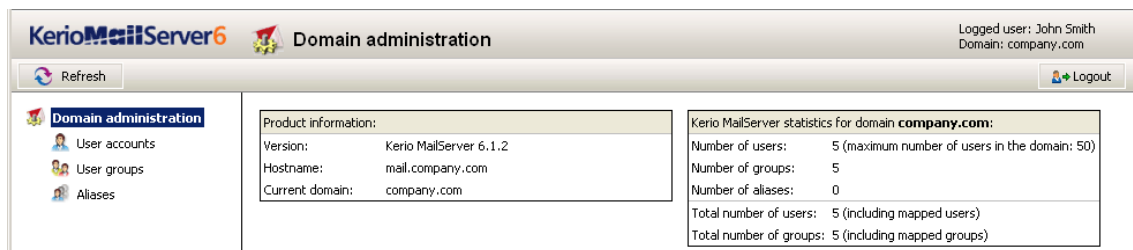


Figure 27.2 Main page

- The left column contains the tree view of sections.
- The right column lists contents of the section previously selected in the left column.

There are two tables in the right column:

Product information

Version

Kerio MailServer version information. To see more detailed information, click the *About* button on the left side of the toolbar.

KMS host name

The name of the computer where the *Kerio MailServer* is running on.

Current domain

The name of the current domain. Administration can be performed only by users with the appropriate rights, who have their user accounts created in the corresponding domain.

User statistics

A number of users, groups and aliases (only the aliases specified directly in the *Aliases* section are considered).

27.7 User accounts

A user account is a username and password used for accessing services on the server. In case of *Kerio MailServer*, one part of the user account is a mailbox. The username and password are used for authentication to this mailbox.

User Account Definition

To create new user accounts, click the *Add user* button in the *User Accounts* section. You can then select from the user account templates, if they are available in *Kerio MailServer*.

The templates in *Kerio MailServer* facilitate creation of user accounts with the same or similar parameters. An example: if the same quota and authentication type is to be specified for all new users, *Kerio MailServer* administrator can create a template that contains these settings. When this template is used, the quota and authentication type will be pre-populated.

Note: The template cannot be created in *KMS Web Administration*. Only the provider with full access rights to *Kerio MailServer* is able to create such templates.

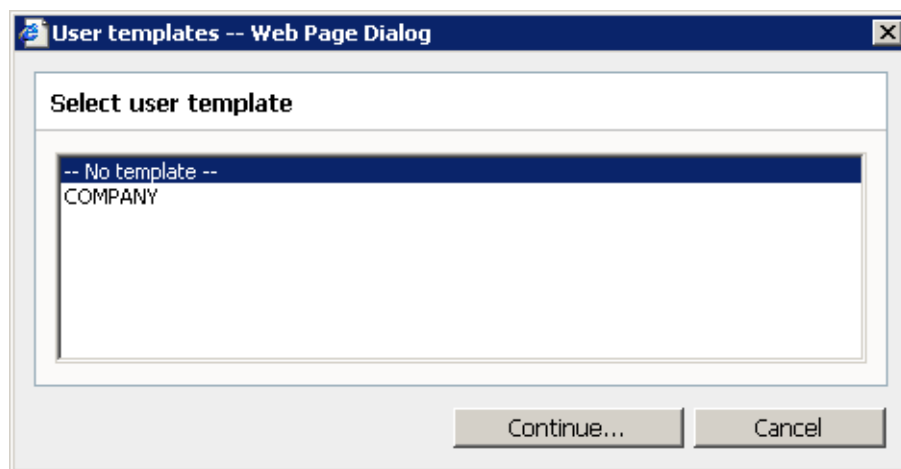


Figure 27.3 Template selection

After the template is selected, a window with the following tabs appears:

General

In the first tab, enter the general user information, e.g. the username and password:

Login name

User login name (note: the domain must be the local primary domain; otherwise enter the full email address, e.g. `user@anothercompany.com`, not only `user`).

The username is not case-sensitive.

The screenshot shows a web-based user administration interface. The title bar reads 'New user | KMS Web Administration | Kerio MailServer 6.1.2 -- Web Page ...'. The 'General' tab is active, with other tabs being 'Mails and Forwarding', 'Groups', and 'Quota and Rights'. The form contains the following fields and options:

- Login name:** Text box containing 'jsmith'.
- Full name:** Text box containing 'John Smith'.
- Description:** Text box containing 'Developer'.
- Authentication type:** Dropdown menu set to 'Internal database'.
- Password:** Text box with masked characters (dots).
- Confirm password:** Text box with masked characters (dots).
- ☐ Account is disabled
- ☒ Enable the default spam rule that moves messages marked as spam to the Junk E-mail folder

At the bottom right are two buttons: 'Add user' and 'Cancel'.

Figure 27.4 User administration — General tab

Full name

A full name of the user (usually first name and surname). This option is required, if the user data from this account are to be exported to a public contacts folder.

Description

User description (e.g. a position in a company). The *Description* entry is for informational purposes only. They can contain any type of information or they can be left blank.

Authentication type

User authentication type. This information can be obtained from your provider.

Password, Confirm password

Only the local user password can be entered or changed. We strongly recommend to change the password immediately after the account is created.

If the password contains special (national) characters, users of some mail clients will not be able to log in to *Kerio MailServer*. It is therefore recommend to use only ASCII characters for passwords.

Account is disabled

Temporary blocking of the account so that you do not have to remove it.

Enable a default spam rule

Check this option to create a sieve rule upon setting up a user account. All incoming emails marked as spam will be automatically moved to the *Junk mail* folder. The rule can be set up only during the process of user account creation.

Email addresses and Forwarding settings

List of additional mail addresses

Multiple email addresses can be added to the list for a user mailbox. The primary user address (cannot be deleted) consists of the the username and domain where the account is located. The other addresses are called aliases. They can be specified either directly in the user definition or in the *Aliases* section. The first option is recommended, because it is easier and more comprehensible. Aliases and their use are described in more detail in chapter 27.9.

Forwarding settings

The *Emails and forwarding* tab enables forwarding to other email addresses. Click *Add* to add an address to which messages from this folder will be forwarded.

If the *Deliver messages to both mailbox and forwarding addresses* option is enabled, the message will be both stored in the local mailbox and forwarded to the addresses specified (otherwise it will be only forwarded, but not stored in the local mailbox).

Adding users into groups

Use the *Add* or *Remove selected* button to select the group where to add the user. First, create the desired group in *Domain settings*→ *Groups* section (see chapter 27.8). You can use the same procedure to add new users to the groups, therefore it does not matter if users or groups are created first.

Other settings

You can specify restrictions for individual mailboxes:

Quota

The user quota prevents cluttering of the server disk. If either of the limits is reached, any new messages will be refused by the server.

If the quota is exceeded, the user will be notified by email and advised to delete some of the messages in the mailbox.

Disk space

The maximum space for a mailbox. For greater ease in entering values you can choose between kilobytes (*KB*), megabytes (*MB*) or gigabytes (*GB*).

New user | KMS Web Administration | Kerio MailServer 6.1.0 beta 5 -- We...

General **Emails and forwarding** Groups Quota and settings

List of additional email addresses:

smith@company.com
john.smith@company.com

Add ...
Edit ...
Remove

Forwarding settings:

☐ No forwarding
☒ Forward to addresses

john@smith.info

Add ...
Edit ...
Remove

☒ Deliver messages to both mailbox and forwarding addresses

Add user Cancel

Figure 27.5 User administration — Email and forwarding tab

Number of messages

The maximum number of messages in the mailbox. Messages that exceed this number will be refused by the mailserver.

The value of either of these items can be set to 0 (zero), which means that there is no limit set for the mailbox.

*Restrictions and settings***This user can send/receive email from ...**

Using this option, the administrator of *Kerio MailServer* can limit communication only to the local domain. This can be useful for internal communication settings in many companies. Users will not be able to send or receive emails to/from any other domain.

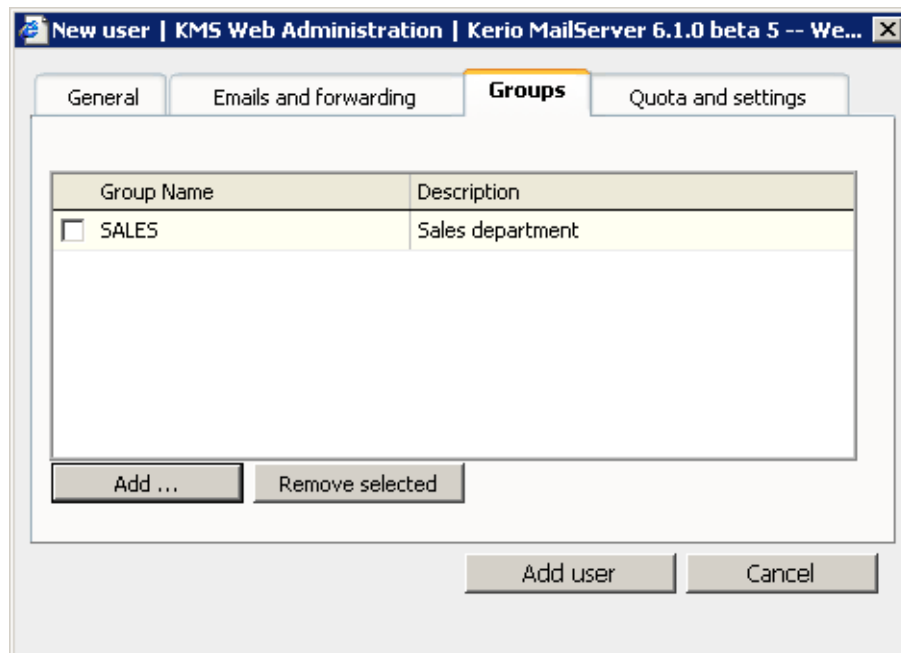


Figure 27.6 User administration — Groups tab

Max. size of outgoing message for this user

Use this option to set the size limit for outgoing messages. By setting the size limit, you can prevent the internet connection from being overloaded by emails with large attachments.

If the limit is set to 0, *Kerio MailServer* behaves the same way as if no limit was set.

Warning: The message size limit can be set by your provider in *Kerio MailServer* for a whole domain. After both limits are set, the following can occur:

1. If the message size limit for a user is higher than the one for the domain, the domain limit will apply.
2. If the message size limit for a user is lower than the one for the domain, the user limit will apply.

New user | KMS Web Administration | Kerio MailServer 6.1.2 -- Web Page ...

General | Mails and Forwarding | Groups | **Quota and Rights**

Quota

Disc space:

Number of messages:

Restrictions and settings

☐ This user can send/receive mail from his/her own domain only

☒ Max size of outgoing messages for this user:

Note: 0 or an empty means unlimited, number overrides default domain setting.

☒ Publish this user information at the public folder

Note: User cannot be published unless the 'Full name' item is specified

Webadmin administration rights and Public folders rights

☒ This user can administer non-admin users/groups and aliases in his/her own domain

☒ This user has the administrator rights to the public folders

Figure 27.7 User administration — Quota and Settings tab

Publish this user information at the public folder

Check this option to add the user contact to the public contacts folder. The contact will be added to the public folder only if the *Full name* field is populated (in the first or second step of the wizard).

Webadmin administration rights

This user can administer non-admin users/groups

A special access right to *Kerio MailServer Web Administration*. This setting is independent on the access rights settings for *Kerio Administration Console*.

This user has the administrator rights to the public folders

A special privilege for management of public folders.

User account editing

To change the user account settings, use the same dialog as for creating an account. Click either the username in the user list or *Edit user* in the *Action* column.

<input type="checkbox"/> Login Name	Full Name	Description	Action
<input type="checkbox"/> dpeterson	Diane Peterson	Sales dept.	 
 jsmith	John Smith	Developer	 
<input type="checkbox"/> jwayne	John Wayne	CEO	 
Number of records: 20			1

Figure 27.8 User account editing

Removing an account

Click the *Remove button* to delete a user account. With the original user account in *Kerio MailServer*, many actions can be performed. Once an account is selected and the *Remove* button is clicked, one of the following actions can be selected. In the dialog box you can set the account to be removed or moved to another user or simply to be kept in the store directory.

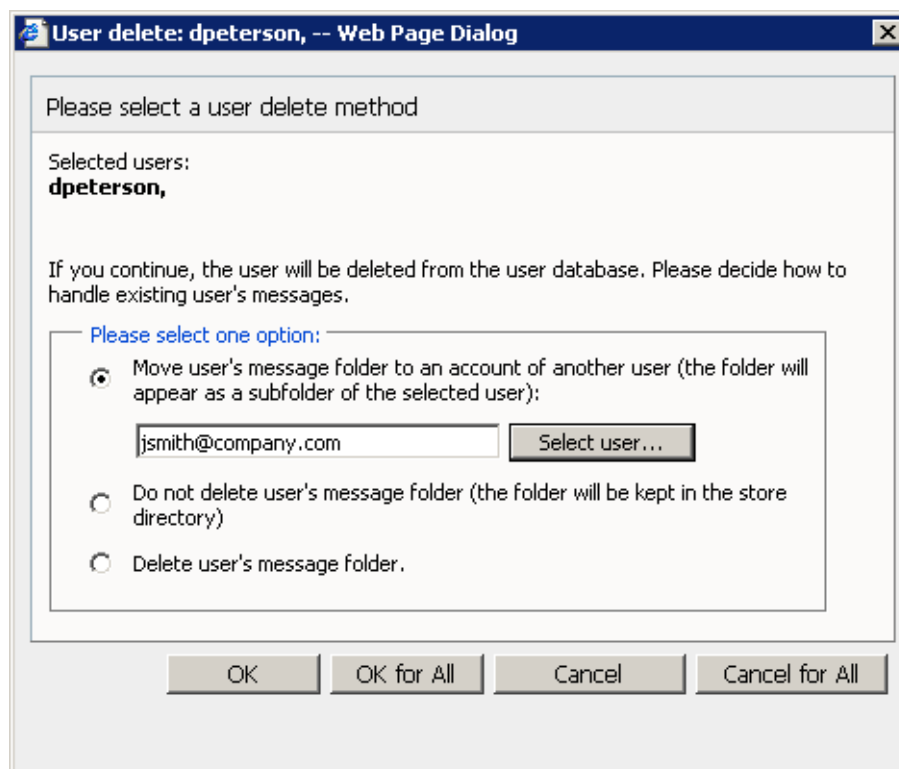


Figure 27.9 Remove user dialog

Move user's message folder ...

This option is useful especially when another user needs to work with messages, events and tasks from this folder.

The entire folder will be moved as a subfolder of the selected account's root folder. The folder name will follow this pattern: *Deleted mailbox — user_name@domain*. This folder will include all original folders of the deleted mailbox.

Note: If any problem arises during moving of the a user account, details are recorder in the *Warning* log (see chapter 23.5).

Do not delete user's message folder ...

The folder will be kept in the store directory.

Delete user's message folder

This option can be used when the user folder does not contain any (or any important) messages, events, tasks, etc.

Searching users

The toolbar provides a search entry which can be helpful especially if the domain includes too many users. Any item (*Login Name*, *Full Name* and *Description*) can be used as the searching criteria, the searching engine looks the specified string up in all of them.

In addition, users can be listed by various criteria, by clicking particular column titles.

Users mapped from the directory service

If users in this domain are mapped from the active directory, they can be viewed also in the *Kerio Web Administration*. However, the data of such accounts cannot be edited. There is the *Show only users from internal database (hide mapped users)* option available that can be used to hide mapped users.

27.8 User groups

User accounts within each domain can be sorted into groups. The main reasons for creating user groups are as followed:

- Group addresses can be created for certain groups of users with aliases (see chapter 27.9) — mail sent to this address will be delivered to all members of the group.
- Specific access rights can be assigned to a group of users. These rights complement rights of individual users.

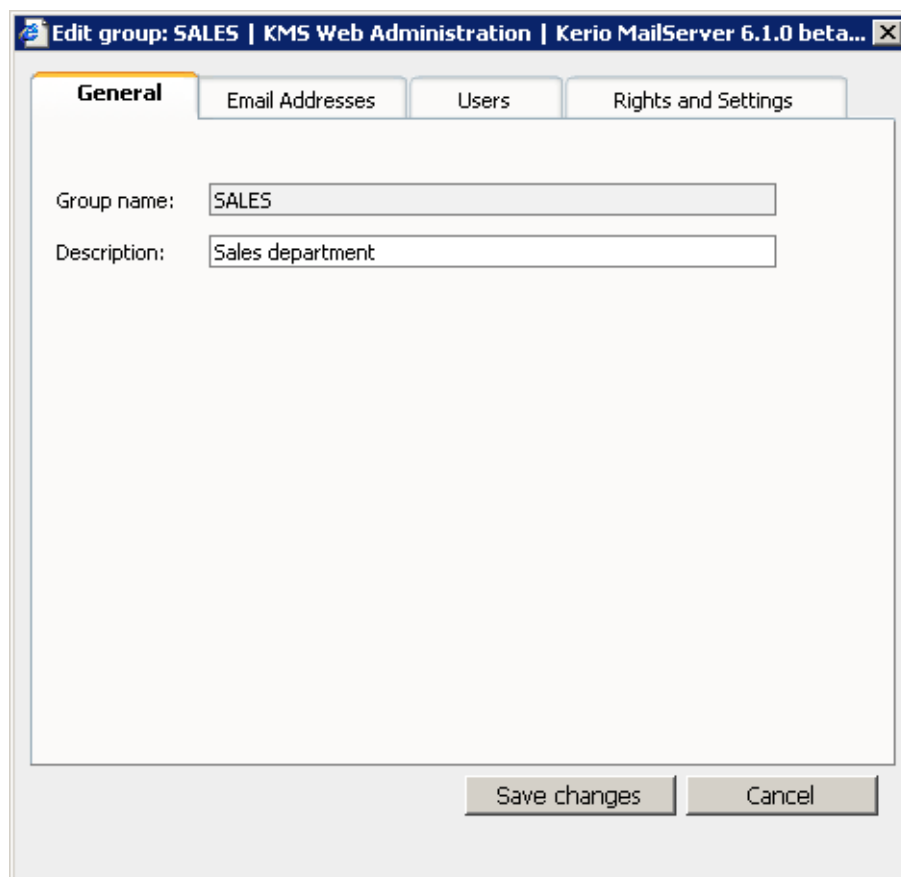
You can define user groups in the *User Groups* section.

Group Definition

Create a new group by clicking on the *Add Group* button in the *User Groups* section. A guide with multiple tabs will be opened.

General

Enter the group name and description in the *General* tab:



The screenshot shows a web-based dialog box titled "Edit group: SALES | KMS Web Administration | Kerio MailServer 6.1.0 beta...". It features four tabs: "General", "Email Addresses", "Users", and "Rights and Settings". The "General" tab is selected and active. Inside this tab, there are two text input fields: "Group name:" with the value "SALES" and "Description:" with the value "Sales department". At the bottom right of the dialog, there are two buttons: "Save changes" and "Cancel".

Figure 27.10 Group management — the General tab

Name

Unique name of the group.

Description

Description of the group; may be left blank.

Group addresses

This step defines all desired email accounts (aliases) of the group. There might be no address assigned to the group (unlike user accounts, the group address is not created automatically from the group name and domain where the group is defined).

An example of group addresses use:

There are three salesmen in a company. They have an account in *Kerio MailServer*. Each of the three salesmen wants to receive all incoming email orders from the clients.

Solution: Create a group named SALES and in the *Mail Addresses* tab, define sales@company.com and info@company.com (see picture 27.11). Assign these addresses to the three salesmen in the *Users* tab (see picture 27.12).

After the group is created, all emails sent to sales@company.com or info@company.com will be delivered to the three salesmen.

There might be no address assigned to the group (unlike user accounts, the group address is not created automatically from the group name and domain where the group is defined).

The group addresses can be added either directly during the group definition or in the *Aliases* section. The first method is recommended — it is easier.

Adding users to the group

Click the *Add* or *Remove selected* buttons to add or remove users to/from this group. If no user accounts are created, the group may be left blank and the users can be added during the process of account definition (see chapter 27.7).

Rights and restrictions settings

Members of this group can send/receive ...

Using this option, the administrator of *Kerio MailServer* can limit communication only to the local domain. This can be useful for internal communication settings in many companies. Users will not be able to send or receive emails to/from any other domain.

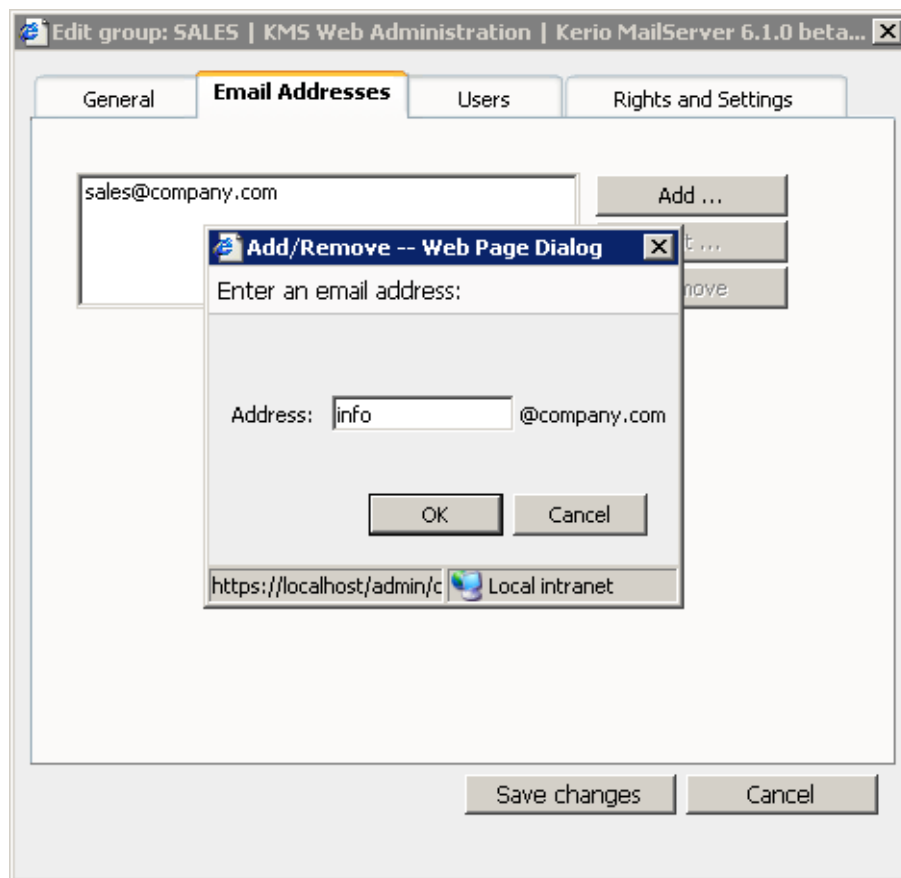


Figure 27.11 Group management — Mail Addresses tab

Publish this group information at the public folder

If this option is enabled, name and email address of the group will be added to the public contacts folder. The group cannot be added to the public folder unless at least one email address has been specified on the second tab.

This user can administer non-admin users/groups ...

A special access right to *Kerio MailServer Web Administration*. This setting is independent on the access rights settings for *Kerio Administration Console*.

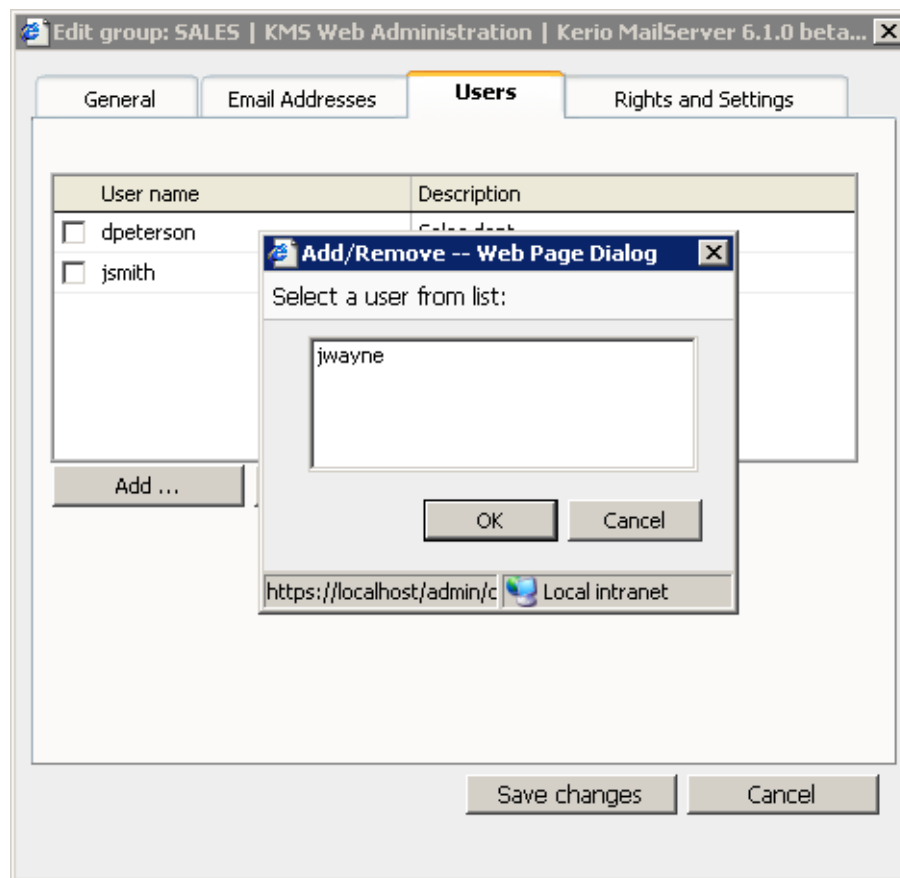


Figure 27.12 Group management — Users tab

Edit group

Parameters can be changed in the same dialog which is used for group creating. Open it and click either on a group name or on the *Edit group* icon in the *Action* column.

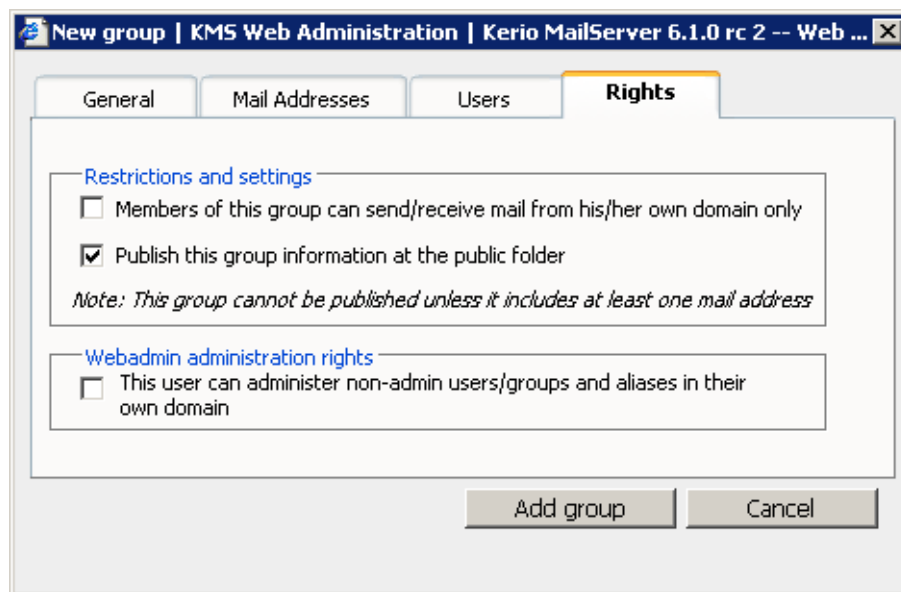


Figure 27.13 Group management — Rights and Settings tab

Remove group

The *Remove Groups* button provided on the toolbar can be clicked to remove any groups selected by checkboxes in the group list.

Search groups

The toolbar provides a search entry which can be helpful especially if the domain includes too many groups. Any item (*Group Name* and *Description*) can be used as the searching criteria, the searching engine looks the specified string up in both of them.

In addition, groups can be listed by various criteria, by clicking particular column titles.

Groups mapped from the directory service

If this domain includes groups mapped from the active directory, they can be viewed also in the *Kerio Web Administration*. However, the data of such groups cannot be edited. There is the *Show only groups from internal database (hide mapped groups)* option available that can be used to hide mapped groups.

27.9 Aliases

An alias is an alternative user name or email address. Each alias can be associated with one or multiple users, depending on its purpose.

For each alias, it is necessary to specify the target address for receiving emails. Emails sent to the aliases can be delivered to one or more user mailboxes at once (a group or a public email folder).

<input type="checkbox"/> Alias Name ▾	Deliver To	Description	Action
<input type="checkbox"/> programmer	programmer@us.company.com	Develop department	 
<input type="checkbox"/> sales	jsmith@company.com	Sales department group address	 
Number of records: 20 ▾			1

Figure 27.14 Aliases

The following examples illustrate the use of aliases:

1. A company needs to use email to communicate internal information to employees. For this purpose, a public mail folder can be created in *Kerio WebMail* and the messages can be sent using an alias.

All messages sent to `info@company.com` will be stored in the *Info* public folder. The alias is defined as follows:

`info → #public@company.com/Info`

2. Messages sent to invalid addresses (i.e. addresses where the part before the @ sign has no corresponding user account nor alias) can be delivered to a selected user or group of users (see figure 27.15). Use the following alias to achieve this:

`* → Admins`

If this (or the next) alias is not defined, *Kerio MailServer* returns such messages to their senders as undeliverable.

3. The * symbol is used as a substitution of any number of characters in an alias (e.g.: `*sms*`, `a*00*`, etc.). The alias will be applied to all email addresses that conform to this mask.
4. To replace just one symbol or character in an alias (usually used in case that users have problems to remember corresponding email address), use the ? symbol. (for example, `?ime` stands for `time`, `dime`, etc.).

Note: Aliases can be used also for assigning another email address to a user or a group, or forwarding messages for a user or a group to other addresses. However, it is recommended to specify these settings directly during the process of user definition (see chapter 27.7), or group definition (see chapter 27.8).

Aliases management

To define aliases, use the *Aliases* section.

Click the *Add Alias* button to display a dialog where a new alias can be created.

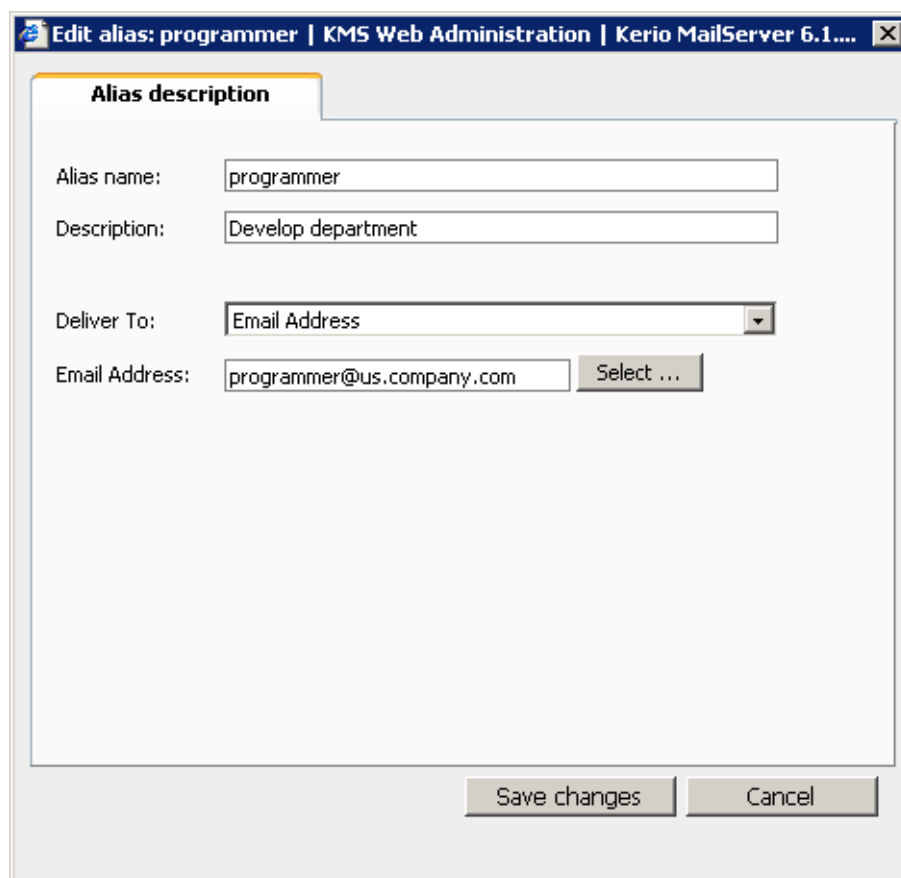


Figure 27.15 Alias creation dialog

Alias name

A virtual address (e.g. sales or john.wayne).

The aliases always apply to a specific domain. You can enter only the local address part into the alias header (i.e. the part before the @ symbol).

Description

Text description of the alias. May be left blank.

Deliver to

The address for receiving emails sent to the alias. Select the place where the messages will be stored:

- *Mail address* — any (user or group) email address. Click *Select* to select a user or a group from the list.
- *Public folder* — public folder name in the following format: #public/Folder.

Click *Remove Aliases* to remove any alias selected by the corresponding checkbox in the list of aliases.

The toolbar provides a search entry which can be helpful especially if the domain includes too many aliases. Any item (*Alias name*, *Deliver to* and *Description*) can be used as the searching criteria, the searching engine looks the specified string up in all of them.

Chapter 28

Kerio Active Directory Extensions

Active Directory Extensions is an extension to the *Active Directory* service (under Windows 2000 and newer versions) with items that include specific information for *Kerio MailServer*. By installation of the extension you can integrate part of *Kerio MailServer* into *Active Directory*. This will simplify actions related to user administration.

Kerio Active Directory Extensions provides the following benefits:

Easy account administration

As of version 5.5, *Kerio MailServer* can (apart from its internal user account database) use also accounts and groups saved in the LDAP database (in *Microsoft Active Directory*). Using LDAP, user accounts can be managed from one location. This reduces possible errors and simplifies administration.

Online cooperation of *Kerio MailServer* with *Microsoft Active Directory*

Additions, modifications or removals of user accounts/groups in the *Microsoft Active Directory* database are applied to *Kerio MailServer* immediately.

Example: A company uses the *Windows 2000* domain and *Kerio MailServer*. A new employee was introduced to the company. This is what has been done until now:

1. A new account has been created in *Active Directory*.
2. The user has been imported to *Kerio MailServer* (or an account using the same name has been created and this name was verified by the Kerberos system).

If you use LDAP database only the first step must be taken. If *Kerio Active Directory Extensions* is deployed, the dialog where new user accounts can be created is extended with a tab where specific information for *Kerio MailServer* can be entered (email addresses, forwarding, quota, etc.).

The account is created only in the *Active Directory* database. *Kerio MailServer* and *Microsoft Active Directory* cooperate online. Accounts in *Kerio MailServer* are created automatically.

Warning:

- Accounts created in *Kerio Administration Console* will be created only locally — such accounts will not be copied into the *Active Directory* database.

- If the *Active Directory* server is not available it will not be possible to access *Kerio MailServer*. It is therefore recommended to create at least one local account with read/write permissions.
- When creating a user account, ASCII must be used to specify username. If the username includes special characters or symbols, it might happen that the user cannot log in.

28.1 Installation of Active Directory Extensions

Use the wizard to install *Active Directory Extensions*. After you confirm the licensing policy, select a destination directory. In the next step a window showing the installation process will be displayed. At the left bottom corner you will find buttons that can be used either to view the installation log (the *View Log* button) or to save the log to file (the *Save Log to File* button).

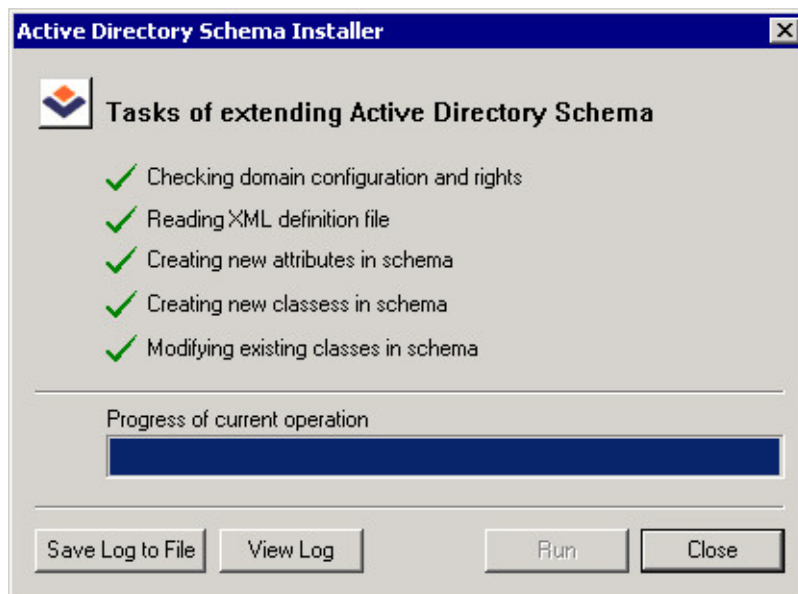


Figure 28.1 Installation process

Notes:

1. According to the version of *Microsoft Internet Explorer* that you use, installation of the *Microsoft XML Parser* component may be required. If the installation is required you must install *Microsoft XML Parser* first, otherwise the *Kerio Active Directory Extensions* installation cannot be finished.
2. Only the English version of *Kerio Active Directory Extensions* is available.

System requirements

Active Directory Extensions in *Windows 2000 Server* supports both *Active Directory NT compatible* and *2000 native* types. In *Windows 2003*, *Active Directory 2000 native* and *Active Directory 2003* are supported.

28.2 Active Directory

Active Directory is a service that stores information about objects (users, groups, hosts, etc.) in *Microsoft Networks*. Applications that support *Active Directory* use the service to learn about parameters and rights of the objects. *Active Directory* is based on a structured database.

Users and groups in the domain are connected to the LDAP *Active Directory* database. LDAP provides some outstanding benefits such as the fact that user accounts are managed from one single point, which eases the administration and reduces possible errors (refer to chapter 8.6). To add users and groups, use *MMC (Microsoft Management Console)*. New users or groups added to the domain connected to *Active Directory* with *Kerio Administration Console* will be stored into the local database of *Kerio MailServer* only.

Run *MMC* from the menu *Start → Settings → Control Panel → Administrative tools → Active Directory Users And Computers*.

28.3 User Account Definition

In *Active Directory Users And Computers* select the *Users* section. Choose the *New → User* option to run the wizard for creating a new account.

Warning: When creating a user account, ASCII must be used to specify username. If the username includes special characters or symbols, it might happen that the user cannot log in.

The standard version of the wizard is extended with a folder that will be used to create a new account within *Kerio MailServer*.

Now, tick the *Create a Kerio MailServer mailbox* option to create in the database all items that *Kerio MailServer* will need to work with. Define the basic email address of a user with the *Alias* item (the user login name defined during the first step of the wizard will be used automatically).

Other account parameters may be defined in *Properties*. Click on the new user account with the right mouse button and select *Properties* in the context menu. Open the *Kerio MailServer Account* folder. This folder provides the following options:

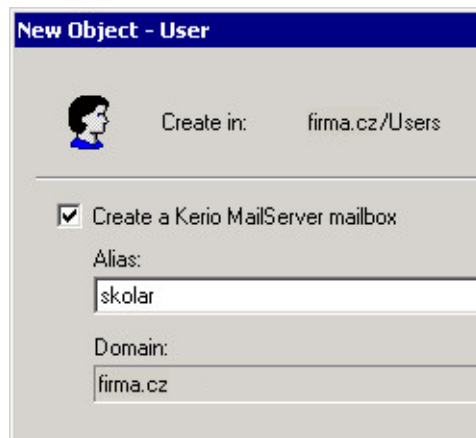


Figure 28.2 User account definition



Figure 28.3 Kerio MailServer Account tab

Mail Account Enabled

Activating this option you will allow the email account to be available in *Kerio MailServer*. If the option is off, the user account will be ignored by *Kerio MailServer*.

E-mail Addresses

Definition of email addresses (aliases) for a particular user. Under the default settings, each user has an email address created from the username and the name of the domain where the account has been defined.

Forwarding

Here, forwarding of mail to the desired email address may be defined. The *Forward to:* option can be used to forward mail addressed to the user to all addresses defined in this entry.

The *Deliver messages to both* option can be used to forward the mail and to store it into the local mailbox (copies of the messages will be sent to defined addresses).

Mailbox Limits

Mailbox limitations according to the *Storage size* and *Number of messages* may be defined. Each limit option may be switched off by the *Do not limit...* option, thus the limitation will be ignored within the mailbox.

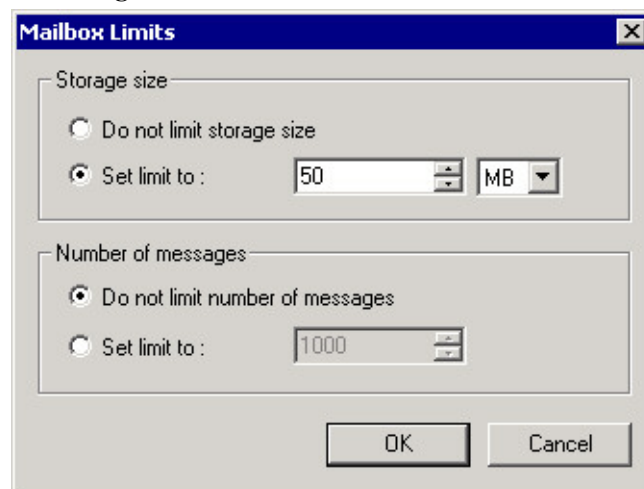


Figure 28.4 Mailbox Limits

WAP Settings

Kerio MailServer enables access to email using a cellular telephone from the WAP protocol. This service can be enabled/disabled by the *Enable/Disable Access to WAP service* option and by entering a PIN code (including from 4 to 32 characters). This code will be used for authentication to the service.

Administration Rights

Definition of *Kerio MailServer* administration rights. The menu provides the following options to select from:

- *No access to administration* — user is not allowed to access the *Kerio MailServer* administration. This option is used by default. We recommend creating a local account for the *Kerio MailServer* administration (see chapter 14.2). In case the Active Directory server is not accessible, administration of KMS will still be possible if the account is managed internally to KMS.
- *Read only access to administration* — user is allowed to access the administration only to read it. User can connect to the server with *Kerio Administration Console* and view the settings, however, he/she is not allowed to edit the administration.
- *Read/write access to administration* — full access to the administration. User is allowed to read and write in the administration. As few users as possible should be granted these rights for security reasons.

28.4 Group Definition

Within *Kerio Active Directory Extensions*, group definition is almost identical to user account definition; however, the wizard for creating new groups is extended by one step. This step enables the administrator to define a primary email address that will be used by the group.

The *Kerio MailServer Account* bookmark allows the administrator to define email addresses of the group (the *E-Mail Addresses* button) as well as access rights to *Kerio MailServer* administration (the *Administration Rights* button).

For detailed information, see chapter 28.3.

Chapter 29

Kerio Open Directory Extensions

Kerio Open Directory Extensions is an extension to *Apple Open Directory* service that allows mapping of the accounts to *Kerio MailServer* (*Kerio MailServer* items are added to the LDAP database scheme). When user accounts are created, edited or deleted in *Apple Open Directory* database, the changes are also made in *Kerio MailServer*.

Warning:

- If an account is created in *Kerio Administration Console*, it will be created only locally, it will not be copied into *Open Directory* database.
- *Warning 2:* If *Open Directory* server is unavailable, logging in to *Kerio MailServer* will be impossible. It is therefore recommended to create at least one local account with read/write permissions.
- When creating a user account in *Apple Open Directory*, ASCII must be used to specify username. If the username includes special characters or symbols, it might happen that the user cannot log in.

29.1 Kerio Open Directory Extensions installation

The installation package with *Kerio Open Directory Extensions* can be downloaded from product web pages of *Kerio Technologies*.

A standard wizard is used for installation of *Kerio Open Directory Extensions*.

When using configurations of Mac OS X servers of *Master/Replica* type, *Kerio Open Directory Extensions* must be installed to the *master* server, as well as to all *replica* servers, otherwise the account mapping will not work.

System requirements

Kerio Open Directory Extensions since version 6.1 can be installed to *Mac OS X 10.3 (Panther)* and later versions.

29.2 Apple Open Directory

Apple Open Directory is a directory service shipped with *Mac OS X Server* systems. This directory service is an equivalent to *Active Directory* created by *Microsoft*. As in *Active Directory*, it allows to store object information in a network (about users, groups, workstations, etc.), authenticate users, etc.

The information about users and groups in *Apple Open Directory* are stored in *Open LDAP* database. When mapping accounts to *Kerio MailServer*, all user accounts are stored in one place and it is not necessary to import and administer them in both *Apple Open Directory* and *Kerio MailServer*. Only definitions of mailbox-specific configurations have to be done in *Kerio MailServer* (see chapter 14).

Warning: When creating a user account in *Apple Open Directory*, ASCII must be used to specify username. If the username includes special characters or symbols, it might happen that the user cannot log in.

29.3 User accounts mapping in Kerio MailServer

In *Mac OS X Server*, no other settings than *Kerio Open Directory Extensions* installation are usually necessary. It is only necessary to save usernames in ASCII. If the username includes special characters or symbols, it might happen that the user cannot log in.

In *Kerio MailServer* the following settings must be specified:

1. User accounts mapping from *Apple Open Directory* must be enabled and defined in domain settings (for more information, see chapter 8.6).
2. User authentication via *Kerberos* must be set in domain settings (for more information, see chapter 8.7).
3. User authentication via *Kerberos* must be set in user settings (for more information, see chapter 14.2).

29.4 Authentication using the apple.map configuration file

When mapping accounts from the *Open Directory*, it is also possible to set type of user authentication to *Kerio MailServer*. In *Open Directory*, it is possible to authenticate users against the password server or the *Kerberos* server (for details, see chapter 30).

The first method (authentication against the password server provides the following benefit. It is not necessary to perform any special settings at the server where *Kerio MailServer* is installed. However, there are also certain disadvantages:

- The authentication is obsolete and it is not reliable enough.
- Users are not allowed to change their user passwords on their own (in the *Kerio WebMail* interface).
- The *Apple* company successively closes support for this authentication method.
- This authentication method is enabled only if *Kerio MailServer* is installed on Mac OS X.

Still, authentication against the Kerberos server is more modern and secure. On the other hand, this authentication method requires additional settings at the server where *Kerio MailServer* is installed. For detailed information on these settings, see chapter 30.

Up to 6.1.2, *Kerio MailServer* used authentication against the password server by default. Since *Kerio MailServer 6.1.3*, the Kerberos authentication method is set as default.

In *Kerio MailServer*, authentication against *Open Directory* is saved in a special file, *apple.map*, used for mapping of users.

If it is necessary or helpful to use the password server authentication method in *Kerio MailServer 6.1.3* and higher, the configuration file for mapping from *Open Directory* must be edited manually, as follows:

1. Use *Kerio MailServer Monitor* or the command prompt line to stop *Kerio MailServer* — *Kerio MailServer Engine* must be stopped before any manual changes taken in configuration files.
2. Open the `/usr/local/kerio/mailserver/ldapmap/apple.map` file. The *apple.map* file is used for mapping of the LDAP database in the *Apple Open Directory*. Besides other information, the file includes setting of authentication method applied as default to users mapped from the *Apple Open Directory* database.
3. Use the search option to find the line including the `Auth_type` variable. Change the value using the following instructions:
 - 4 — for authentication against the password server, use the `Auth_type 4` value
 - 3 — for authentication against the Kerberos server, use the `Auth_type 3` value

4. Save the change and start *Kerio MailServer*.

The instructions provided can be also applied to switch to the Kerberos server authentication method while *Kerio MailServer 6.1.2* or earlier is used.

Chapter 30

Kerberos Authentication

This chapter provides simple and well-organized guidelines to configuration of user authentication at Kerberos.

Kerberos is a client-to-server system which enables authentication and authorization of users to increase security while using network resources. Kerberos is described by IETF RFC 1510.

Kerio MailServer includes support for Kerberos V5.

Note: Pi eení p padn ch probl m s konfigurac  v m mohou pomoci n sleduj c  z znamy:

- *MS Windows* — logs are located in the *Start → Settings → Control Panel → Administrative Tools → Event Viewer* menu
- *Linux* — logs can be found in the default directory `/var/log/syslog`

However, this applies only to the Kerberos client. Logging of traffic at the server's side can be performed by adding the following configuration into the `/etc/krb5.conf` file:

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
```

Note: These settings applies to Kerberos MIT. Different configuration must be used for Kerberos Heimdal.

- *Mac OS X Server* — logs in the *Server Admin* application (see chapter [30.4](#))
- *Kerio MailServer* — logs can be found in the *Logs* section of the administration console. In this case, the *Warning*, *Error* and *Debug* logs are to be considered (*Authentication modules* must be running). For detailed description on individual logs, refer to chapter [23](#).

30.1 Kerio MailServer on Windows

Authentication against Active Directory

For authentication at the *Active Directory*, it is necessary to specify the *Active Directory*'s domain name in *Kerio MailServer*. This can be set under domain settings in the *Kerio Administration Console* (see figure 30.1).

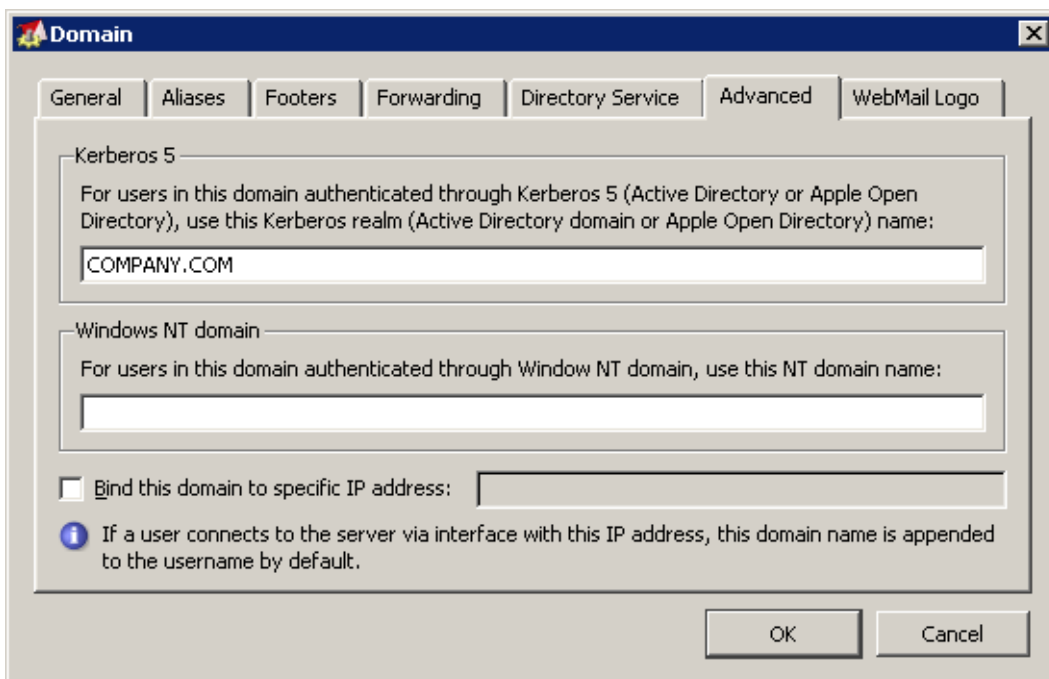


Figure 30.1 Setting the Active Directory domain in Kerio MailServer

Specify the domain name in the *Advanced* dialog (see figure 30.1) and ensure that:

1. *Kerio MailServer* is a member of the domain to be authenticated against. If *Kerio MailServer* is not the domain member, the Kerberos system will not be working and the users will have to use a local password, i.e. different from the password for the domain.
2. *Kerio MailServer* uses *Active Directory Controller* as the primary DNS server — this should be done automatically by adding the host in the domain (see item 1).

If the network configuration requires authentication against multiple domain controllers at a time, add all domain controllers where *Kerio MailServer* will be authenticated as DNS servers.

3. time of *Kerio MailServer* and *Active Directory* (including the time zone) is synchronized — this should be done automatically by adding a host to the domain (see item 1).

Authentication against Open Directory

For authentication at the *Open Directory*, *Kerio MailServer's* Kerberos realm must be specified (e.g. COMPANY.COM).

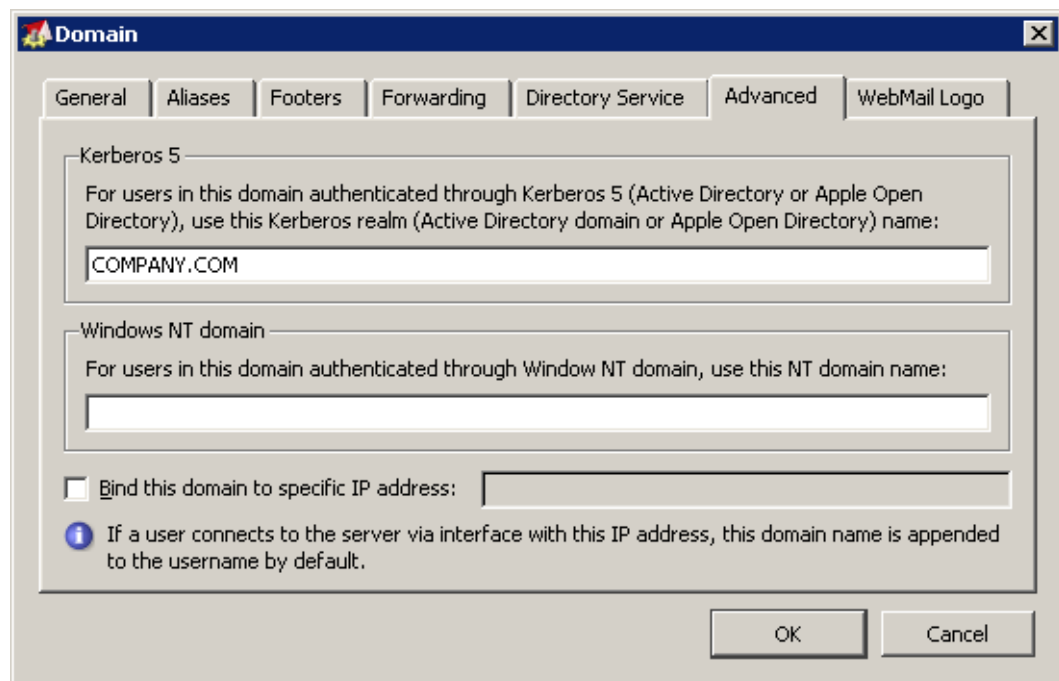


Figure 30.2 Specification of Kerberos realm in Kerio MailServer

Specify the *Open Directory* domain name (Kerberos realm) in *Kerio MailServer* and ensure that:

1. *Kerio MailServer* is a member of the domain to be authenticated against. If *Kerio MailServer* is not the domain member, the Kerberos system will not be working and the users will have to use a local password, i.e. different from the password for the domain.
2. DNS server (IP address or DNS name of the computer where *Apple Open Directory* is running) is set correctly at the computer with *Kerio MailServer*.
3. time of *Kerio MailServer* and *Open Directory* (including the time zone) is synchronized — this should be done automatically by adding a host to the domain (see item 1).

Authentication against a stand-alone Kerberos server

To use authentication against a stand-alone Kerberos server (*Key Distribution Center*), it is necessary to maintain the username and password database both in *Key Distribution Center* and in *Kerio MailServer*.

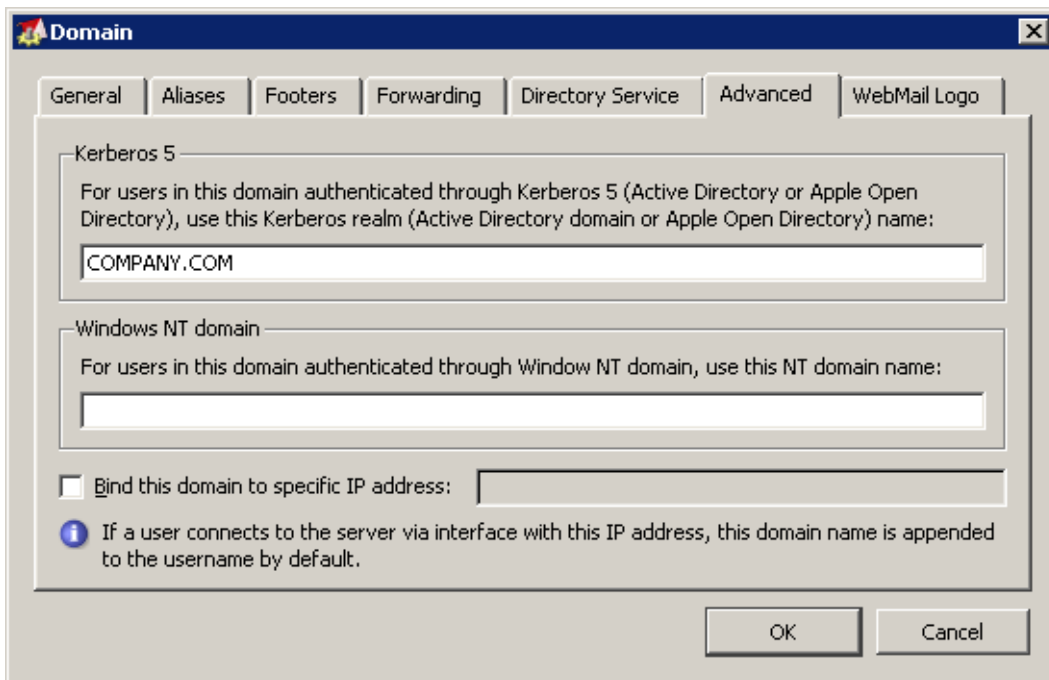


Figure 30.3 Specification of Kerberos realm in Kerio MailServer

Specify the Kerberos area (Kerberos realm) name in *Kerio MailServer* and ensure that:

1. *Kerio MailServer* is a member of the Kerberos area to be authenticated against:
 - the Kerberos client must be installed on the computer,
 - username and password used for authentication at the system must be defined at the *Key Distribution Center*.
2. DNS server must be set correctly at *Kerio MailServer's* host (*Key Distribution Center* uses DNS queries).
3. Time of *Kerio MailServerem* and *Key Distribution Center* (all hosts included in the Kerberos area) must be synchronized (including time zone).

Note: Before starting the Kerberos server, check out whether SPN (Service Principal Name) functions correctly.

When the previous steps are followed successfully, set authentication in *Kerio MailServer* on the *Advanced* tab under *Configuration* → *Domains*, (see chapter 8.7).

30.2 Kerio MailServer on Linux

Authentication against Active Directory

Before setting Kerberos user authentication at Linux, it is recommended to check that authentication against the domain functions correctly (check this by logging in the system using an account defined in the *Active Directory*). If *Kerio MailServer* is not the domain member, the Kerberos system will not be working and the users will have to use a local password, i.e. different from the password for the domain.

It is also necessary to ensure the following:

1. *Kerio MailServer's* host uses the domain controller of the *Active Directory* domain as the primary DNS server.

If the network configuration requires authentication against multiple domain controllers at a time, add all domain controllers where *Kerio MailServer* will be authenticated as DNS servers.

2. Time of the *Kerio MailServer* host and the *Active Directory* must be synchronized (including time zone).

For proper authentication, define the `/etc/krb5.conf` file.

An example of the `krb5.conf` file:

```
[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    ticket_lifetime = 24000
    default_realm = COMPANY.COM
    dns_lookup_realm = false
    dns_lookup_kdc = yes

[realms]
    COMPANY.CZ = {
```

```
kdc = server.company.com
admin_server = server.company.com
default_domain = company.com
}

[domain_realm]
    .company.com = COMPANY.COM
    company.com = COMPANY.COM

[kdc]
    profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
    pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
    }
```

If authentication against the Kerberos server works in full functionality, it is possible to set authentication at *Kerio MailServer*. To perform these settings, go to the *Directory Service* and *Advanced* tabs under *Configuration* → *Domains* (for details, see chapters 8.6 and 8.7).

Authentication against Open Directory

Before setting Kerberos user authentication at Linux, it is recommended to check that authentication against the domain functions correctly (check this by logging in the system using an account defined in the *Open Directory*). If the attempt fails, check out the following issues:

1. *Kerio MailServer* must belong to the Kerberos area (Open Directory domain) against which it authenticates. If *Kerio MailServer* is not the area member, the Kerberos system will not be working and the users will have to use a local password, i.e. different from the password for the domain.
2. the DNS service must be set correctly at the *Kerio MailServer's* host.
3. time of the *Kerio MailServer* host and the *Open Directory* must be synchronized (including time zone).

For proper authentication, define the `/etc/krb5.conf` file.

An example of the `krb5.conf` file:

```
[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    ticket_lifetime = 24000
    default_realm = COMPANY.COM
    dns_lookup_realm = false
    dns_lookup_kdc = yes

[realms]
    COMPANY.CZ = {
        kdc = server.company.com
        admin_server = server.company.com
        default_domain = company.com
    }

[domain_realm]
    .company.com = COMPANY.COM
    company.com = COMPANY.COM

[kdc]
    profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
    pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
    }
```

If authentication against the Kerberos server works in full functionality, it is possible to set authentication at *Kerio MailServer*. To perform these settings, go to the *Directory Service* and *Advanced* tabs under *Configuration → Domains* (for details, see chapters 8.6 and 8.7).

Authentication against a stand-alone Kerberos server (KDC)

To use authentication against a stand-alone Kerberos server (*Key Distribution Center*), it is necessary to maintain the username and password database both in *Key Distribution Center* and in *Kerio MailServer*.

Before setting Kerberos user authentication at Linux, it is recommended to check that authentication against the Kerberos area functions correctly (check this by logging in the system using an account defined in the *Key Distribution Center*). If the attempt fails, check out the following issues:

1. *Kerio MailServer* is a member of the Kerberos area to be authenticated against:
 - the Kerberos client must be installed on the computer,
 - username and password used for authentication at the system must be defined at the *Key Distribution Center*.
2. the DNS service must be set correctly at *Kerio MailServer's* host (*Key Distribution Center* uses DNS queries).
3. Time of *Kerio MailServer* and *Key Distribution Center* (all hosts included in the Kerberos area) must be synchronized (including time zone).

For proper authentication, define the `/etc/krb5.conf` file.

An example of the `krb5.conf` file:

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  ticket_lifetime = 24000
  default_realm = COMPANY.COM
  dns_lookup_realm = false
  dns_lookup_kdc = yes

[realms]
  COMPANY.CZ = {
    kdc = server.company.com
    admin_server = server.company.com
    default_domain = company.com
  }
```

```
[domain_realm]
    .company.com = COMPANY.COM
    company.com = COMPANY.COM

[kdc]
    profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
    pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
    }
```

Note: Before starting the Kerberos server, check out whether SPN (Service Principal Name) functions correctly.

Then, perform corresponding settings in *Kerio MailServer* (see chapter 8.7).

30.3 Kerio MailServer on Mac OS

Authentication against Active Directory

If *Kerio MailServer* is installed on Mac OS X and user accounts are mapped from the *Active Directory*, perform the following settings:

DNS configuration

To ensure that Mac OS X can access the *Active Directory*, enable resolving of DNS name from *Active Directory*. For this reason, it is also necessary to set *Active Directory* as the primary DNS server:

1. Open the *System Preferences* application and click on *Network* (see figure 30.4)
2. to open the *Network* dialog box. On the TCP/IP tab, specify the IP address of the *Active Directory* server in the *DNS servers* entry.

If the network configuration requires authentication against multiple domain controllers at a time, add all domain controllers where *Kerio MailServer* will be authenticated as DNS servers.

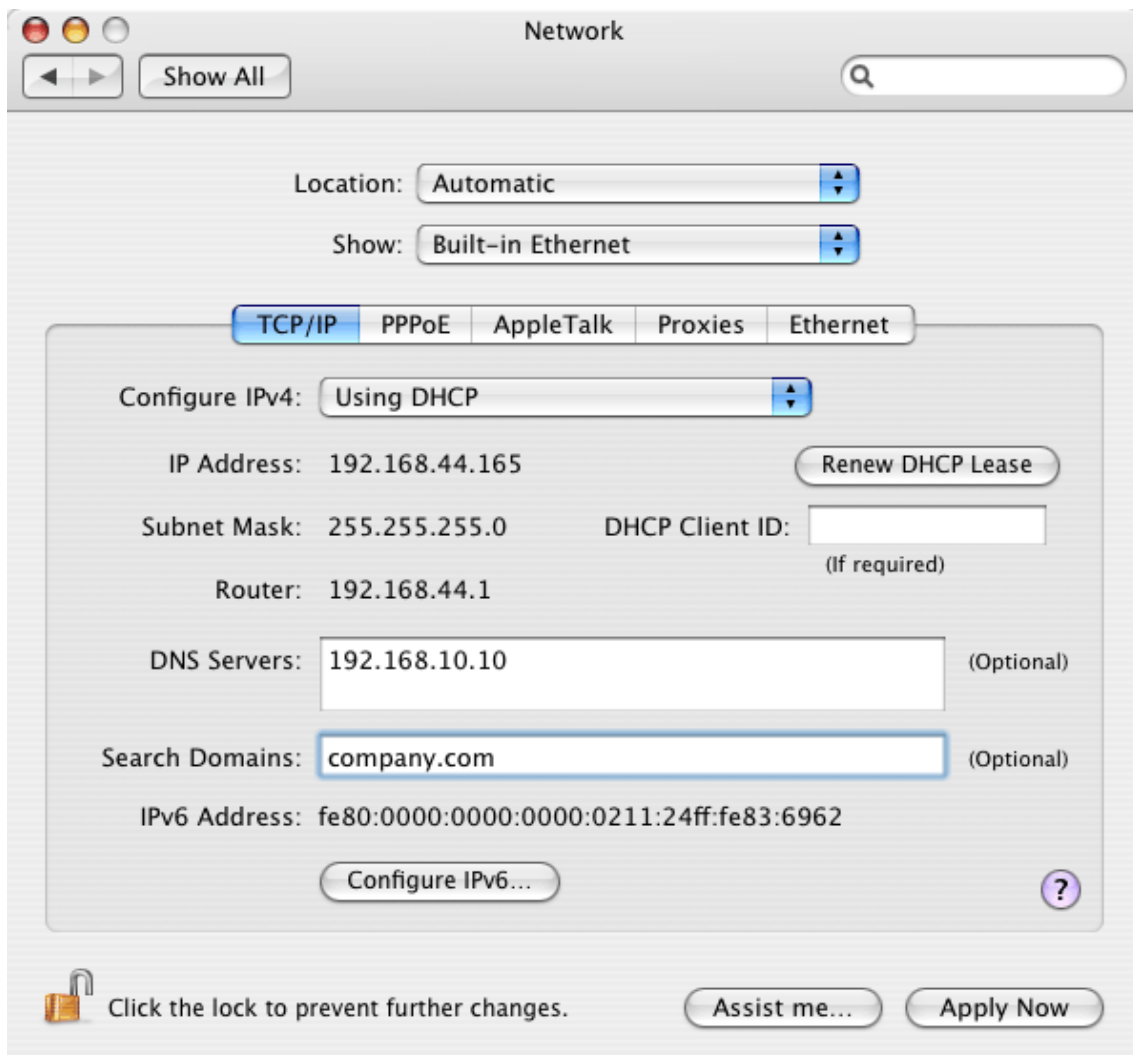


Figure 30.4 DNS configuration

Connection of the Kerio MailServer host to the Active Directory domain

To connect the computer to the *Active Directory* domain, use the *Directory Access* utility (*Applications* → *Utilities*) which is included in all basic *Apple Mac OS X* systems. For the configuration, follow these instructions:

1. Run the *Directory Access* application and enable the *Active Directory* service in the *Services* section (see figure 30.5). Enter authentication name and password. The user who makes changes in the application needs administration rights for the system.
2. Enable the service, click on *Configure* and specify the *Active Directory* domain name (see figure 30.6).

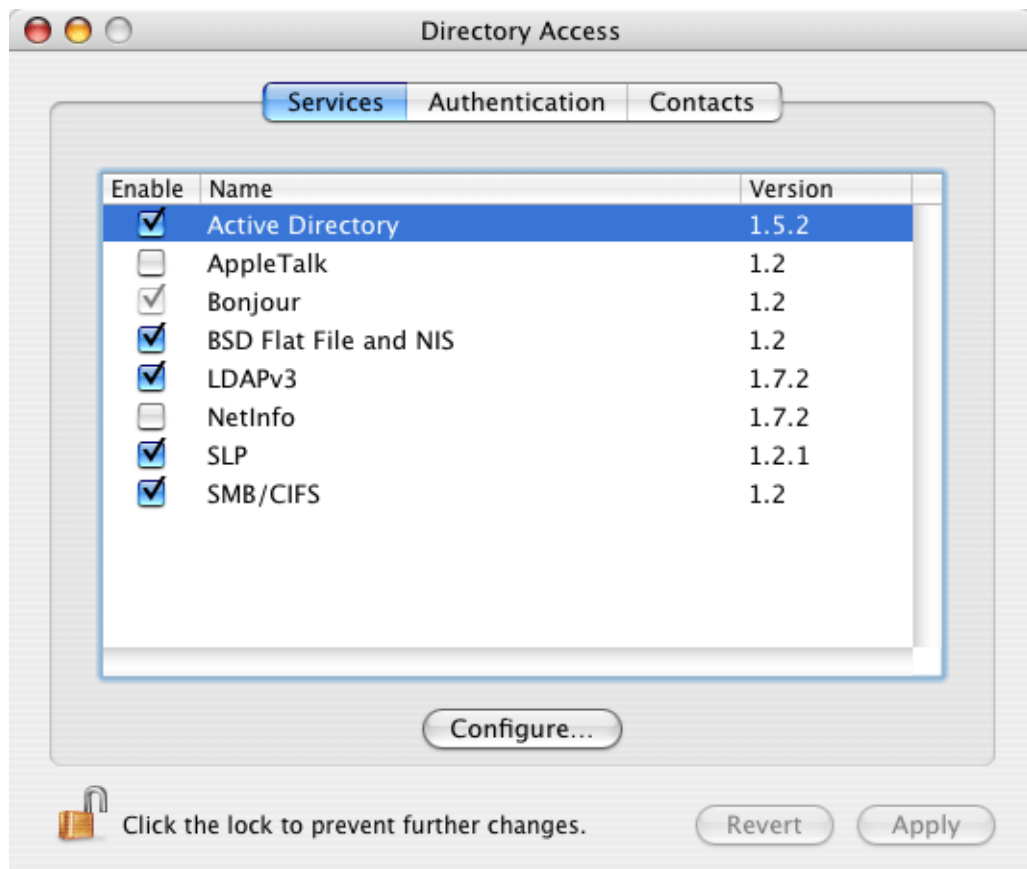


Figure 30.5 Directory Access — Services

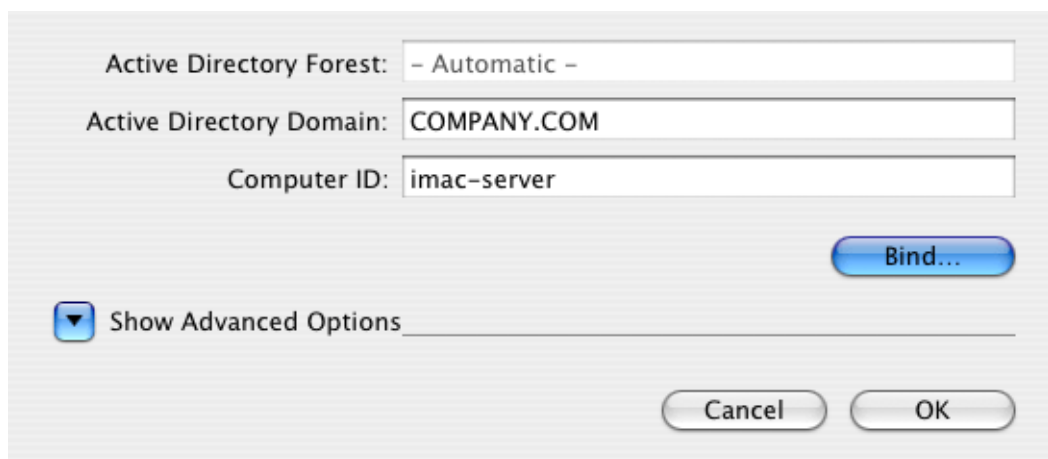


Figure 30.6 Directory Access — configuration

3. Click on *Bind* and set username and password for the *Active Directory*, administrator. The administrator will be allowed to add computers to the *Active Directory* domain (see figure 30.7).

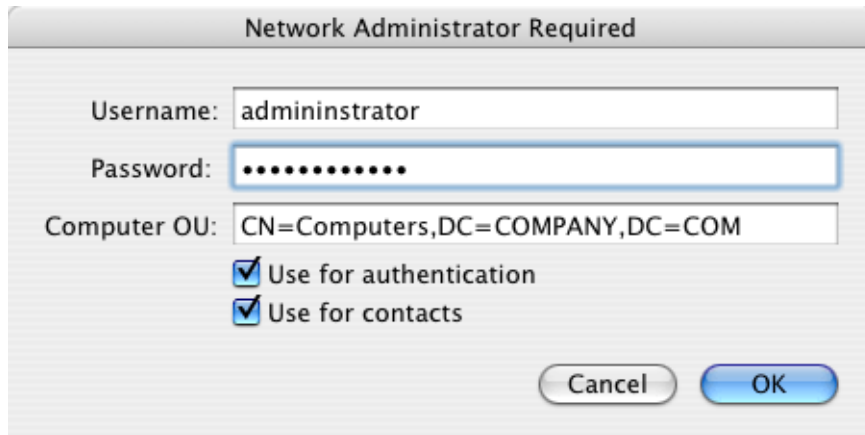


Figure 30.7 Directory Access — specification of administrator's login data

If all settings are done correctly, it will take only a few seconds to connect the computer to the domain.

Kerberos settings

Once Mac OS X is successfully connected to the *Active Directory* domain, the special `edu.mit.Kerberos` file is created in the `/Library/Preferences/` directory. Make sure that the file has been created correctly. You can use the following example for comparison:

```
# WARNING This file is automatically created by Active Directory
# do not make changes to this file;
# autogenerated from : /Active Directory/company.com
# generation_id : 0
[libdefaults]
    default_realm = COMPANY.COM
    ticket_lifetime = 600
    dns_fallback = no
[realms]
    COMPANY.CZ = {
        kdc = server.company.com. :88
        admin_server = mail.company.com .
    }
```

Using the `kinit` utility, it is possible to test whether *Kerio MailServer* is able to authenticate against the *Key Distribution Center*. Simply open the prompt line and use the following command:

```
kinit -S host/name_KMS@KERBEROS_REALM user_name
```

for example:

```
kinit -S host/mail.company.com@COMPANY.COM jsmith
```

If the query was processed correctly, you will be asked to enter password for the particular user. Otherwise, an error will be reported.

Authentication against Open Directory

Kerio MailServer can either be installed on the server with the *Apple Open Directory* directory service or on another server.

If *Kerio MailServer* is installed on the same server as *Open Directory*, it is not necessary to perform any additional configuration besides installation of the *Kerio Open Directory Extension* installation. If it is installed on another computer, external authentication through *Kerberos* to *Open Directory* must be set.

Kerio MailServer can be installed on servers with *Mac OS X 10.3* or *Mac OS X 10.4*. The settings are similar for both versions. The following description applies to configuration on *Mac OS X 10.4*, any discrepancies will be mentioned.

External authentication is configured with a special application, *Directory Access*. The application can be found under *Applications* → *Utilities* → *Directory Access*. This application is used to create the special `edu.mit.Kerberos` authentication file which is located under `/Library/Preferences`. The following settings must be performed to make the authentication work properly:

1. Start the *Directory Access* application.
2. On the *Services* tab, check the *LDAPv3* item (see figure 30.8).

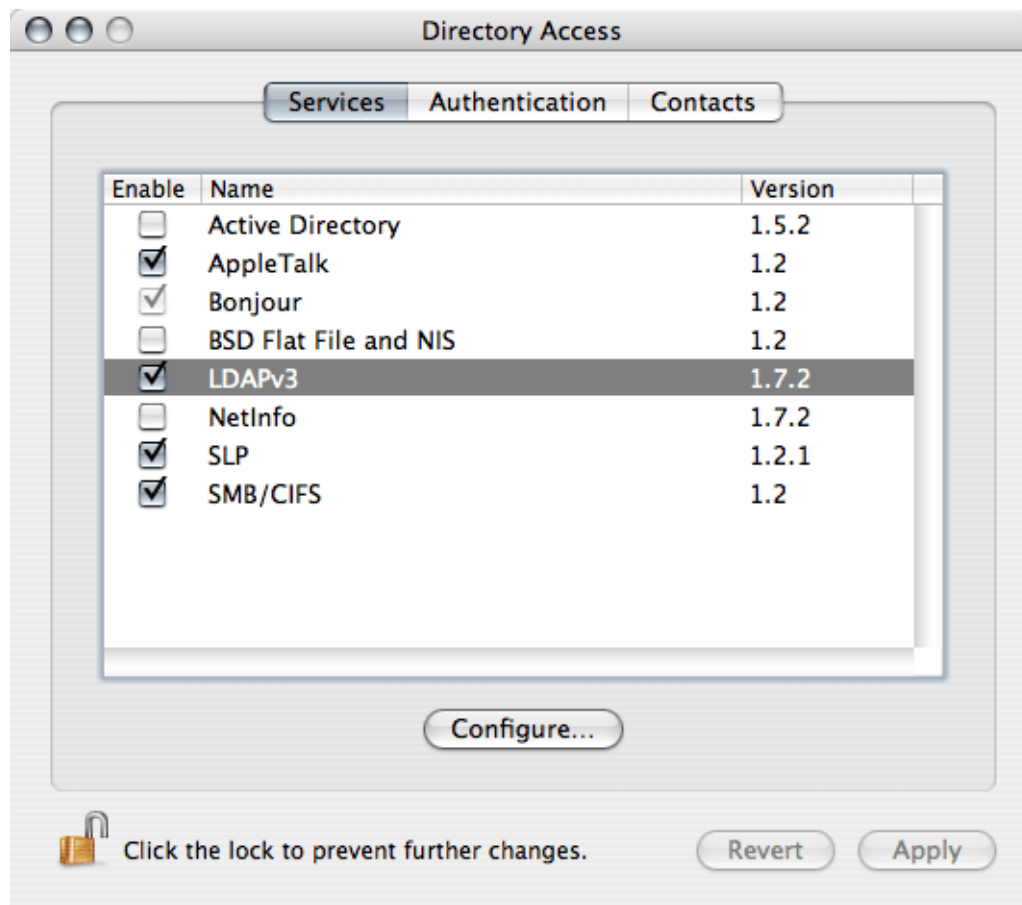


Figure 30.8 Directory Access — checking LDAP

3. On the *Services* tab, use the mouse pointer to park the DAPv3 item and click on *Configure*.
4. In the next dialog, click *New*.
5. This will open a dialog box where IP address and name of the server can be specified. Enter IP address or DNS name of the server where *Apple Open Directory* is running. Once the server is specified, click on the *Manual* button (not necessary in the *Mac OS X 10.3* version) and enter a name in the *Configuration name* text box (this item is used for reference only).
6. Save the configuration and select *Open Directory Server* in the *LDAP Mappings* menu.
7. Once *Open Directory Server* is selected, the dialog for specification of the search suffix is opened (*Search Base Suffix*). The suffix must be entered as shown in the example in figure 30.9:

mail1.company.com → dc=mail1,dc=company,dc=com

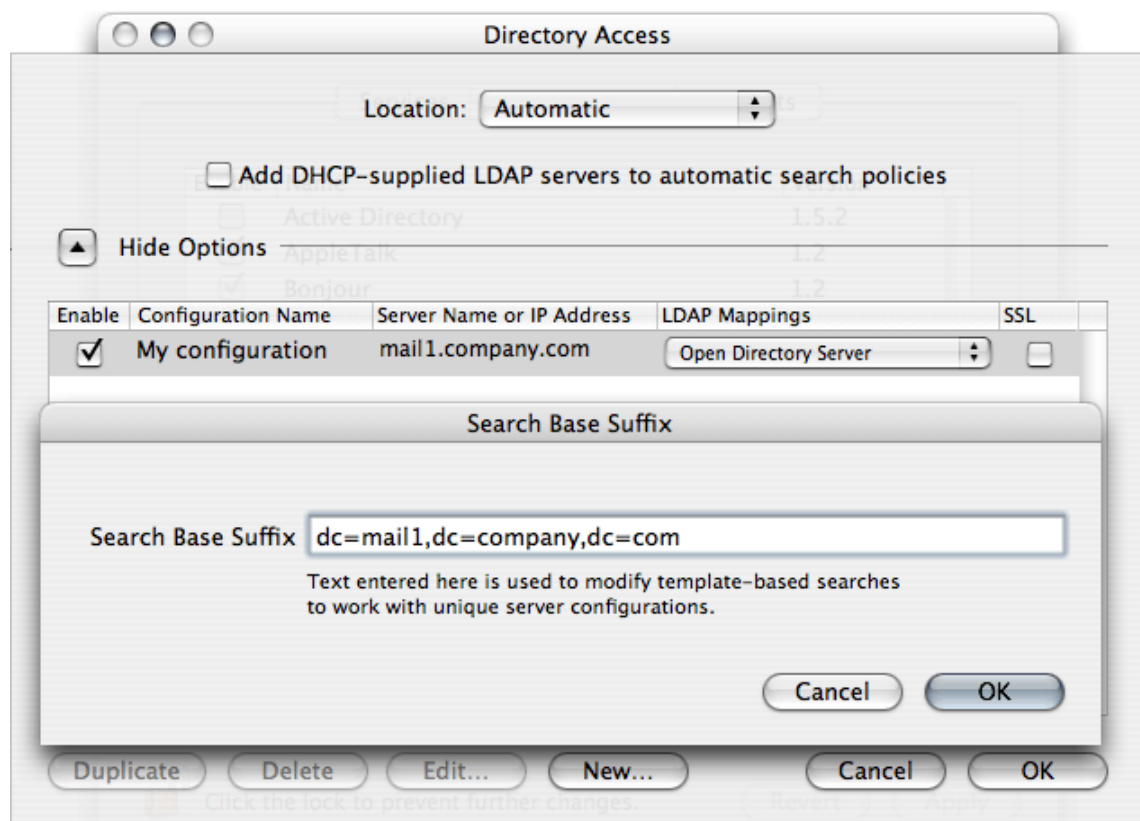


Figure 30.9 Directory Access — configuration of the Open Directory server

The figure implies that the suffix must be specified as follows: `dc=subdomain,dc=domain`. Number of subdomains in the suffix must meet the number of subdomains in the server's name.

8. Now, authentication will be set for the *Open Directory* server. Switch to the *Authentication* tab (see figure 30.10).

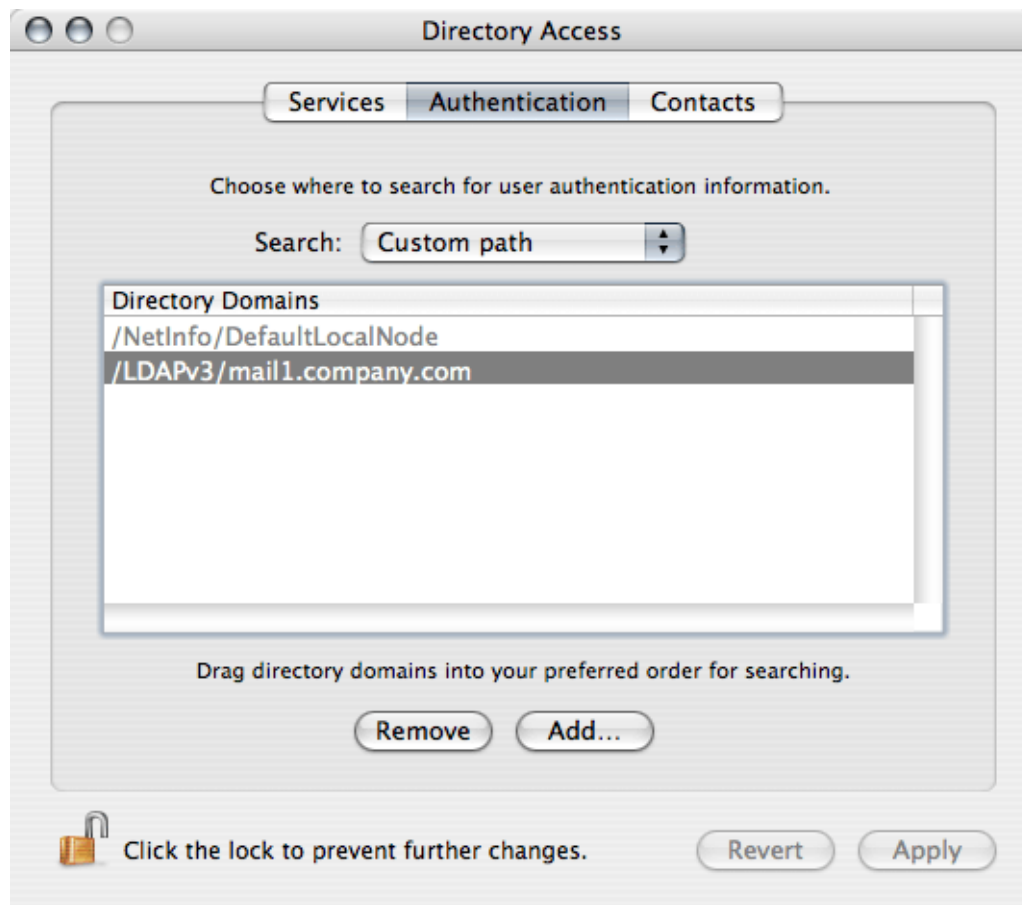


Figure 30.10 Directory Access — Authentication settings

9. In the *Search* menu, it is necessary to select *Custom path*.
10. Enter the name of the *Open Directory* server to the *Directory Domains* list. Click on *Add*. The *Directory Access* application automatically enters the *Open Directory* name specified on the previous tab. Simply confirm the offer.
11. Save the settings by the *Apply* button.

Directory Access creates the `edu.mit.Kerberos` file in the `/Library/Preferences` directory. Check if the file includes correct data. The following parameters should be included:

```
# WARNING This file is automatically created by Active Directory
# do not make changes to this file;
# autogenerated from : /Active Directory/company.com
# generation_id : 0
[libdefaults]
```

```
default_realm = COMPANY.COM
ticket_lifetime = 600
dns_fallback = no
[realms]
COMPANY.CZ = {
    kdc = mail1.company.com.:88
    admin_server = mail.company.com .
}
```

Using the `kinit` utility, it is possible to test whether *Kerio MailServer* is able to authenticate against Kerberos. Simply open the prompt line and use the following command:

```
kinit -S host/name_KMS@KERBEROS_REALM user_name
```

for example:

```
kinit -S host/mail.company.com@COMPANY.COM jsmith
```

If the query was processed correctly, you will be asked to enter password for the particular user. Otherwise, an error will be reported.

Now, simply change configuration in *Kerio MailServer*:

- In the *Domains* section in the *Kerio MailServer's* administration console, specify parameters on the *Directory Service* and the *Advanced* tabs (the *Apple Open Directory* realm must be specified in the *Kerberos 5* entry)
- In the *Kerio MailServer's* administration console, the *Apple Open Directory* authentication type must be set for user accounts

Authentication against a stand-alone Kerberos server (KDC)

To use authentication against a stand-alone Kerberos server (*Key Distribution Center*), it is necessary to maintain the username and password database both in *Key Distribution Center* and in *Kerio MailServer*.

Before setting Kerberos user authentication at *Kerio MailServer*, it is recommended to check that authentication against the Kerberos area functions correctly (check this by logging in the system using an account defined in the *Key Distribution Center* at the host where *Kerio MailServer* will be installed). If the attempt fails, check out the following issues:

1. *Kerio MailServer* is a member of the Kerberos area to be authenticated against:
 - the Kerberos client must be installed on the computer,
 - username and password used for authentication at the system must be defined at the *Key Distribution Center*.

2. the DNS service must be set correctly at *Kerio MailServer's* host (*Key Distribution Center* uses DNS queries).
3. Time of *Kerio MailServer* and *Key Distribution Center* (all hosts included in the Kerberos area) must be synchronized (including time zone).

Kerberos functionality can be tested by checking the `/Library/Preferences/edu.mit.Kerberos` file. The following parameters should be included:

```
# WARNING This file is automatically created by Active Directory
# do not make changes to this file;
# autogenerated from : /Active Directory/company.com
# generation_id : 0
[libdefaults]
    default_realm = COMPANY.COM
    ticket_lifetime = 600
    dns_fallback = no
[realms]
    COMPANY.CZ = {
        kdc = server.company.com. :88
        admin_server = server.company.com.
    }
```

Using the `kinit` utility, it is possible to test whether *Kerio MailServer* is able to authenticate against Kerberos. Simply open the prompt line and use the following command:

```
kinit -S host/name_KMS@KERBEROS_REALM user_name
```

for example:

```
kinit -S host/mail.company.com@COMPANY.COM jsmith
```

If the query was processed correctly, you will be asked to enter password for the particular user. Otherwise, an error will be reported.

Note: Before starting the Kerberos server, check out whether SPN (Service Principal Name) functions correctly.

When the previous steps are followed successfully, set authentication in *Kerio MailServer* on the *Advanced* tab under *Configuration* → *Domains*, (see chapter 8.7).

30.4 Starting Open Directory and Kerberos authentication settings

In *Open Directory*, it is possible to authenticate users against the password server (refer to chapter 29.4) or the Kerberos server (for details, see chapter 30). As mentioned in chapter 29.4, authentication against the password server does not require any additional settings, while Kerberos authentication might be quite difficult to configure. This chapter therefore focuses on correct setting of the authentication against the Kerberos server in *Open Directory*.

After Mac OS X Server's startup, make sure that both the *Open Directory* service and the Kerberos server are running. This can be done in the *Server Admin* application (*Applications* → *Server* → *Server Admin*).

The welcome dialog of *Server Admin* consists of two basic sections. The left one includes a list of hosts and services which are running at these hosts. This section also includes the host where the *Open Directory* service is supposed to be started. If the service is already running, it is bold and marked with a green symbol (see figure 30.11).

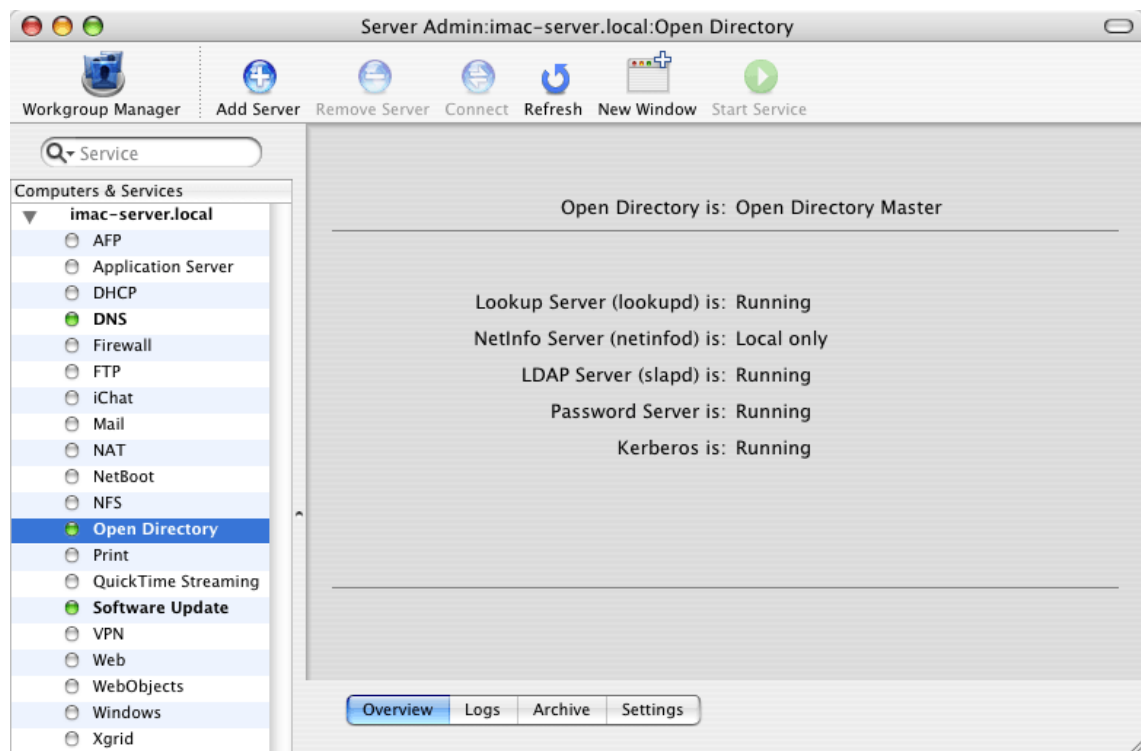


Figure 30.11 The Open Directory service

The right section usually includes information about the selected service, its logs and settings.

The directory service should be started automatically by the first startup of the Mac OS X Server. If it is not running, mark it by the mouse pointer and click the *Start Service* button at the toolbar. In the right section of the window, find out which *Open Directory* services are and which are not running (see figure 30.11). The Kerberos entry is important. If the Kerberos server is running, no additional settings are required. If not, check out the following issues:

1. On the *Settings* tab, the server must be set as *Open Directory Master*. Authentication is required to edit these settings. Use username and password of the administrator account which was created in the *Open Directory*, for example the *diradmin* user (see figure 30.12).

Create a new Open Directory master domain

Creating a new Open Directory master domain requires you to create a new administrator account for that domain. This account needs to have a unique name, short name and user ID.

New Account

Name:

Short Name: User ID:

Password:

Verify:

Domain Info

Kerberos Realm:

Search Base:

Search base is optional.

Figure 30.12 Setting of administration username and password

2. The DNS service must be configured correctly.
3. DNS name (hostname) of the server where *Open Directory* is running must be set correctly.

Once the Kerberos server is started successfully, it is recommended to test correct configuration by the `kinit` utility. Simply open the prompt line and use the following command:

```
kinit -S host/name_KMS@KERBEROS_REALM user_name
```

for example:

```
kinit -S host/mail.company.com@COMPANY.COM diradmin
```

If the query was processed correctly, you will be asked to enter password for the particular user. Otherwise, an error will be reported.

Note: Logs available on the *Logs* tab can be helpful for troubleshooting.

Chapter 31

Kerio Outlook Connector

Kerio Outlook Connector is an extension to *MS Outlook*. It allows scheduling and sharing different types of data. Thanks to this modification, *MS Outlook* is able to work with groupware data (contacts, calendar, tasks) stored in *Kerio MailServer*. The main benefit of the shared data store is that the data is available via the Internet anywhere necessary. To access the data, you'll need just an Internet connection and a web browser (the *Kerio WebMail* interface) or *MS Outlook* with *Kerio Outlook Connector* or *MS Entourage*.

Kerio MailServer and *MS Outlook* communicate via MAPI. MAPI (Messaging Application Programming Interface) is a versatile interface for email transmission. It is a software interface that enables any MAPI client to communicate with any mailserver (*Microsoft Outlook* and *Kerio MailServer* in this case).

Kerio Outlook Connector since version 6.1 provides support for digital signatures. The function and settings for digital signatures are described in standard *MS Outlook* help.

TIP: If you intend to handle your email also offline, follow the instructions in chapter 31.8.

For proper functionality of the *Kerio Outlook Connector*, the following services must be running in *Kerio MailServer*:

- *HTTP(S)* — the protocol is used for automatic updates of the *Kerio Outlook Connector* and also for communication with the *Free/Busy* server.
- *IMAP(S)* — the MAPI interface uses the IMAP protocol in *Kerio MailServer*.
- *SMTP(S)* — the protocol is used for email sending.

Installation of the *Kerio Outlook Connector* can be run under Windows 2000 Professional (version Service Pack 4), XP, MS IE 6.0 and later.

Kerio Outlook Connector supports the following email clients:

- MS Outlook 2000 + version Service Pack 3 (if the service pack version is not installed, *Kerio Outlook Connector* installation cannot be started)
- MS Outlook XP + version Service Pack 3 (the version of *MS Outlook XP* must have this format: 10.0.6515.xyz)
- MS Outlook 2003 + version Service Pack 1 (if the service pack version is not installed, *Kerio Outlook Connector* installation cannot be started)

Note: All settings relate to *MS Windows XP* and *MS Outlook 2003*. If you use a different version of *MS Outlook 2000*, the settings may differ (see chapter 31.4).

Installation of the *Kerio Outlook Connector* can be run either independently or along with *Kerio MailServer Migration* (refer to chapter 37):

31.1 Upgrade the Kerio Outlook Connector

The *Kerio Outlook Connector* upgrade is automatic and user-independent. Current versions of *Kerio Outlook Connector* are checked for by *Kerio MailServer Engine* and displayed in an administration console (*Advanced options* section, *Upgrade* tab (see chapter 16.6)).

Warning: Upgrading from *Kerio Outlook Connector 6.0.0 - 6.0.8* requires a manual installation of *Kerio Outlook Connector 6.1* or higher. Future versions of the *Connector* will automatically be upgraded by the *MailServer*.

New versions of *Kerio Outlook Connector* are stored in `/webmail/download` directory, where *Kerio MailServer* is installed.

Warning: If only HTTPS traffic is allowed in *Kerio MailServer* (e.g. for security reasons), it is necessary that a trustworthy *Kerio MailServer* certificate is installed in *Internet Explorer* of the client station (a self-signed certificate can be used). Otherwise, new versions will not be updated automatically.

31.2 Installation and configuration without the migration tool

If you install *Kerio Outlook Connector* without using the migration tool, profile and email account must be set manually. Installation of the *Kerio Outlook Connector* for *Kerio MailServer* is performed by the wizard.

Warning:

- *MS Outlook* must be installed on the computer prior to the *Kerio Outlook Connector* installation, otherwise the application will not function properly.
- When the upgrade or downgrade of *MS Outlook* is performed, *Kerio Outlook Connector* must be reinstalled.

Profile creation

The user profile is a file where personal information in *MS Outlook* is stored. The profile is essential in the following situations: either the computer is accessed by multiple users and each of them needs his/her own email address and personal settings or a user can access multiple mailboxes and wants to use different personal settings for each of them. Settings for a new profile can be configured in the *Start → Settings → Control Panel → Mail* menu.



Figure 31.1 Profile setup

To open the profile settings window, click *Show Profiles*.

Click on the *Add* button to create a new profile and enter its name. Name of the new profile can be specified in the dialog box.

In this dialog, it is also possible to define whether always an only one particular profile will be used or whether list of installed profiles will be offered for selection during each connection establishment.

Prompt for a profile to be used

Upon each *MS Outlook* startup, a window with the list of available profiles appears. One of the profiles can be later selected as the default.

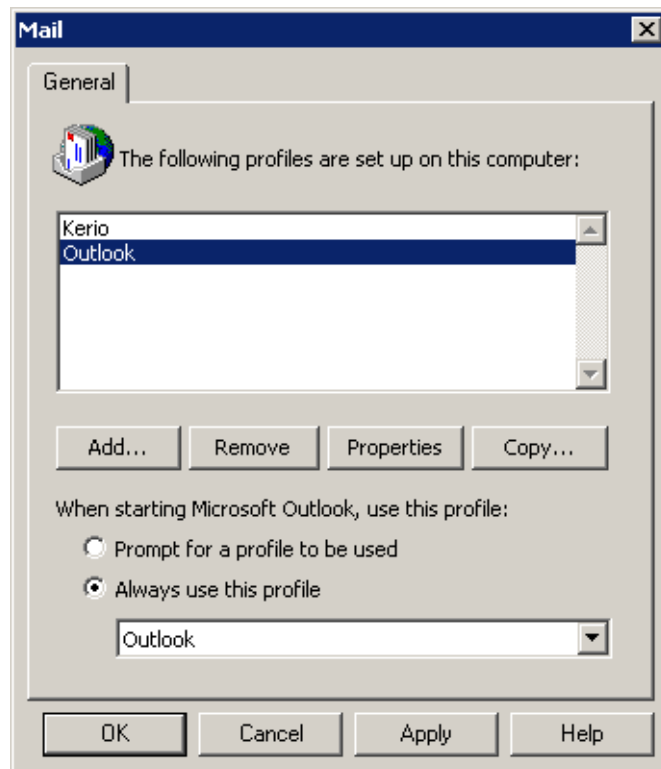


Figure 31.2 Creation of a profile

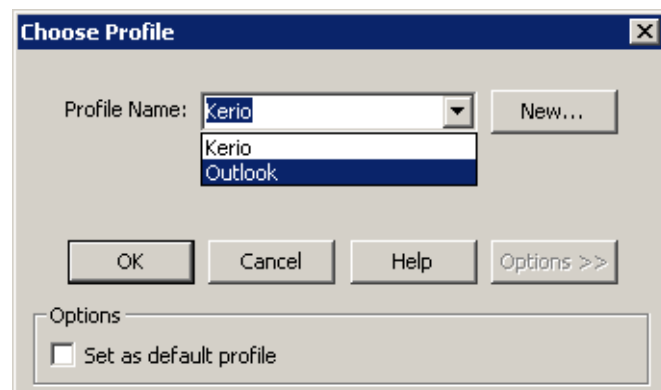


Figure 31.3 Choose Profile

Always use this profile

The profile selected under *Always use this profile* will be used by default.

Warning: Each *MS Outlook* profile may be used only by one account connected via *Kerio Outlook Connector*. Functionality of POP3 and IMAP accounts located in the same profile is not affected by *Kerio Outlook Connector Store*.

Note: If you use *MS Outlook 2000*, make sure that you add *Kerio MailServer* a *Outlook Address Book* items during configuration (for more information, see chapter 31.4). In higher versions of *MS Outlook*, *Outlook Address Book* is added automatically.

Initial settings

Always configure the email account settings only after the profile creation. The email account can be added using the *Tools* → *Email accounts* menu.

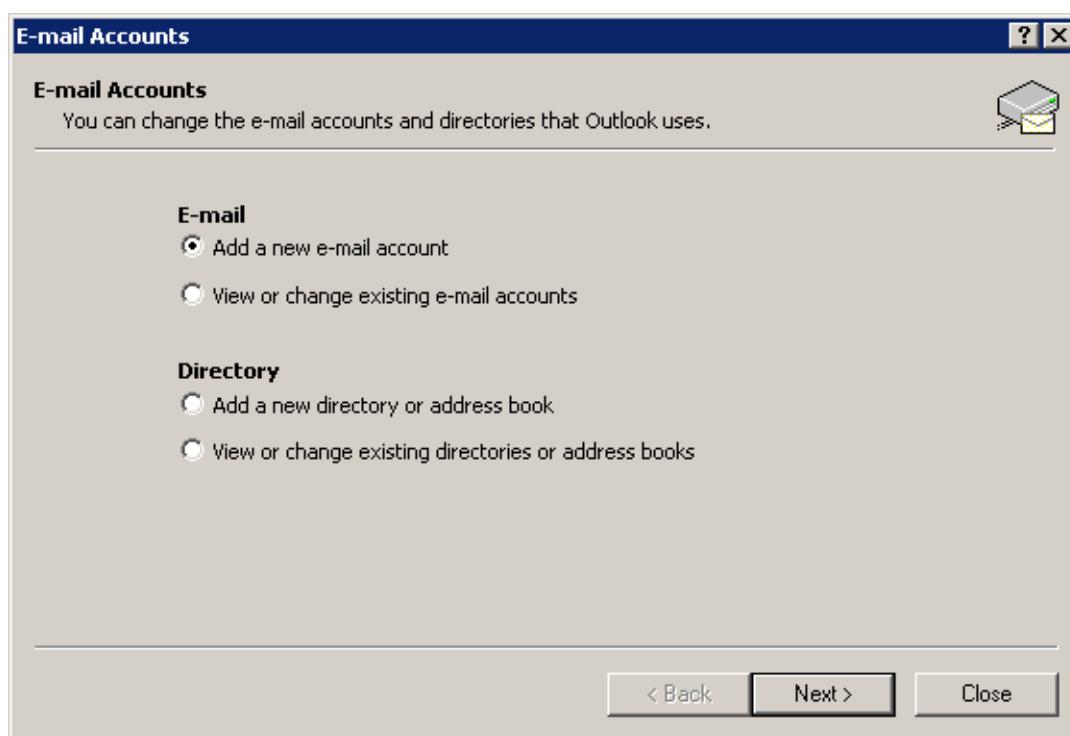


Figure 31.4 Account settings — creation of new account

Email accounts or an address book can be added or changed immediately after the wizard is opened. To create a MAPI account, select the *Add a new email account* option.

In the second step, select a server type for the new account. *Kerio MailServer* is always required in this case.

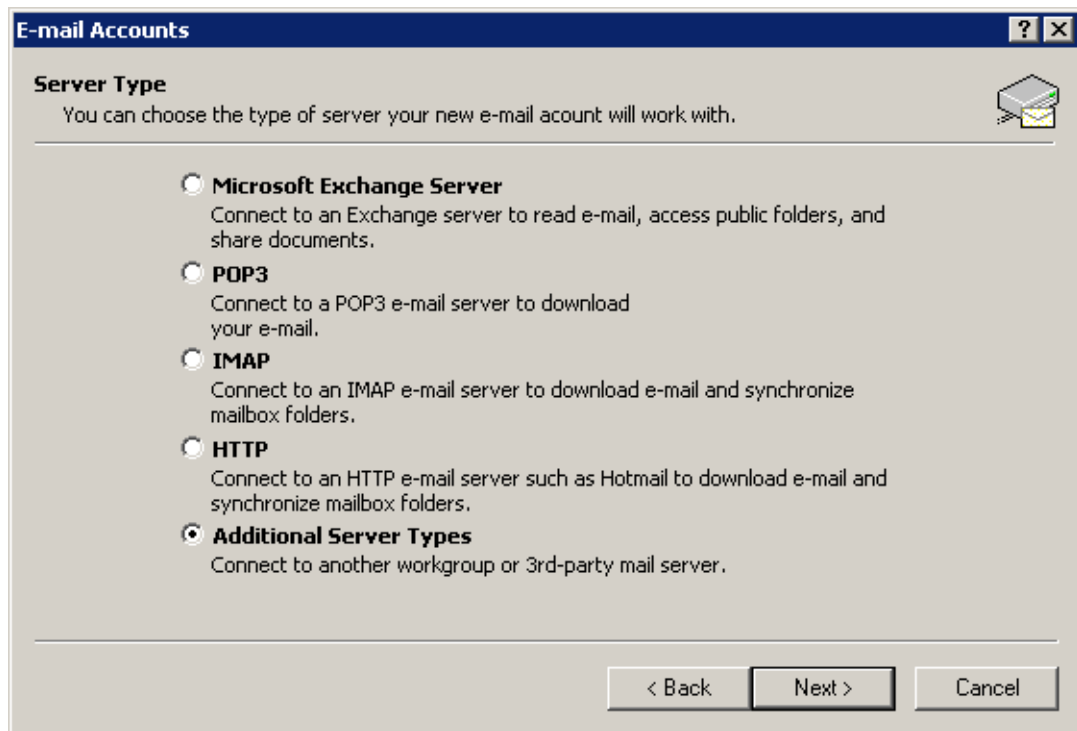


Figure 31.5 Account settings — server type selection

In the next step, the settings for *Kerio Outlook Connector* are defined. This can be done using two tabs in the *Kerio Outlook Connector* window:

Server Name

DNS name or IP address of the MailServer.

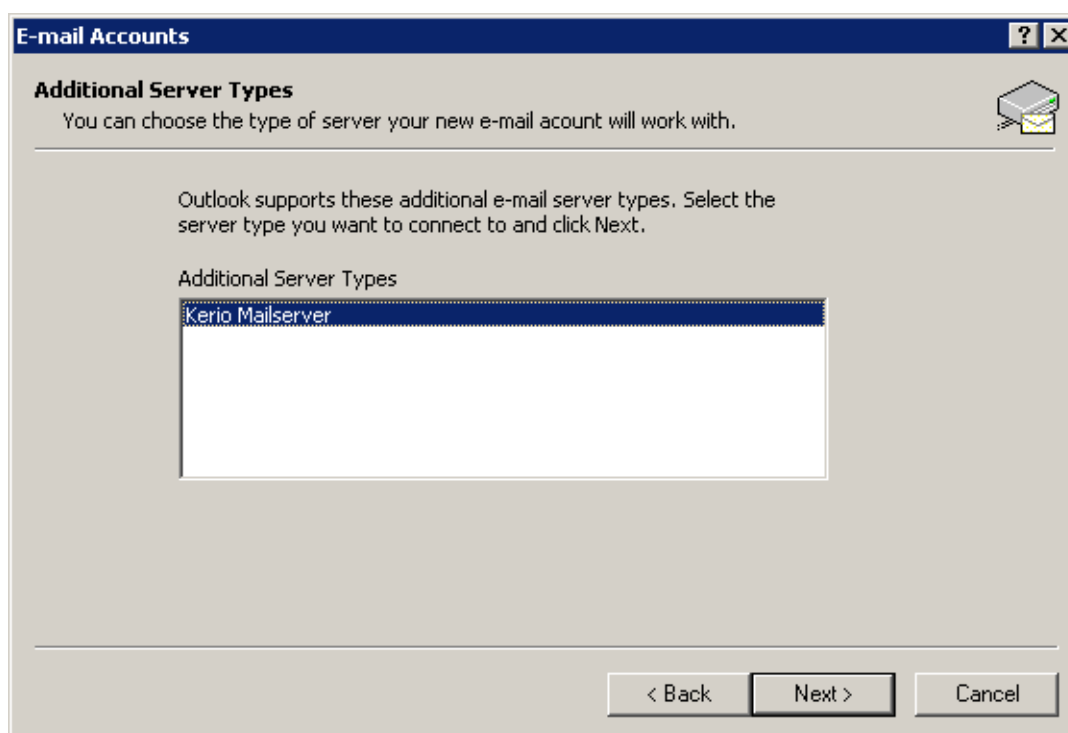


Figure 31.6 Account settings — Kerio MailServer selection

Secure Password Authentication

This option allows using the NTLM authentication. When checked, users are not required to set usernames and passwords — the authentication will be used instead. In order for the NTLM authentication to be functional, both the computer as well as the user account have to be parts of the domain used for authentication.

Warning: NTLM (SPA) can be used only on *Windows* operating systems. *Linux* and *Mac OS* operating systems do not support this type of authentication (see table 16.2).

Username

Username used for logging to the MailServer. If the user does not belong to the primary domain, a complete email address is required (jwayne@company.com).

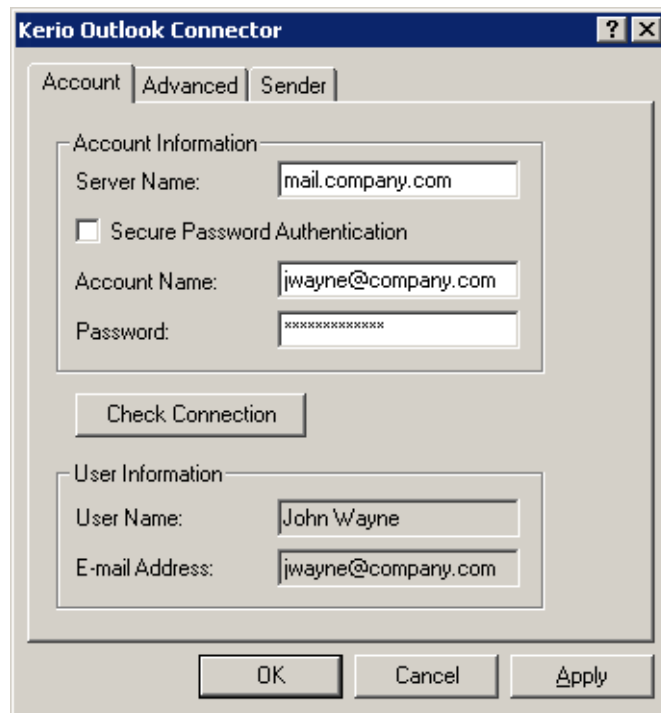


Figure 31.7 Account settings — connection settings

Password

User password.

Press the *Check connection* button to test if correct user data has been specified and if the connection to *Kerio MailServer* works properly. If the test is finished successfully, a corresponding *User Name* and *Email Address* are automatically filled in.

Use the *Advanced Settings* tab to change some of the communication settings.

IMAP and SMTP port

Port used for communication with the server by IMAP and SMTP protocols. The port numbers must be the same as the port numbers set in *Kerio MailServer*.

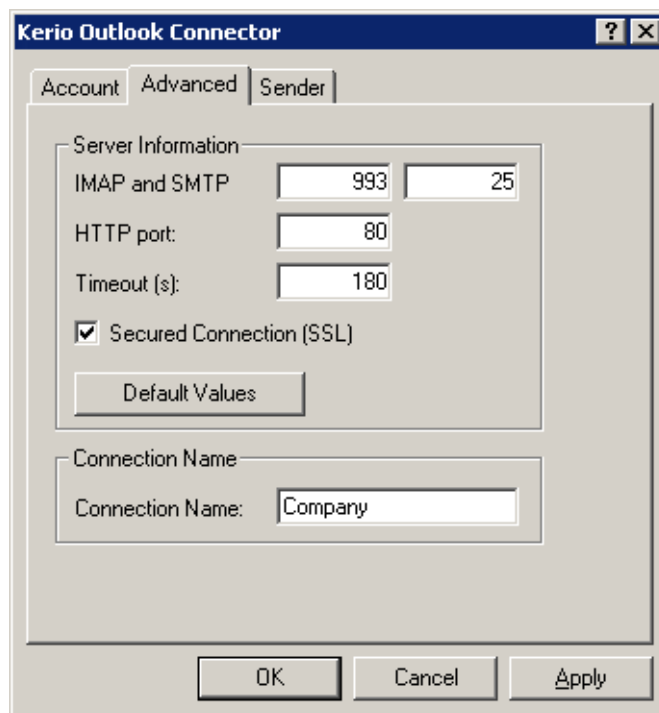


Figure 31.8 Account settings — ports

HTTP port

The HTTP(S) protocol uses the *Free/Busy* calendar and applications for automatic updates of *Kerio Outlook Connector*. Port number must be identical with the port number for the HTTP(S) service used by *Kerio MailServer*.

Timeout

Time spent by the application waiting for a response from *Kerio MailServer*.

Secured Connection (SSL)

This option enables the SSL-encrypted communication using IMAP, SMTP and HTTP.

The *Default Values* button changes all settings to their default values.

Connection name

Kerio Outlook Connector Store is used by default. This name can be changed.

Name and its visibility, email address and a *Reply-To* address can be set in the *Name* tab.

Use Following Name

This option allows to select any user name which will be used for outgoing mail. For better understanding, read the following examples:

Example 1:

Multiple users can use the email account. Using the *Name* tab, name of the account can be replaced by the name of a corresponding user. The following format will be

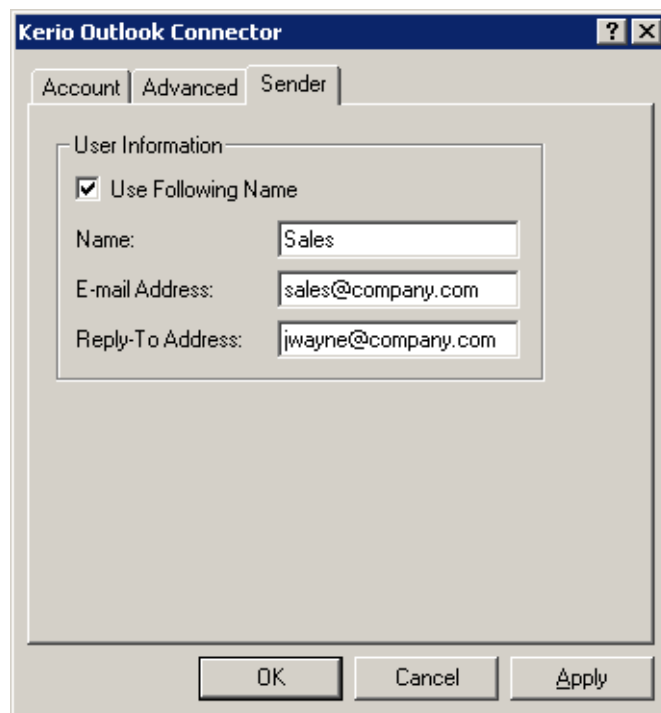


Figure 31.9 Account settings — sender information settings

used for the *From* item:

the.particular.username@company.com <techsupport@company.com>

Example 2:

The *Use Following Name* option can be also used in the reversed principle. It means that a common information can be entered in the *Name* text field and the account can belong to a particular user. The format of the *From* item will be as follows:

Technical support <jsmith@company.com>

Name

The name that appears in sent email messages.

Email Address

The email address from which the messages are sent.

Address for replies

Address to which replies will be sent (the *Reply-To:* item).

Note: If 2000 is used, changes performed on the *Sender* tab will take effect after a restart of the application.

Data file settings

In order for *Kerio Outlook Connector* to work properly, it is necessary to set the *[Kerio Outlook Connector Store]* as the default data file. If the file has not been selected automatically before, it can be specified in the *Tools → Email Accounts → View or Change Existing Email Accounts* menu. The *Email Accounts* window contains the *Deliver new email to the following location* option, where *Kerio Outlook Connector Store* can be selected.

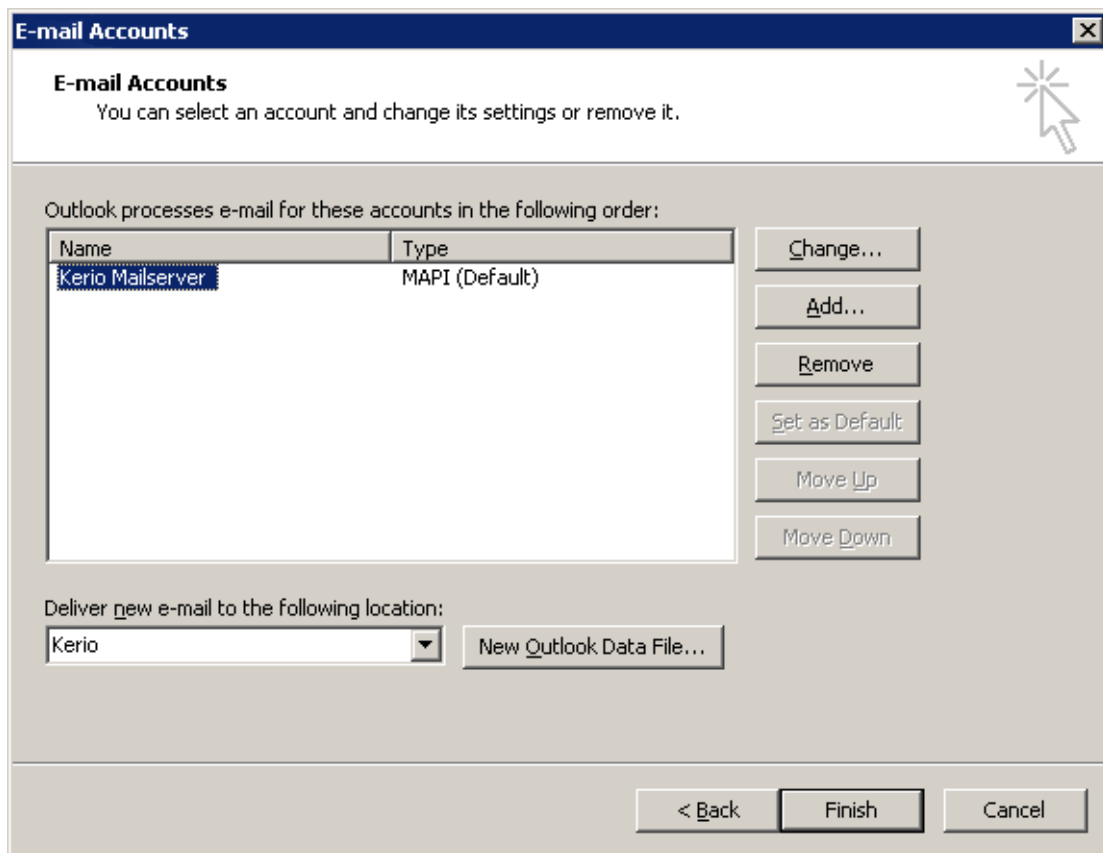


Figure 31.10 Data file settings

Kerio Outlook Connector can also check whether the *Kerio Outlook Connector Store* is selected as a default message store. By default, the check is enabled and if the *Kerio Outlook Connector Store* is not selected as a default store when *MS Outlook* is started, a warning is displayed.

This option can be enabled/disabled in the *Tools → Options → Preferences* menu (with the *Kerio Technologies* logo).

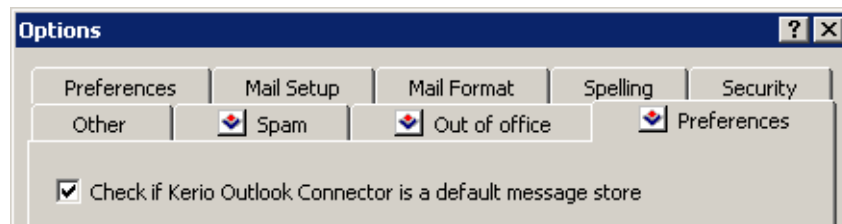


Figure 31.11 The store checking option

31.3 Installation and profile creation using the migration tool

Kerio Outlook Connector can be installed on client hosts during migration of user accounts from *MS Exchange* to *Kerio MailServer*. Migration is performed using a special *Kerio MailServer Migration* application (for more information about server migration using *Kerio MailServer Migration*, see chapter 37). Together with the installation, basic settings of the user profile and account are configured. Installation can be performed on all client computers at once. Each user whose mailbox has been migrated receives a message with a link to automatic installation of *Kerio Outlook Connector*.



Figure 31.12 User profile creator

When the user clicks the link, a dialog is displayed where the e-mail address and password for access to their mailbox must be specified. After the basic settings have been specified, the installation is started. If the installation was completed successfully, profile creation confirmation appears. Check *Set it as a default profile* to set this profile as the default one. After opening this profile in *MS Outlook*, a MAPI account named *Kerio Outlook Connector Store* will be created, where all user folders, messages, events as well as tasks previously used in *MS Exchange* will be stored.

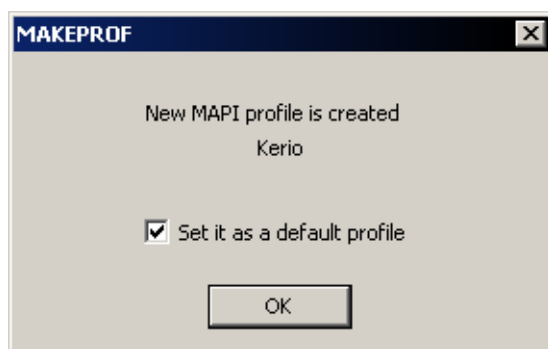


Figure 31.13 Successful profile creation information

Note: If *Kerio Outlook Connector* is installed in *MS Outlook 2000*, additional configuration of the profile created is necessary. Add *Outlook Address Book* service into the profile manually (for more information, see chapter 31.4).

Warning: Each *MS Outlook* profile may be used only by one account connected via *Kerio Outlook Connector*. Functionality of POP3 and IMAP accounts located in the same profile is not affected by *Kerio Outlook Connector Store*.

31.4 Installation and configuration of MS Outlook 2000

The installation of *Kerio Outlook Connector* in *Outlook 2000* is different from the installation in previous versions:

1. *Outlook 2000* must have Service Pack 3 installed; if the Service Pack is missing, the installation of *Kerio Outlook Connector* will fail.

Outlook 2000 must be installed in the *Corporate or Workgroup* mode. If the installation of *Outlook 2000* is performed in the *Internet only* mode, change the mode in *Tools* → *Options* → *Email services* → *Reconfigure email support* (the installation disc of *Outlook 2000* might be required).

2. Another difference applies to the new profile creation. For more information about profiles and their creation in *Outlook*, see chapter 31.2.

After a successful installation of *Kerio Outlook Connector*, create a new profile. This can be done in the following ways:

- Profile creation using a migration tool (see chapter 31.3).
- Manual profile creation (see chapter 31.2).

If a migration tool is used for profile creation, click *Tools* → *Services* and add the *Outlook Address Book* item to the profile. If the *Outlook Address Book* will not be added to the profile, contacts folders will not work properly.

If a profile is created by hand, it is possible to follow the method described in chapter 31.2. The only difference is that it is necessary to add the *Kerio MailServer* and *Outlook Address Book* services during creation. Both services can be added to the profile later in *Tools* → *Services* menu.

31.5 Spam/Not Spam buttons displaying problems

Sometimes it may happen that the *Spam/Not Spam* buttons may be missing on the toolbar when the *Kerio Outlook Connector* or *MS Outlook* is started. In such a case, it is necessary to allow *Kerio Outlook Connector* in forbidden items of *MS Outlook*.

The dialog for forbidden items can be found under *Help* → *About Microsoft Office Outlook*. Click *Disabled items* to open the dialog and simply uncheck *Kerio Outlook Connector*.

31.6 Private events

Up to *Kerio MailServer 6.1.2*, events were not classified as public or private. Since 6.1.3, this information is distinguished. By default, all events created in *Kerio MailServer 6.1.2* and lower are set as public in 6.1.3 and higher. To make a public event a private one, simply open the event and change the classification by hand.

31.7 Messages signed in MS Outlook

If your messages are digitally signed, check the *Send clear text signed message when sending signed messages* option under *Tools* → *Options* on the *Security* tab (see figure 31.14). This option provides that also *Kerio WebMail* users may read the message.

Note: The settings shown here applies to *MS Outlook 2003*. For *MS Outlook (2000/XP)*, the settings may differ slightly.

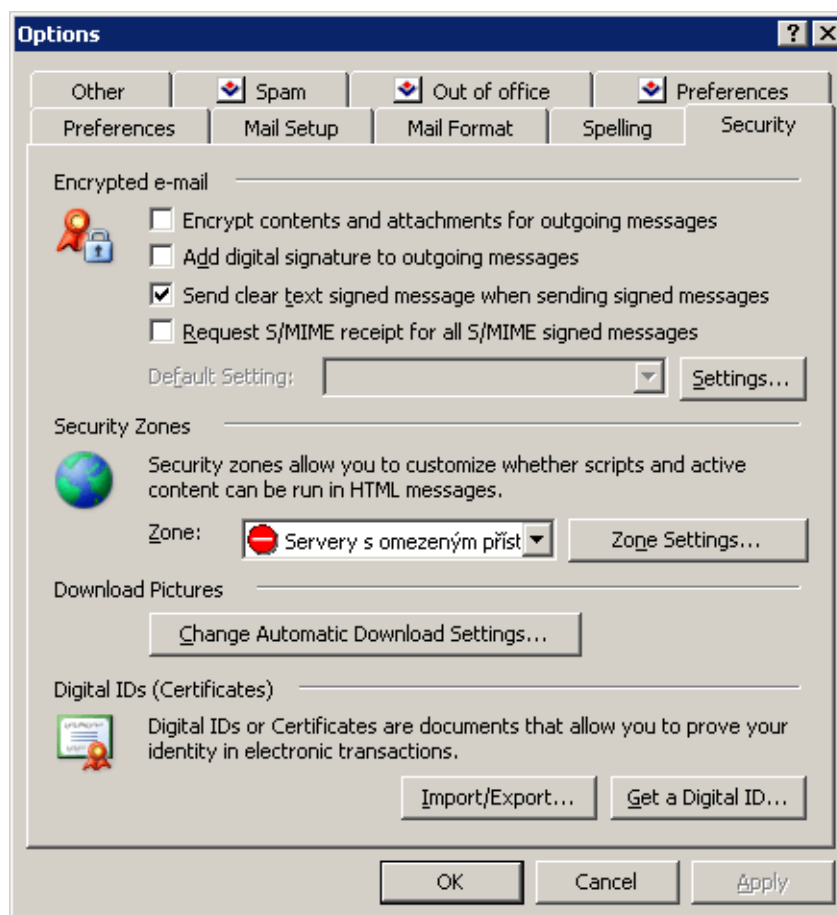


Figure 31.14 Settings of verification of signed messages

31.8 Kerio Outlook Connector and Kerio Synchronization Plug-in

This section provides a solution for the case when users need to use groupware features of *Kerio Outlook Connector* and work in the offline mode at the same time.

Kerio Outlook Connector itself does not allow working in the offline mode. However, it is possible to use *Kerio Synchronization Plug-in*.

Kerio Synchronization Plug-in is an extension for *MS Outlook* that enables using of some groupware features in POP3 and IMAP accounts as well as working in the offline mode. For more information about *Kerio Synchronization Plug-in*, refer to chapter 32.

Follow these instructions to make it possible to use both products in one *MS Outlook*:

1. Two profiles must be created in *MS Outlook* (see chapter 31.2).

TIP: When defining profiles, do not forget to set that the list of profiles is opened upon each startup of *MS Outlook* (see figure 31.15).

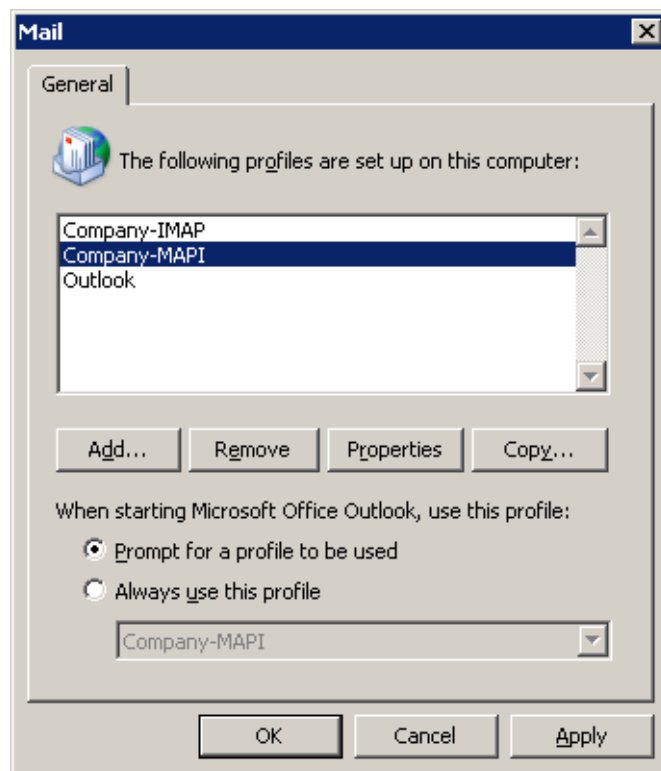


Figure 31.15 Setting the profile list

2. Install the *Kerio Outlook Connector* in one profile and create a standard MAPI account there (for more information, see chapter 31.2).
3. In the other profile, create a standard IMAP account first that will connect to the same account as the MAPI account created in the previous step.

Install the *Kerio Synchronization Plug-in* in this profile. If both accounts are configured properly, all groupware features of a MAPI account are available online in the first profile and the other profile with *Kerio Synchronization Plug-in* can be used for working in the offline mode while working in the IMAP account. The IMAP account will be synchronized with the data at the server using the parameters set (see chapter 32.2).

31.9 Sharing and Mapping in MS Outlook

Kerio MailServer enables creating of shared folders and their mapping. A shared folder is any folder of any user who has decided to share it with other users (or groups of users) and grant specific rights to them. Mapping is subscription of shared folders by users with appropriate rights.

Here is an example for better understanding of the issue:

There are two invoice clerks in a company. Both accept orders by email, so they use special email folders for these orders. If any of them goes for vacations or has to stay at home for any reasons, the other one needs to access her order folders.

The clerks both need rights to access the work folders of each other. This can be enabled by sharing of the folders. They simply select folders to share and set access rights for the other user (the other clerk).

If the user rights are set correctly, we can start the mapping. Mapping is always performed by the user with whom the particular folder was shared. The user simply opens a corresponding dialog in *MS Outlook* where she specifies her name. The shared folder then appears in the user's folder tree.

It only depends on the access rights assigned to the folder. Mapped folders can be available:

- for reading only,
- for reading and writing,
- for administration purposes.

Folder Sharing

In *MS Outlook* with the *Kerio Outlook Connector*, folders can be shared in *Properties* dialog window of the particular folder. To open the *Properties* window, right-click on a corresponding folder. This opens the context menu, where the *Properties* option is included. In the dialog, use the *Sharing and Security* tab to set sharing preferences.

The *Sharing and Security* tab allows users to share a particular folder with other users and set their user rights.

The *Add* button opens a window where a user or a group of users for sharing can be added. To select a user from the address book, click the *Address Book* button.

Click *Remove* to remove an individual user or a group of users and disable sharing.

Permissions for a specific user can be set in the menu under the user list:

- *Admin* — users with this level of rights can share a specific folder with other users. and remove items in the group or the group itself. This user is not allowed only to remove access rights for the user who created the group.
- *Editor* — the user can edit items in the folder (add and remove items, etc.).

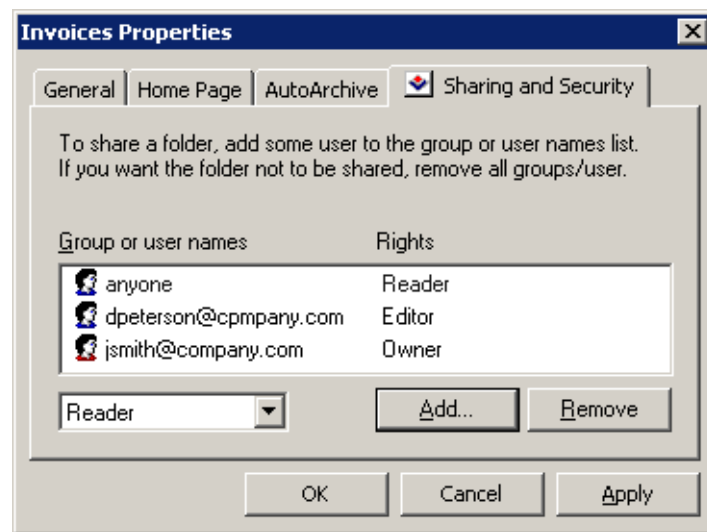


Figure 31.16 Folder Sharing

- *Reader* — the user is allowed only to read the folder's items. No editing is allowed.

When setting the access rights, the special *anyone* or *authuser* user accounts can be used. This way, the access rights can be granted to all (or logged) users.

Shared folder mapping

Folder mapping is used for connecting the shared folders of other users. Use the *Options* dialog of the root folder (right-click the *Kerio Outlook Connector Store* root folder and select *Properties for Kerio Outlook Connector*).

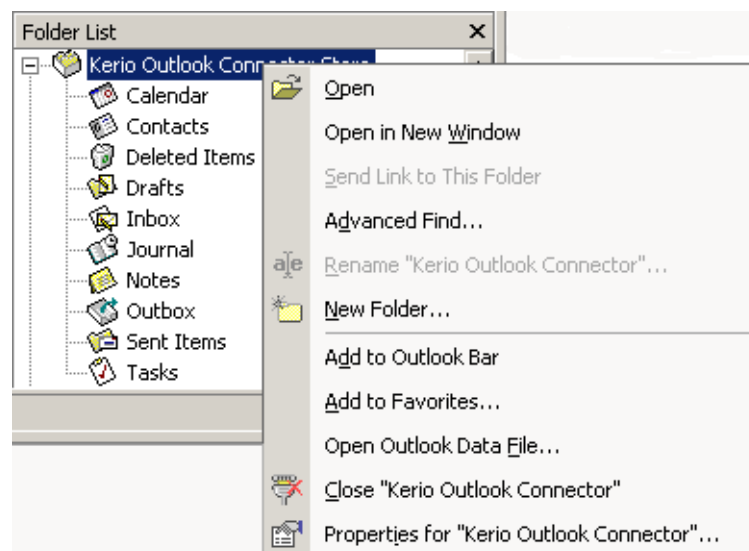


Figure 31.17 Context menu of the root folder

Use the *Folder mapping* tab to connect shared folders of a selected user. In the *Mapping name* textbox, the email address of the folder's owner is specified as *~owner@company.com*. If one or more folders are shared by the owner, these folders will be displayed in the *Folder* menu. To confirm the connection, click the *Add* button next to the list of folders. If the folder was connected properly, it appears in the list of mapped folders in lower part of the window. From here, the folders can be removed using the *Remove* button.

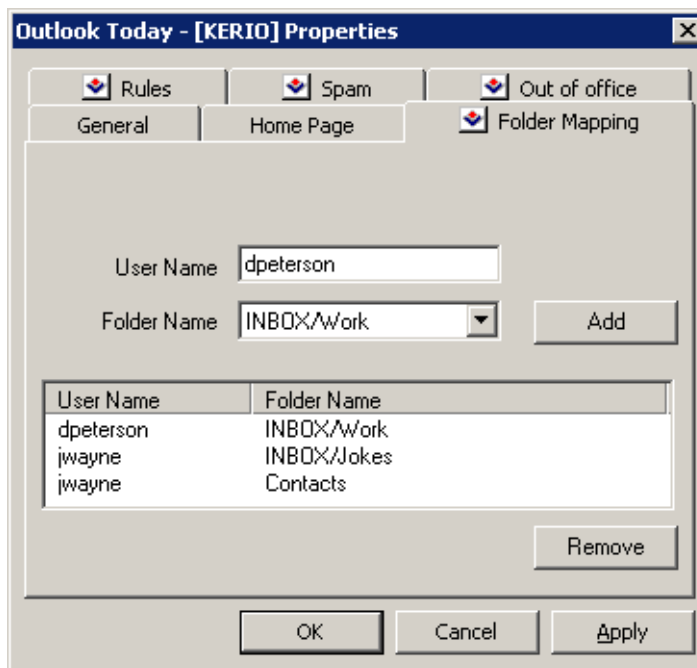


Figure 31.18 Folder mapping

Public folders are mapped to all users automatically.

31.10 Public and archive folders

Public folders

Public folders can be created only by users with appropriate access rights. By default, these rights are assigned to the admin of the *Kerio MailServer's* primary domain. The Admin can optionally assign administration rights to other users (for more information, see chapter 14.1).

To create a public folder, simply right-click the *Public folders* folder and select *New folder* in the pop-up menu. Specify the folder name and type in the corresponding fields of the dialog box that appears.

It is also necessary to set the user rights for all users that will access the public folder. The rights are added the same way as in case of sharing.

Public folders will be shared automatically with all selected users as subfolders of *Public folders*.

Archive folders

These folders are available to users with corresponding rights only. By default, only the admin of the primary domain is allowed to access the folders (the first account created in the configuration wizard during the installation of *Kerio MailServer*).

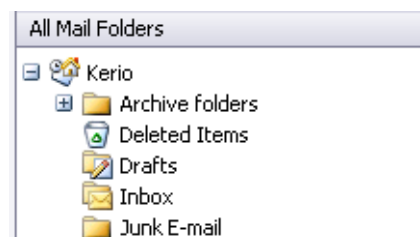


Figure 31.19 Archive folders

Archive folders can also be made available for other users. The sharing process is the same as for other folders (for description, refer to chapter 31.9). However, since messages of all users are archived, only a confidential administrator (or a tiny group of confidential persons) should be allowed to access these folders.

31.11 Rules for incoming messages

Rules for sorting and filtering mail at the server can be defined using *Kerio Outlook Connector* (the same rules that can be defined in the *Kerio WebMail* interface).

Warning: After installation of the *Kerio Outlook Connector*, the standard *MS Outlook*'s dialog for administration of rules for incoming mail and alerts *Rules and alerts* (*Tools* → *Rules and alerts*).

Use the root folder options dialog to create rules for incoming messages (right-click the *Kerio Outlook Connector* root's → *Kerio Outlook Connector Properties* folder).

The dialog includes rules defined. You can enable or disable rules using appropriate matching fields. Mark any rule to view detailed information about this rule in the *Rule description* window.

Rules are tested from the top downwards. You can use the *Up* and *Down* buttons to move rules within the list.

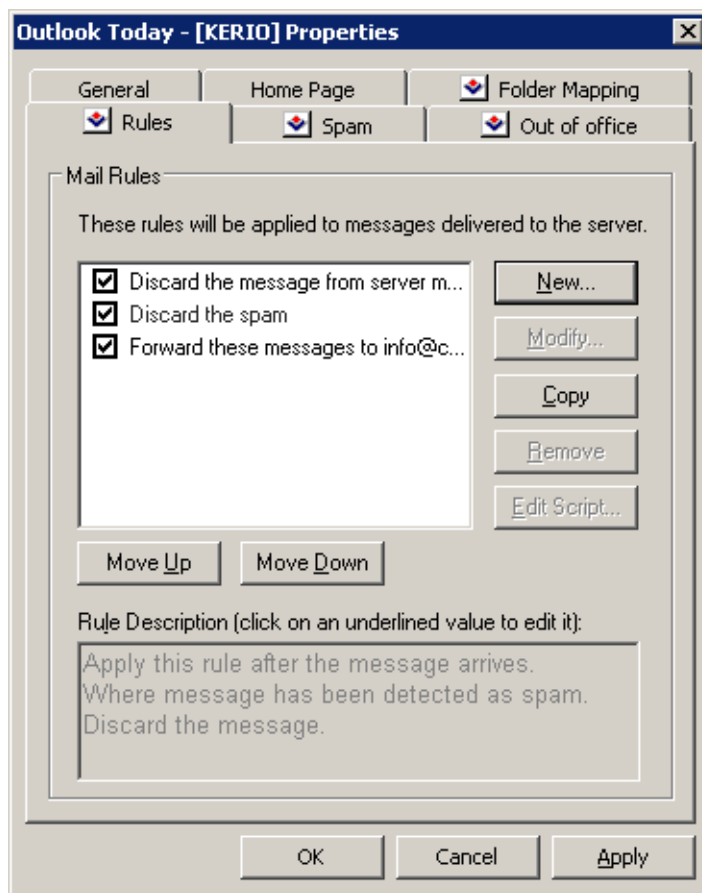


Figure 31.20 Rules for incoming messages

The following buttons and functions are available:

- *New* — creates a new rule (see below).
- *Modify* — edits selected rule (see below).

- *Copy* — copies an existing rule. This rule must be renamed. This function can be useful when you intend to create a new rule that differs only in a few parameters from the selected rule.
- *Remove* — removes the selected rule.
- *Edit* — edits the rule source using the *Sieve* code (standard code used for sorting rules descriptions). We recommend you not to use this function unless you are experienced in the *Sieve* code.

Creating or changing a rule

Use the *New* or the *Modify* button to open the *Rule Editor* dialog which includes the following sections:

Rule Editor ? X

Select your Conditions and Actions first, then specify the values in the Description.

1. Select the Conditions for your rule:

- ☐ Where the recipient (To or Cc) line contains address
- ☒ Where the From line contains address
- ☐ Where the To line contains address
- ☐ Where the Cc line contains address

2. Select the Actions for your rule:

- ☐ Reject message (return to sender)
- ☐ Keep in INBOX
- ☒ Discard the message
- ☐ Send notification

3. Rule Description (click on an underlined value to edit it):

Apply this rule after the message arrives.
Where the From line contains 'spam.cz'
Discard the message

4. Name of the rule:

Discard the message from server spam.cz

OK Cancel

Figure 31.21 Rule Editor

1. *Select the conditions for your rule* — conditions that must be kept so as the email administration meets this rule. One or more conditions from this list can be selected:

Where the recipient (To or Cc) line contains address

The To or the Cc (Copy To) entry includes defined string.

Where the From line contains address

The From entry contains the string.

Where the To line contains address

The To entry contains the string.

Where the Cc line contains address

The Cc (Copy To) entry contains the string.

Where the Sender line contains address

The Sender entry includes the string. This entry is often contained in messages sent automatically (mailing lists, etc.) where it stands for the From entry.

Where the Subject contains specific words

The Subject entry contains defined string(s).

Kerio MailServer spam filter can be set so that the Subject entry will include results of antispam tests (the value is represented by asterisks). Using this feature spam may be filtered easily. Simply insert the number of asterisks that will specify the rule. Messages that match this rule will accept this specification.

Where the message has an attachment

At least one attachment must be appended to the message.

Where the message size is more than size

The message size exceeds the specified value. To specify the size you can select from the following units: bytes (*B*), kilobytes (*KB*) and megabytes (*MB*).

Where the message was detected as a spam

Spam are undesirable messages sent to users. You can use the *Kerio MailServer* antispam filter to protect your users from such messages. *Kerio MailServer* spam filter uses special header items that include evaluation and information on antispam tests applied on the particular message (refer to chapter 17).

For all messages

This rule is valid for all incoming messages.

2. *Select the Actions for your rule* — select an action that will be taken for messages matching with condition in section 1

Move the message to a specified folder

Move the message to the selected folder (you can choose a folder from a list). You can also specify shared or public folders in one of the following forms: ~user/shared_folder or #public/public_folder if the appropriate user has write rights for this folder.

Forward the message to an address

Forward to a specified address. In this case no other actions are performed.

Reject message (return to sender)

The message will not be stored in a local mailbox and the user will never be informed about it.

Keep in Inbox

This action must be combined with another (i.e. with *Move*, *Forward*, *Reject*, etc.). It cannot be combined with the *Discard the message* action.

Discard the message

The message will not be stored in any local folder. This action cannot be combined with the *Keep in INBOX* action.

Send notification

Sends notification (i.e. a short text message) to a specified address, typically to a cellular phone. It is necessary to define even cellular phones by email addresses, for example john.blumonday@t-mobile.com.

The following macros can be used in the message text:

- \$from\$ — the notification will show the message sender or the address contained in the *From* field.
- \$from-name\$ — the notification will show the name of the message sender.
- \$subject\$ — the notification will show the message subject.
- \$text\$ — the notification will show the message text. Only the first 128 characters will be displayed. To reduce the number of displayed characters, edit the macro as follows: \$text[50]\$ (the number in brackets represents the maximum number of characters displayed in the notification).

Note: Notifications are sent in the plain text format (ASCII characters only). All regional characters in the text will be skipped.

Send autoreply

The automatic reply with a specified text. The automatic reply will be sent to each sender's address only once a week (so that the automatic reply does not create a loop in case there is an automatic reply set at the other end).

Stop processing more rules

If the message complies with this rule, no more rules will be processed. Using this function a user can create more complex rule systems for individual condition types. Rules are tested rule by rule from the top downwards.

Note: Notifications and autoreplies are protected against looping. This means that the system does not send a notification in reply to received notification or automatic replies. The detection of notification or automatic replies is performed using special items in the message header. Only notifications and automatic replies generated by *Kerio MailServer* are detected.

3. *Rule description* — description of the rule function (it is generated automatically according to the rule definition). Highlighted entries are interactive — click them to set other parameters.

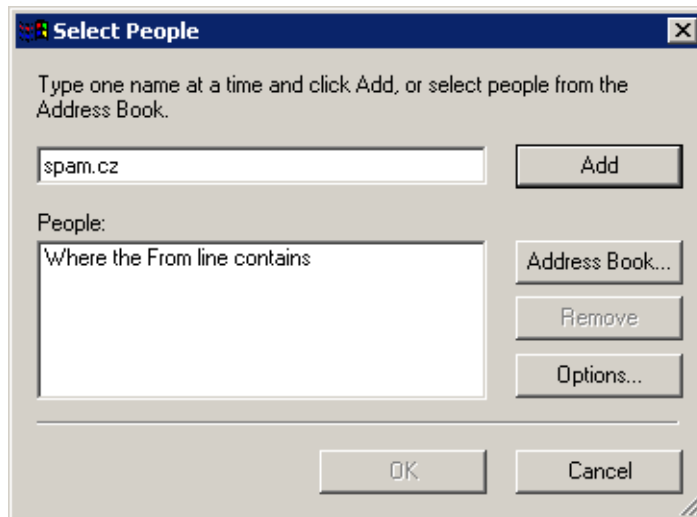


Figure 31.22 Select People

Click on the *Options* button to open the *Rule Condition Options* dialog — see above.

is

The entry must exactly match with the specification.

is not

The entry must not match with the specification.

contains

The entry must contain the (sub)string.

does not contain

The entry must not contain the the specified (sub)string.

matches

The entry must match the expression (the expression can contain the ? and * wildcards that can represent one or more characters).

does not match

The entry must not match the expression.

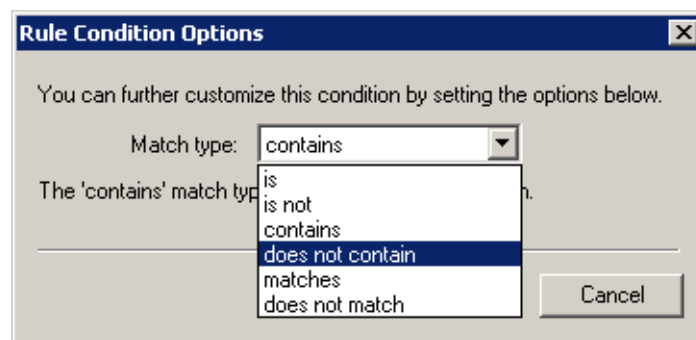


Figure 31.23 Rule Condition Options

Note: If more than one condition is defined, an appropriate logical operator must be used (*and* — both conditions must be met, *or* — at least one of the conditions must be met).

Example: You intend to create a rule that would drop all messages incoming from the *spam.com* domain which often sends undesirable messages (spam).

1. Select the *Where the line From contains* condition in the first dialog section.
2. Select the *Discard the message* option in the second section.
3. Select the *contains* option in the third section and specify the domain name (*spam.com*).
4. Enter a name for the rule (i.e. *Drop all messages from the spam.com domain*).

Out of office

A special sieve rule for automatic replies can be set on the *Out Of Office* tab in *Tools* → *Options*. This rule can be used when a user is not available in the office for a certain time. Enable the rule and specify the message that will be used as an automatic reply.

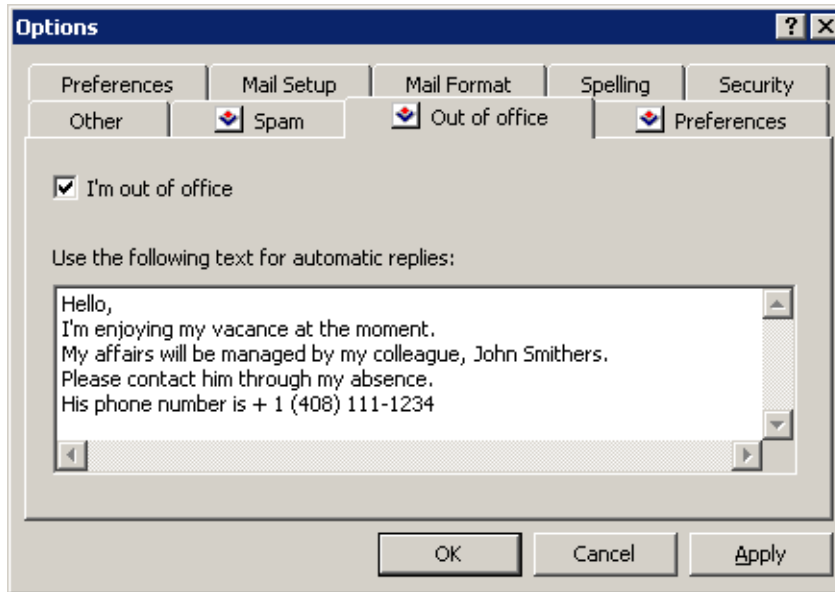


Figure 31.24 The Out of office tab

Note: The *I'm out of office* rule beats the rules for incoming messages (see chapter 31.11). If the filter includes a rule which sends automatic replies, the action set in this rule will not be taken.

The *I'm out of office* rule consists of the following items:

- *Condition:* The rule will be applied to all incoming messages.
- *Action:* The text entered will be sent to each sender's address included in an incoming message only once a seven days. This restriction is applied because some users can be subscribed to multiple mailing lists. If the reply was sent every time a message to the board is delivered, the mailing list's moderator might forbid the user access the mailing list.

31.12 Spam filter

Kerio MailServer includes the *SpamEliminator* antispam filter. For more information, see chapter 17. *SpamEliminator* is based on content analysis (spam messages usually contain specific attributes that can be searched for and evaluated by the filter). Each message is assigned a numeric score; if this value exceeds the limit set in *Kerio MailServer*, the message is marked as spam.

The spam filter may let some spam messages through from time to time by mistake (their score is low) and mark some regular messages as spam (their score is too high). For the reasons above, the antispam filter allows modification to the database used for

recognition of spam messages. This method, however, requires user input. Users have to reassign the incorrectly evaluated messages to correct types (spam / non-spam) so that the filter learns to recognize them in the future.

Kerio Outlook Connector uses the *Spam* and *Not spam* buttons located in the toolbar to mark the messages correctly. Highlight the incorrectly marked message and click one of the buttons. The filter updates the database (after a certain number of incorrectly marked messages) and the probability of incorrect evaluation decreases.

You can add the *Spam* and *Not spam* buttons to the toolbar in *Tools* → *Customize* menu or remove them. The *Toolbars* tab includes the *Kerio Outlook Connector* option. Simply select or unselect it by clicking to enable/disable the bar with the buttons.

The *Spam* button displays a warning message by default. To treat the message as spam and discard it, a confirmation is required. Use the *Tools* → *Options* menu on the *Spam* tab (see figure 31.25) to enable/disable displaying of the warning message.

Warning: If the *Spam/Not Spam* buttons are not available after installation or startup of *MS Outlook*, it is necessary to remove *Kerio Outlook Connector* from all forbidden items of *MS Outlook* (see chapter 31.5).

The Spam tab

The *Spam* tab provides several tools to fight spam:

Confirm marking mail message as spam

This option enables/disables alert window displayed upon clicking on the *Spam* button which is available in the toolbar.

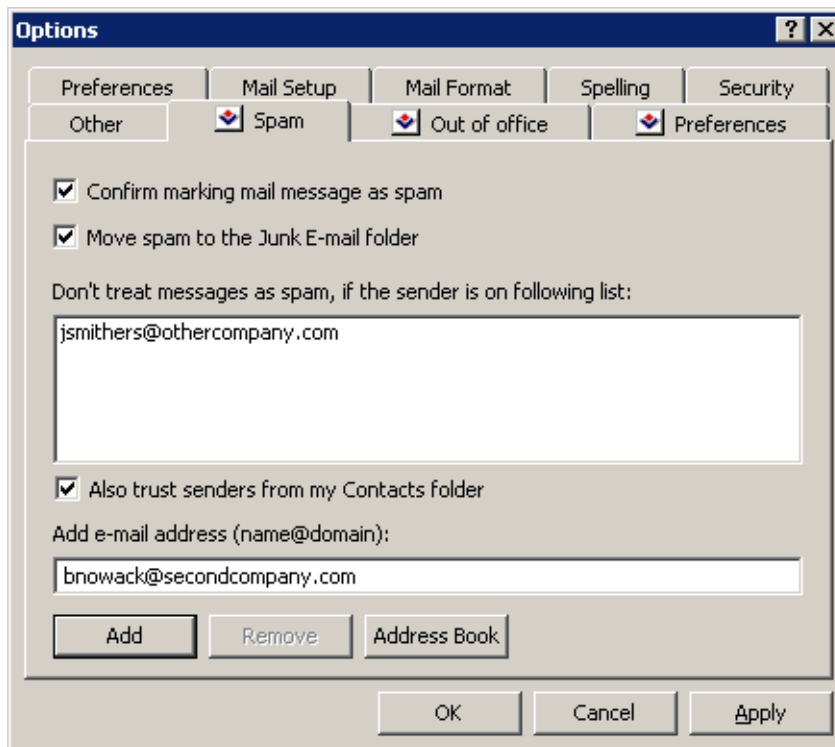


Figure 31.25 The Spam tab

Move spam to the Junk E-mail folder

If this option is enabled, all email considered as spam will be delivered to the *Spam* folder automatically.

Note: The *Move spam to the Junk E-mail folder* rule beats rules for incoming mail (see chapter 31.11). If the filter includes any rule which in any way handles messages marked as spam, the action set in this rule is ignored.

This option also enables adding email addresses to the list of trustworthy users (see below).

Also trust senders from ...

So called *Spam whitelist*. In this list, senders that will automatically be considered as non-spammers can be added/removed.

A new email address can be added in the *Add e-mail address* entry. This address must be specified in the `username@domain` format.

Also trust senders from my Contacts folder

If this option is enabled, messages marked as spam which were sent from addresses included in the main contact folder are not automatically moved to the *Spam* folder. This option supposes that email addresses in one's contact list are trustworthy. If this option is enabled, it is not necessary to include addresses saved in the contact list in the whitelist.

31.13 Searching contacts via the MAPI interface

MS Outlook extended by the *Kerio Outlook Connector* enables searching through contacts via the MAPI interface. This helps users search specific user information (usually email addresses) and it enables automatic completion of addresses while they are typed.

Automatic look-up in contacts makes available personal user contacts (i.e. contacts stored in user's personal contact folders) and contacts in all public and shared *Contacts* folders subscribed by the user.

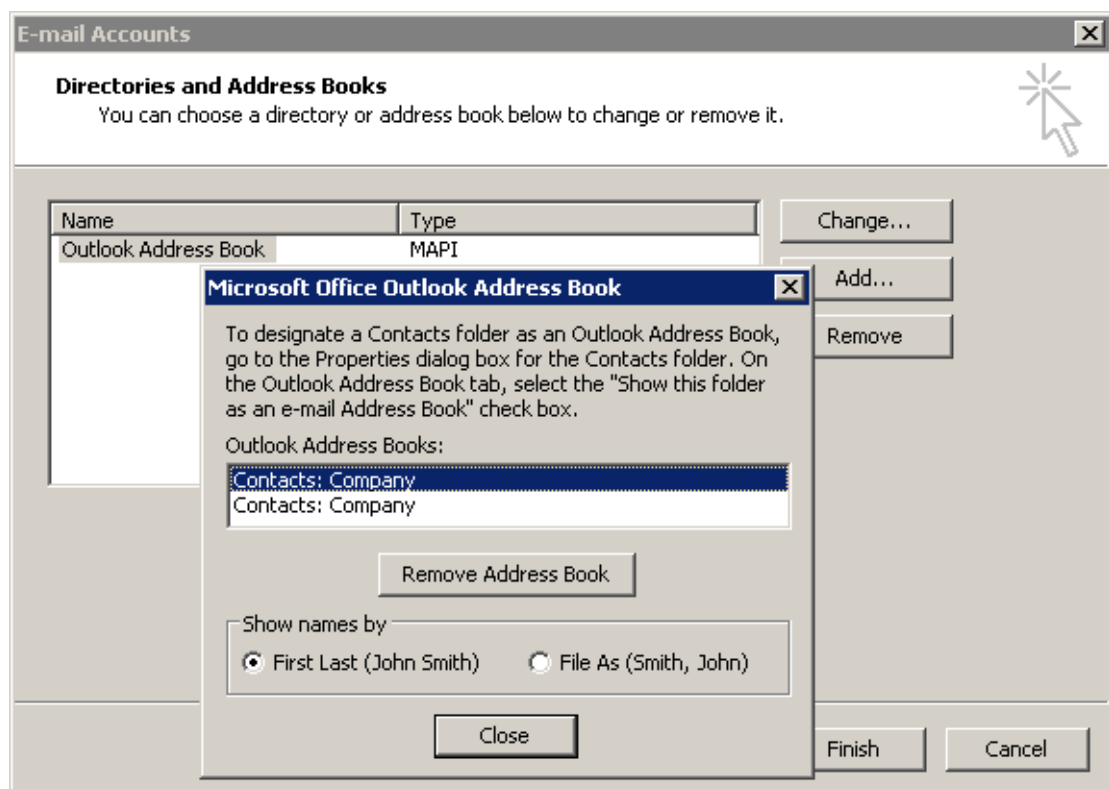


Figure 31.26 Directory management

By default, the automatic lookup is performed in contacts in the default directory of *MS Outlook* called *MS Outlook Address Book*. The address book can be handled in *Tools* → *E-mail accounts* → *View or change existing directories or address books*.

It is necessary to add to the *MS Outlook Address Book* any folders with contacts where lookup should be performed. Contact folders can be set as address books in properties of the selected contact folder on the *MS Outlook Address Book* tab (see figure 31.27).

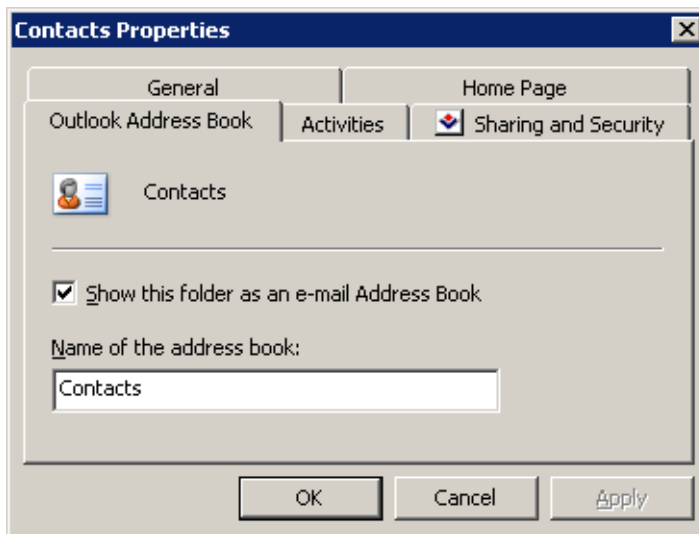


Figure 31.27 Show this folder as an e-mail Address Book

Warning: Searching criteria are first and second names. Do not use user names to look up a contact.

31.14 Error in settings of contact folders used as address books

During the startup process of *MS Outlook* extended with the *Kerio Outlook Connector*, a warning can be displayed that informs of an error detected in settings of contact folders which are used as address books (see figure 31.28).



Figure 31.28 Error in settings of contact folders used as address books

This error can be fixed by removing all address books in *MS Outlook*:

1. In the *Tools* menu, select *E-mail Accounts* to open a wizard where new accounts and address books can be created. In the wizard, select *View or change existing directories or address books*.
2. Remove all listed address books and close the wizard.
3. Restart *MS Outlook*.

Removing address books does not delete contact folders. All contacts are kept intact. Once all address books are removed from *MS Outlook* and the application is restarted, it is possible and recommended to add the address books again (for details, see chapter 31.13).

31.15 Contacts forwarding

It is recommended to forward the contacts in the vCard format (*Actions* → *Forward as vCard*). When a contact is opened in a client application that supports vCard format (*Kerio WebMail*, *Mozilla Mail*, etc.), the received contact can be added to the contacts folder.

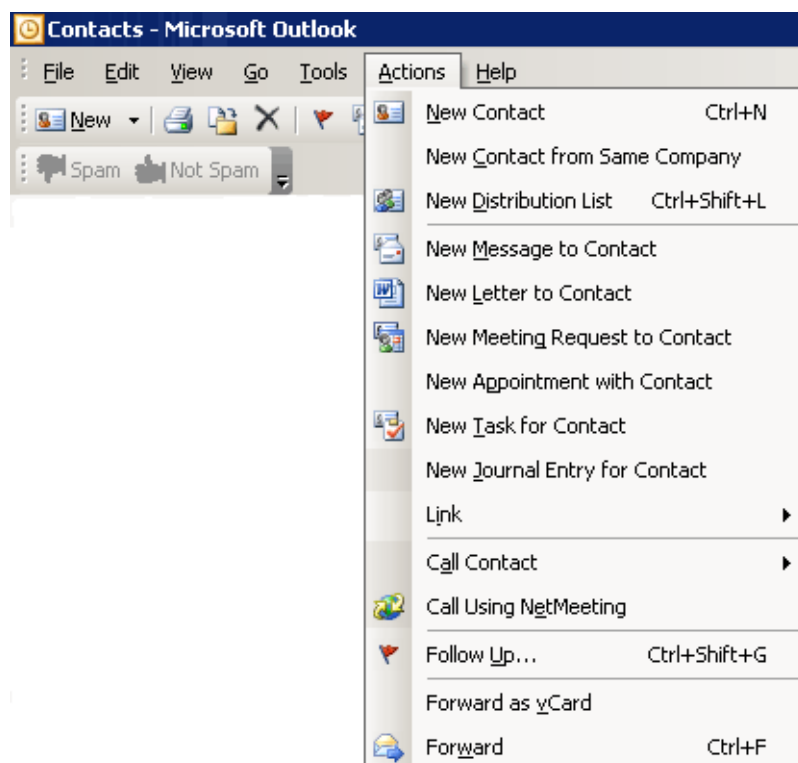


Figure 31.29 Forward as vCard

If *MS Outlook* receives a message with a contact in vCard format, the recipient can simply click the link in the message and the standard form for creating new messages is opened.

31.16 User login data

If a user password has been changed by an administrator in *Kerio MailServer*, it can be also changed in *MS Outlook*. The password can be changed directly in the account settings (click *Tools* → *Email accounts* → *View / change the email accounts*).

The password can be also changed in the *Login* dialog that is displayed in case the *Outlook* application fails to log in with the existing login and password.

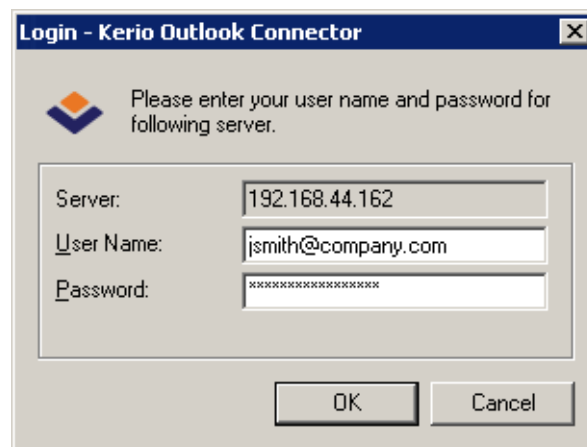


Figure 31.30 Login dialog

The dialog contains the following items:

Server

DNS or IP address of the computer that the user is logging to.

Username

Username including domain.

Password

A textbox for the new password.

31.17 Usage of the Free/Busy server

Free/Busy server is a public calendar that graphically displays the free/busy information for all users that have an account in *Kerio MailServer* and use the calendar in *MS Entourage* or *MS Outlook* (with the Kerio Outlook Connector installed).

The *Free/Busy* calendar does not display content of events, it only shows when the particular event takes place and whether a user is free or busy. Therefore, this calendar is

suitable for office purposes such as finding out whether people involved in a problem are free for a meeting. However, it is not possible to view also what the user is doing at a particular time. The only information that can be found is that the user is either busy or free at a particular moment.

This implies that this type of calendar is perfect for planning of meetings and sessions. The user who adds a new meeting can view when the people involved are free or busy. It is therefore not necessary to ask individual users when they are free. However, the following conditions must be met to enable this function:

- all users must have an account in *Kerio MailServer*,
- the users involved must use the calendar in *MS Entourage*, in *MS Outlook* (with the *Kerio Outlook Connector*) or in *Kerio WebMail* to handle their events.

The *Free/Busy* calendar displays all meetings and events included in the main calendar folder and its subfolders. If you want that some events (e.g. items of a private calendar) are not shown in the *Free/Busy* calendar, create a new calendar folder out of the branch of the main calendar and its subfolders.

The properties for *Free/Busy* server can be set in the *Tools* → *Options* menu in the *Preferences* tab. Click the *Calendar options* button to open a dialog. In this dialog, click the *Free/Busy Options* button.

The *Free/Busy Options* dialog contains information about the *Free/Busy* server. In order for the *Free/Busy* server to work properly, it is necessary to specify the URL address of the *Free/Busy* server in the *Search location* textbox (the last item in the dialog box) in the following format:

`http://212.56.22.12:port/freebusy/%SERVER%/%NAME%`

The mail domain and username of the meeting participant will be entered for %SERVER% and %NAME% values.

If the free/busy server is specified in the configuration, users can select the most convenient time for all participants of the scheduled meeting. The *Scheduling* tab lists all meeting participants (in the left section of the dialog box) along with their free/busy data. The different shades of blue or violet indicate the busyness of the users. The users with no data on the free/busy server (users with no account, users that do not use the calendar) are marked with grey.

Warning: It is necessary to specify each user by their usernames and domains (username@domain). Aliases cannot be used to display *Free/Busy* information.

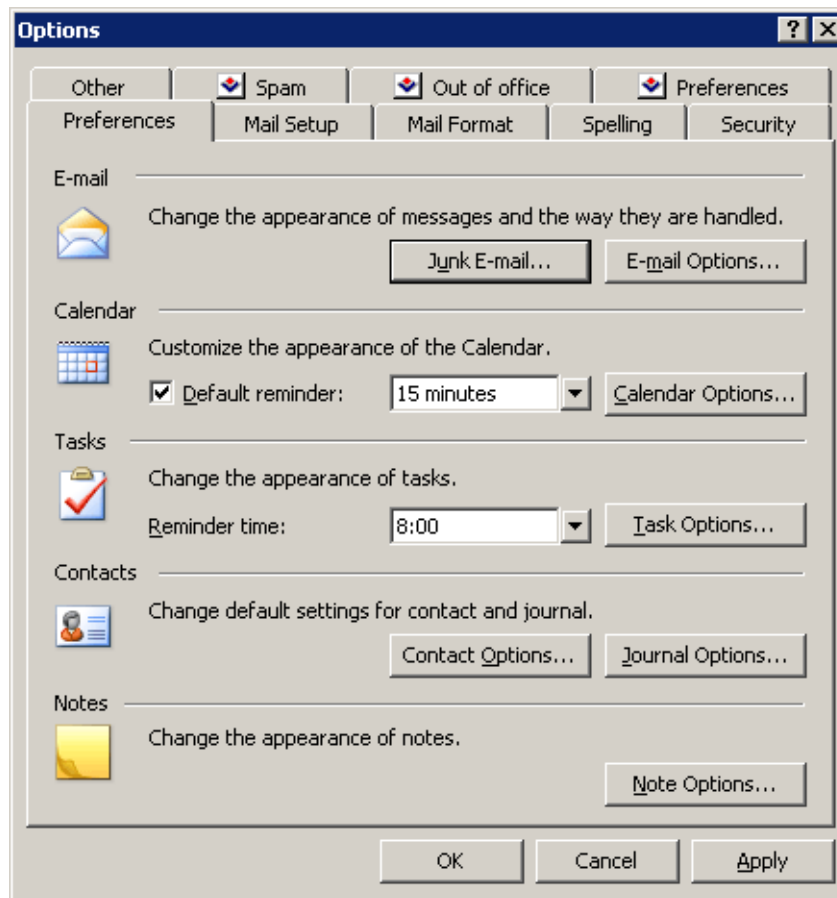


Figure 31.31 Free/Busy settings — preferences

The violet box in the schedule represents the time span of the scheduled meeting. It can be moved, extended or narrowed down using the cursor. The meeting start time is marked with green color, end time is marked with red.

Warning:

- For successful authentication to *Free/Busy* server, specify the *Subject* item in the *Appointment* tab.
- If only HTTPS traffic is allowed in *Kerio MailServer* (e.g. for security reasons), it is necessary that a trustworthy *Kerio MailServer* certificate is installed in *Internet Explorer* of the client station (a self-signed certificate can be used). Otherwise, new versions will not be updated automatically.

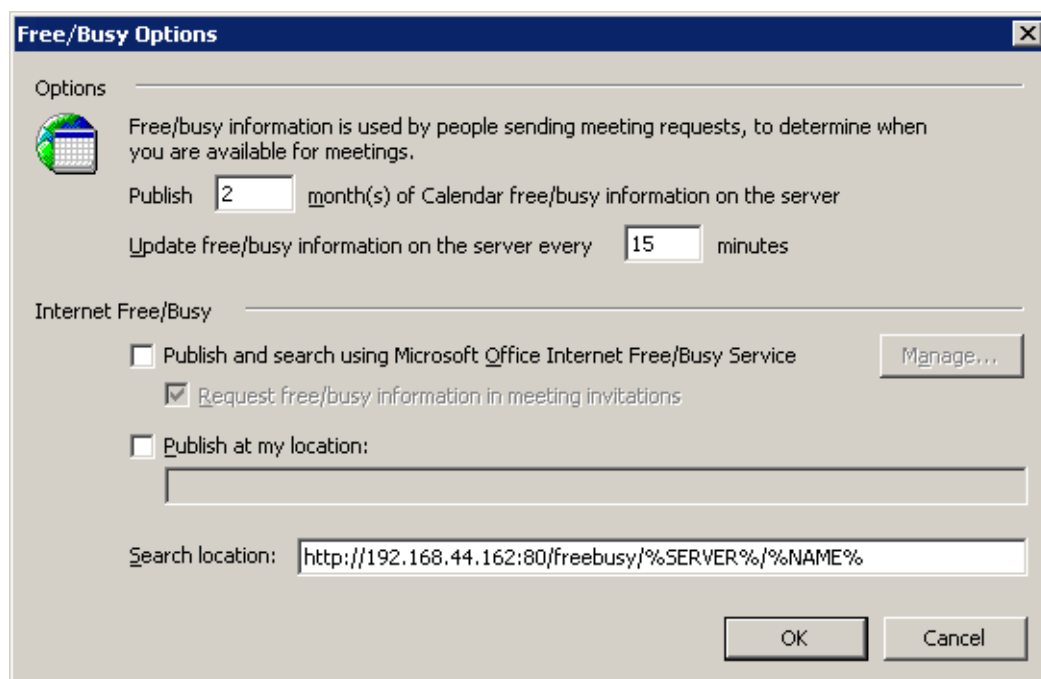


Figure 31.32 Free/Busy settings — options

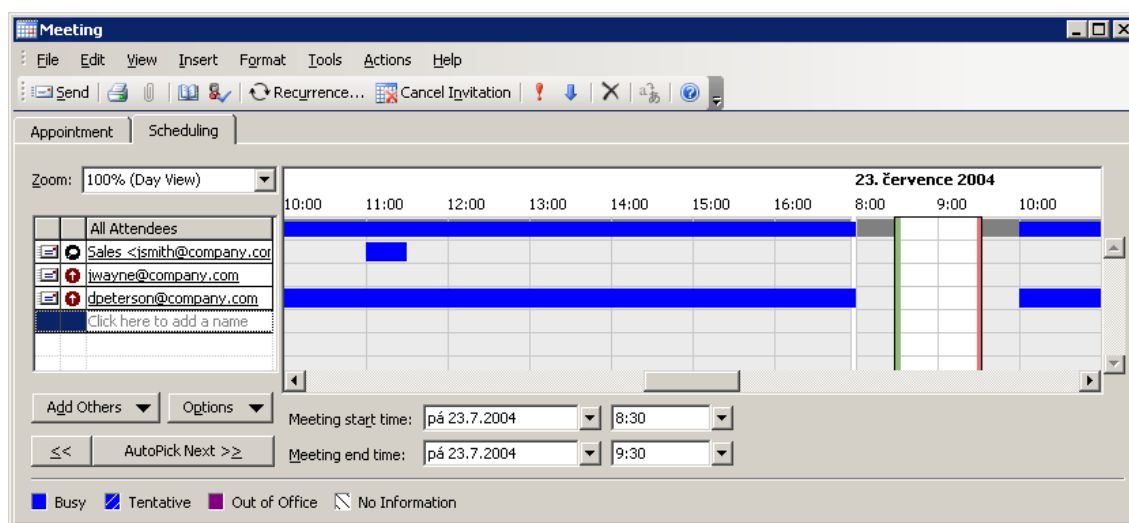


Figure 31.33 Usage of the Free/Busy calendar

Chapter 32

Kerio Synchronization Plug-in

Kerio Synchronization Plug-in is an extension to *MS Outlook* enabling basic groupware features (calendars and contacts) via IMAP or POP3. The *Kerio Synchronization Plug-in* was designed for users that travel frequently and need to have access to email, calendar, and contacts when internet access is not available. Besides that, the main benefit of the plug-in is the offline mode, where it is possible to switch to the online mode and connect to *Kerio MailServer* to synchronize changed data.

Kerio Synchronization Plug-in uses the SyncML protocol. SyncML is a versatile protocol used to synchronize data acquired at various types of devices, in any network and in any store. In *Kerio Synchronization Plug-in* it is based on the HTTP service.

Warning: *Kerio MailServer* supports synchronization by the SyncML protocol only for the client extension of *Kerio Synchronization Plug-in*.

For proper functionality of *Kerio Synchronization Plug-in*, the following services must be running in *Kerio MailServer*:

- *HTTP(S)* — the protocol is used for the synchronization as well as for automatic updates of the plug-in.
- *IMAP(S)* — for IMAP accounts, if used.
- *POP3(S)* — for POP3 accounts, if used.
- *SMTP(S)* — the protocol is used for email sending.

Kerio Synchronization Plug-in can be applied to the following versions of *MS Outlook*:

- MS Outlook 2000 + version Service Pack 3
- MS Outlook XP + version Service Pack 1
- MS Outlook 2003 + version Service Pack 1

Warning: It is not possible to use *Kerio Outlook Connector* and *Kerio Synchronization Plug-in* within the same profile. Both applications can be installed and used in one *MS Outlook*, however, they cannot be both used by one account simultaneously. *Kerio Synchronization Plug-in* can synchronize only with an IMAP or POP3 account. It is not possible to use it for synchronization of MAPI accounts.

TIP: If you want to use all groupware features provided by the *Kerio Outlook Connector* and to work in the mail client offline at the same time, we recommend to set *MS Outlook* as described in chapter [31.8](#).

32.1 Installation

A standard wizard is used for the *Kerio Synchronization Plug-in* installation.

If more than one user share one *MS Outlook* and they want to use *Kerio Synchronization Plug-in* for their accounts, the following conditions must be met:

1. each user uses a proper profile (in each profile, synchronization will be performed at one account),
2. each user installs the *Kerio Synchronization Plug-in* separately,
3. the first installation is performed under the local administrator's account,
4. each user has the "Power User" rights or at least each user is allowed to write in the directory where the *Kerio Synchronization Plug-in* is installed.

Warning:

- *MS Outlook* must be installed on the computer prior to the *Kerio Synchronization Plug-in* installation, otherwise the application will not function properly.
- If *MS Outlook* version is updated, *Kerio Synchronization Plug-in* must be reinstalled.

Automatic updates

Kerio Synchronization Plug-in is updated automatically and independently from users. Up-to-date versions of *Kerio Synchronization Plug-in* are checked by the *Kerio MailServer Engine*. Availability of new versions can be viewed in the administration console (the *Update Checker* tab in the *Advanced Options* section — see chapter 16.6).

New versions of *Kerio Synchronization Plug-in* are stored in the directory

Kerio\MailServer\webmail\download

32.2 Synchronization

Synchronization is performed in the main personal calendar folder and the main personal contacts folder only. Optionally, synchronization of the main public calendar/contacts folder can also be set.

Within synchronization, only changed and modified information is exchanged between the MailServer and *MS Outlook*. Objects changed both at the server and the client will be duplicated.

If the installation is completed successfully, the user is informed by an alert that *Kerio Synchronization Plug-in* must be set first:

The *Synchronize* menu is now provided in the toolbar. This menu contains the following items (see figure):

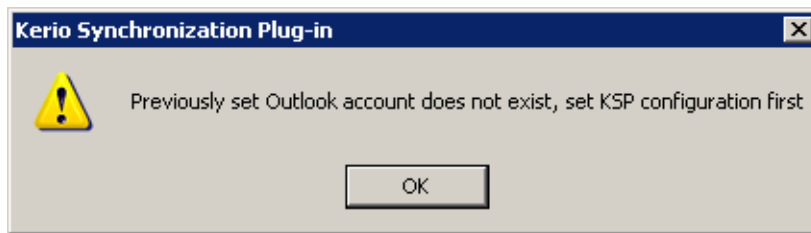


Figure 32.1 Running MS Outlook upon the plug-in installation

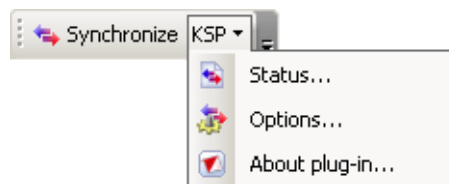


Figure 32.2 Toolbar

Status

This dialog includes logs providing synchronization process information. If the synchronization is completed successfully, details are provided for all folders synchronized including the information about which of folders were or were not synchronized successfully.

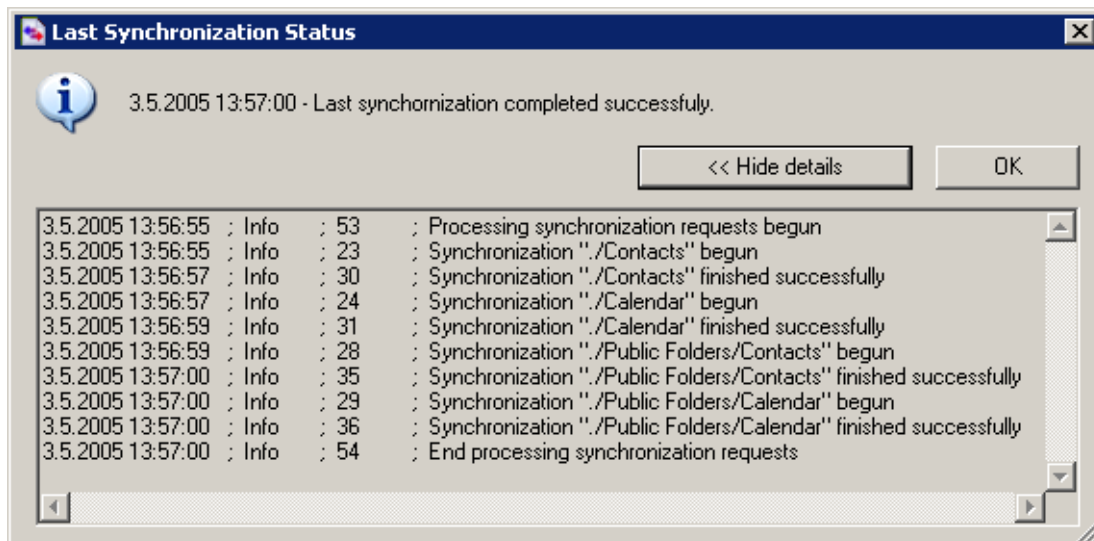


Figure 32.3 Synchronization status

It is recommended to check the log to see whether the synchronization was completed successfully.

Options

The following dialog can be used for settings:

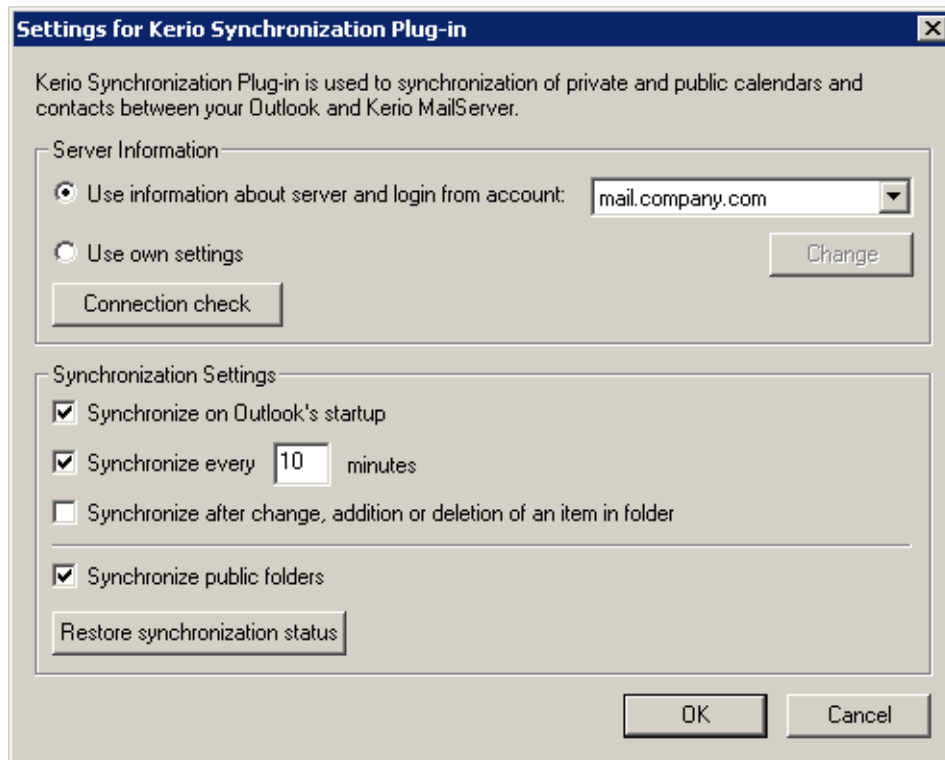


Figure 32.4 Synchronization settings

Use information about server ...

The plug-in in the combo box menu provides all IMAP and POP3 accounts in the current profile.

Use own settings

Click *Change* to open a dialog where parameters for a corresponding account can be set.

In addition to specification of server name, user name and user password, SPA (NTLM) authentication can be enabled through this dialog. If the option is enabled, the user will not be asked for username and password — instead, the authentication will be applied automatically. For smooth functionality of SPA authentication, it is necessary that the host and the user account belong to the domain where the user will be authenticated.

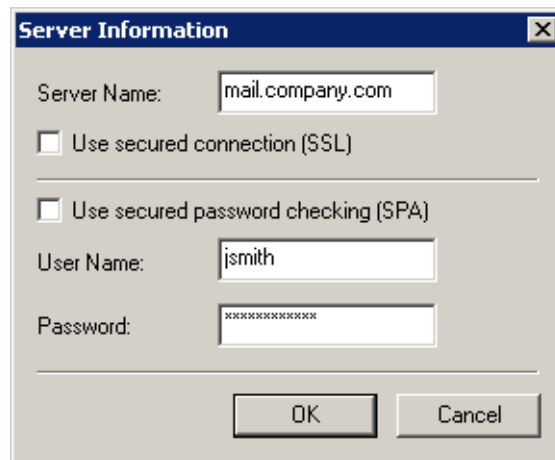


Figure 32.5 Manual account setting

Using the *Connection check* button you can easily check whether it is possible to connect to the server using the data specified.

The following options define when the synchronization is performed. Optionally, the criteria may be combined:

Synchronize on Outlook's startup

The synchronization is performed upon each startup of *MS Outlook*. If only this option is enabled, it is necessary to close and reopen the application when switching to the online mode to perform the synchronization. Therefore, it is recommended to combine this option with one or both of the following ones.

Synchronize every ... minutes

Interval that will be used for the regular synchronization.

Synchronize after change...

Synchronization will be performed upon any change, i.e. when a new item (contact, event) is added or another is removed.

It is not recommended to enable this option if the line used for connection to the network is not fast enough for frequent synchronization.

Kerio Synchronization Plug-in also allows synchronization of public folders. Only the main folders of calendars and contacts are synchronized.

Synchronize public folders

This option can be used to synchronize public folders.

The *Restore synchronization status* button performs synchronization with respect to the current status at the server. It is usually used when an event or a contact is modified in an undesirable way or removed.

Chapter 33

MS Entourage support

MS Entourage is a mail client for Mac OS X, supported by *Kerio MailServer*. This support uses the interface for *MS Exchange* in *Entourage* and it includes:

- support for groupware data such as mail, calendars, contacts and public folders
- *Free/Busy* server for meetings management
- connection of various LDAP databases for contact look-up
- learning of the Bayesian filter by moving folders to Junk E-mail or INBOX (for detailed information, see chapter 17.1).

Cooperation of *Kerio MailServer* with *MS Entourage* is supported directly. This means that no extension is required to be installed at client stations. It is only necessary to set correctly the basic parameters for an *Exchange* account.

For proper functionality of *Microsoft Entourage*, the following services must be running in *Kerio MailServer*:

- *HTTP(S)* — *Kerio MailServer* uses this service to communicate with the WebDAV interface and with the *Free/Busy* server.
- *LDAP(S)* — used for searching for contacts in the *Kerio MailServer*'s LDAP database.
- *SMTP(S)* — used for email sending (only for *MS Entourage X* and for IMAP and POP3 accounts in any version)
- *IMAP(S)* — this service must be running if *MS Entourage X* is used.

Kerio MailServer supports the following versions of the mail client:

- *MS Entourage X* for Mac OS X
- *MS Entourage 2004* and MS Office 2004 for Mac sp1 — 11.1.0 for Mac OS X
- *MS Entourage 2004* and MS Office 2004 for Mac sp2 — 11.2.1 for Mac OS X

MS Entourage must be installed on one of the following versions of Mac OS X:

- Mac OS X 10.2 jaguar
- Mac OS X 10.3 Panther
- Mac OS X 10.4 Tiger

Warning: Each user profile in *MS Entourage* can be used for an only *Exchange* account. Any other account will be dysfunctional. Functionality of POP3 and IMAP accounts is not affected by the account settings.

33.1 Initial settings

The settings differ according to what version of *MS Entourage* is used. For this reason, the settings will be described in three parts. First, setting of *MS Entourage* version X will be focused. Second, version 2004 will be described. Third, setting of version 2004 with Service Pack 2 will be focused.

These versions of *MS Entourage* use different methods of access to the server data. In *MS Entourage X*, messages are downloaded from server using the IMAP protocol and calendars with contacts are synchronized using WebDAV interface (Web Distributed Authoring and Versioning). *MS Entourage 2004* and higher uses WebDAV interface for downloading and sending of email messages as well.

Other differences are shown in table 33.1.

Character	MS Entourage X	MS Entourage 2004	MS Entourage 2004 sp2
Searching contacts via LDAP	YES	YES	YES
Free/Busy support	YES	YES	YES
Delegating folders	NO	YES	YES
Support for public folders with contacts and calendars	NO	NO	YES
Support for calendar and contact folders in a single account	NO	NO	YES

Table 33.1 Supported features

There are only minor differences as to setting up *Kerio MailServer* support for *MS Entourage*:

MS Entourage X

Entourage X is configured according to the fact whether it is installed for the first time or the application has already been used and a new email account is just being created.

The *Entourage Setup Assistant* is started upon a successful installation of the application (or when a new profile is to be created). The wizard requires basic user information and it is necessary to follow it up to step seven. In step seven, it is possible to say that the email account will be set later (*I will set up my e-mail account later*). The configuration is not standard so that the account must be set by hand. Therefore, close the wizard at this stage.

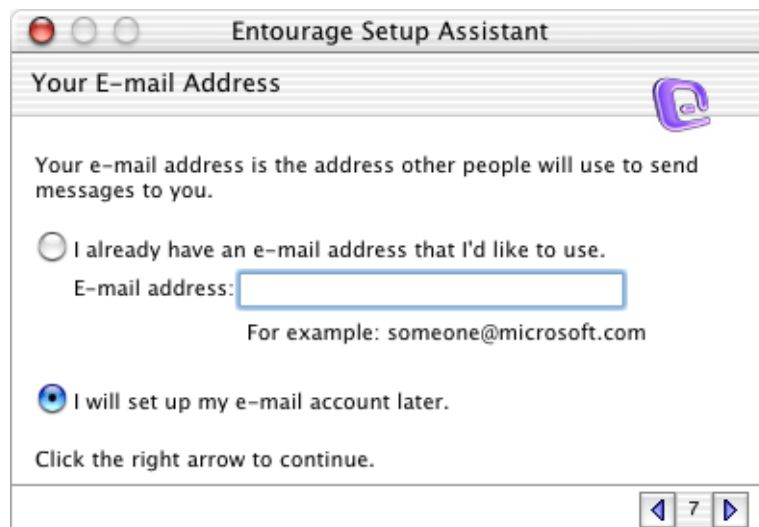


Figure 33.1 Entourage Setup Assistant

The following steps are identical for all users. To create an account, go to *Tools → Accounts*. The *Accounts* dialog which is divided into four tabs will be opened. In order for *MS Entourage* and *Kerio MailServer* to cooperate properly, a special account has to be created. Use the toolbar in *Tools → Accounts* menu. The *Accounts* window consists of several tabs. Use the *Exchange* tab to create the account. After selecting this tab, click the *New* button located in the toolbar above the tabs. In the *Edit Account* dialog box, click the *Configure account manually* button (located in the lower left part) and enter the parameters for the new account.

There are four tabs available in the *Edit Account* dialog box; it is necessary to specify the following parameters:

On the *Account Settings* tab, the username and MailServer are defined:

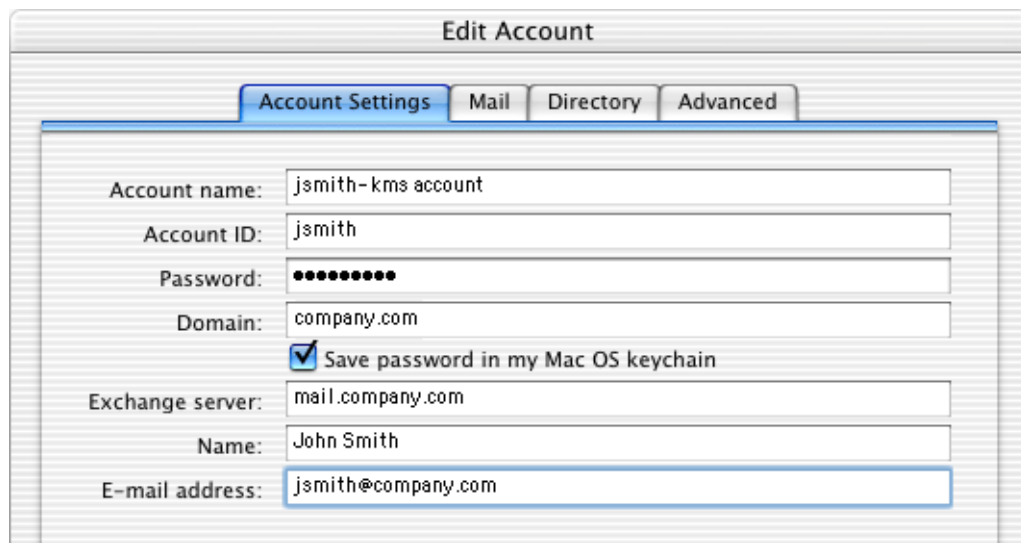


Figure 33.2 Manual account setting — basic settings

Account name

The name of the email account.

Account ID

Username used for login to *Kerio MailServer*. Username can be specified in two formats, either `user` or `user@domain`. If a user account is created in a domain which is not set as primary, use the `user@domain` pattern for specification of the username. Otherwise the user's attempts to connect to the LDAP database might fail.

Password

User password used in *Kerio MailServer*.

Domain

Name of the email domain where the user has an account.

Exchange server

DNS or IP address of the machine where *Kerio MailServer* is running.

Name

Any name (the first name and last name of the user is recommended) that will be displayed in the message header.

E-mail address

The email address of the user.

On the *Mail* tab, DNS name or IP address of the SMTP server (IP address of the computer where *Kerio MailServer* is running) is required.

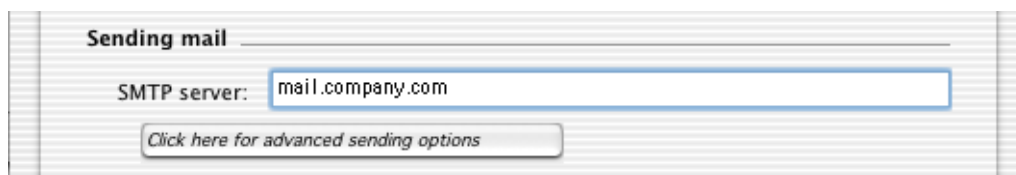


Figure 33.3 Manual account setting — SMTP server

To enable look-up in contacts using LDAP, specify the DNS name or IP address of the LDAP server on the *Directory* tab (usually *Kerio MailServer*).

Use the *Click here for advanced options* button. The *Override default LDAP port* option must be disabled (unchecked), otherwise searching in the LDAP database will not be functional.

Note: *MS Entourage* supports only the main private contact folder. it does not support displaying of the shared version and the public contact folder and it also does not support private contact subfolders created in *Kerio WebMail*. However you can add addresses from these other Contact folders through an LDAP search when creating a new email (see chapter 33.2).

On the *Advanced* tab, it is possible to enter a URL address to the *Free/Busy* server. The *Free/Busy* server is a public calendar that displays the free/busy data for all users that

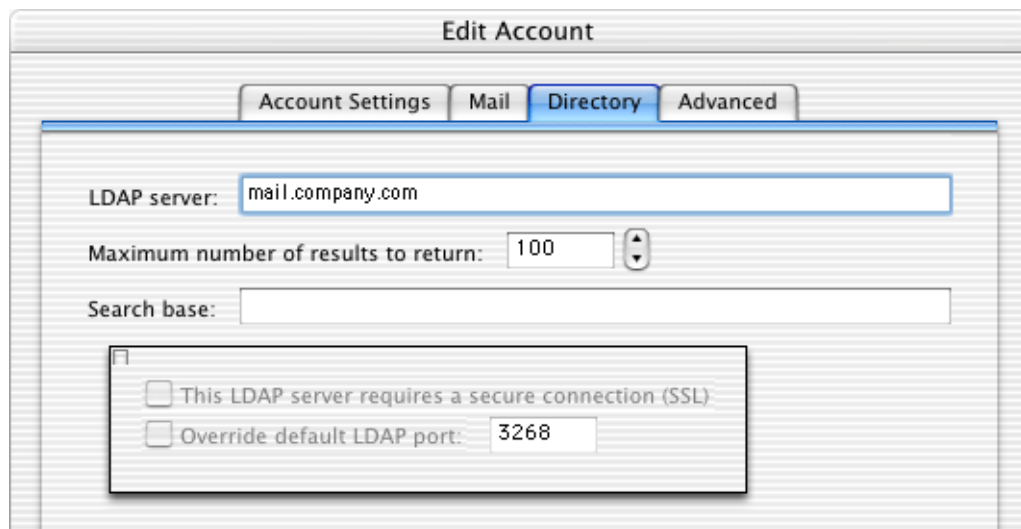


Figure 33.4 Manual account setting — LDAP server

have an account in *Kerio MailServer*, and work with the calendar in *MS Entourage*, in *MS Outlook* or in the *Kerio WebMail* interface. For details on usage of the *Free/Busy* feature, see chapter 33.3.

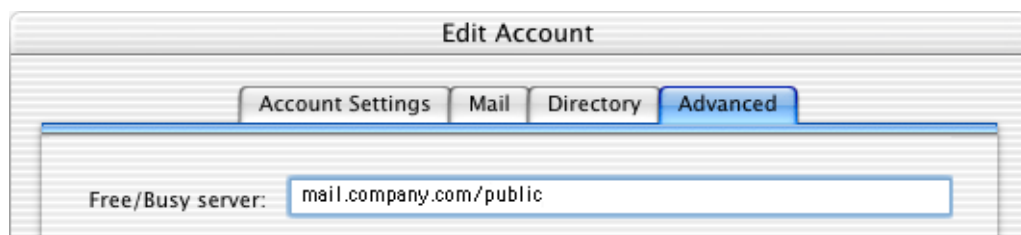


Figure 33.5 Manual account setting — Free/Busy server connection

If the *Free/Busy* server is enabled in the configuration of the corresponding account, the user can view free/busy state of all users while creating meetings.

MS Entourage 2004

Whenever a new profile is created or right upon a successful installation of the application, the *Entourage Setup Assistant* is started automatically. It is recommended not to use this wizard to create a KMS account.

To set the account in *MS Entourage*, use *Tools* → *Accounts* menu. On the *Exchange* tab. Click *New* to open the *Edit Account* dialog where parameters of the new account need to be specified manually by using the *Configure account manually* button.

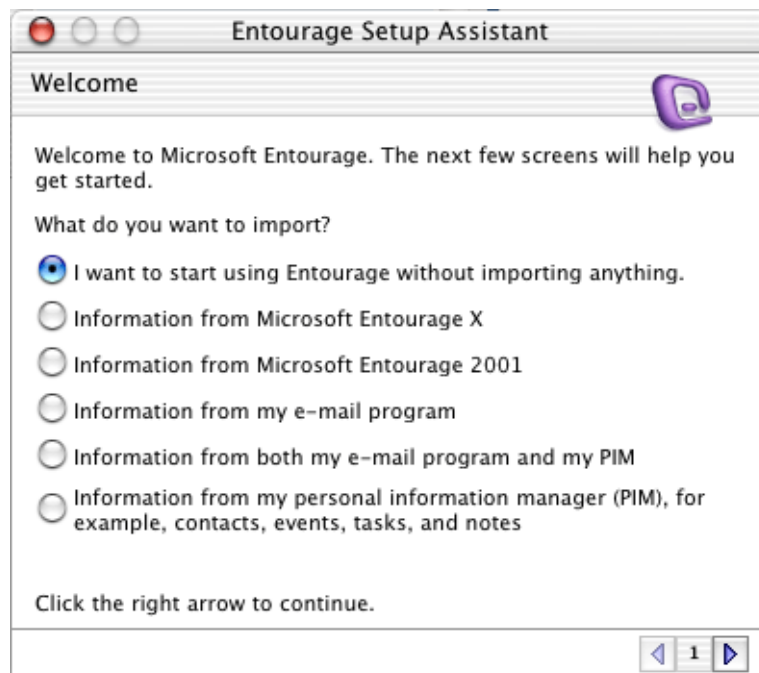


Figure 33.6 Entourage Setup Assistant

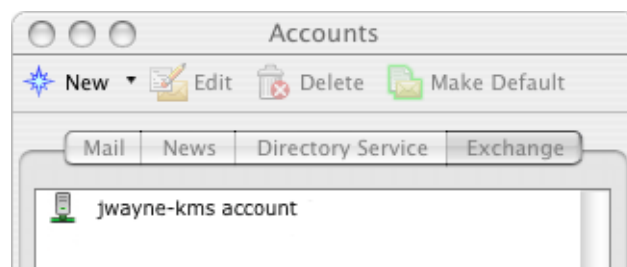


Figure 33.7 Accounts

There are several tabs available in the *Edit Account* window. Three tabs are used to specify the account settings:

On the *Account Settings* tab, the username and the server are defined:

Account name

The name of the email account.

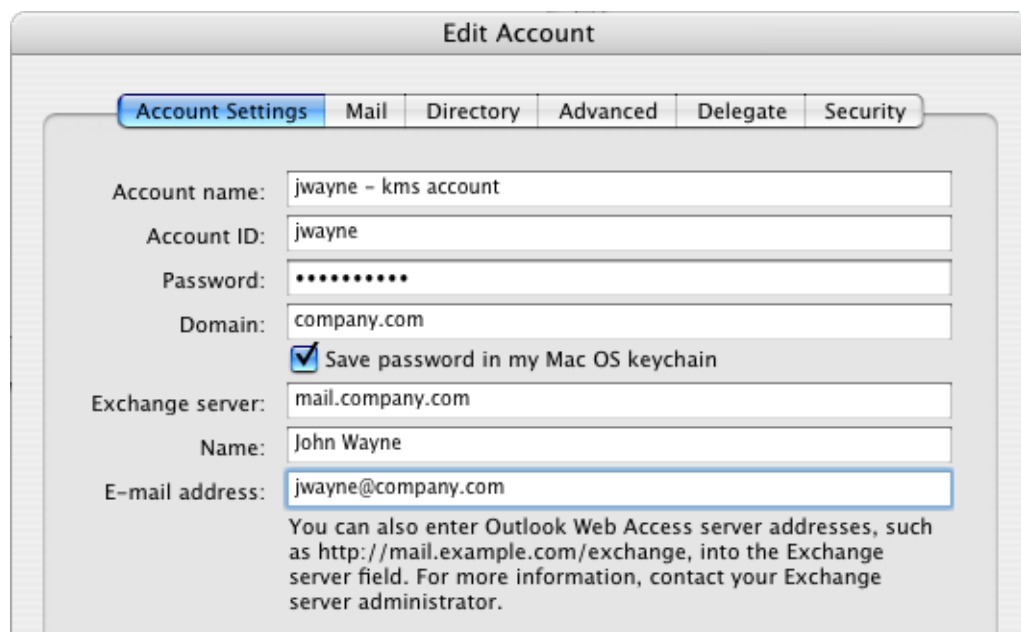


Figure 33.8 Manual account setting — basic settings

Account ID

Username used for login to *Kerio MailServer*. Username can be specified in two formats, either `user` or `user@domain`. If a user account is created in a domain which is not set as primary, use the `user@domain` pattern for specification of the username. Otherwise the user's attempts to connect to the LDAP database might fail.

Password

User password.

Domain

Name of the email domain where the user has an account.

Exchange server

DNS or IP address of the machine where *Kerio MailServer* is running.

Name

Any name (the first name and last name of the user is recommended) that will be displayed in the message header.

E-mail address

The email address of the user.

Specify the DNS name or IP address of the SMTP server on the *Directory* tab (usually your *Kerio MailServer*).

Use the *Click here for advanced options* button. The *Override default LDAP port* option must be disabled (unchecked), otherwise searching in the LDAP database will not be functional.

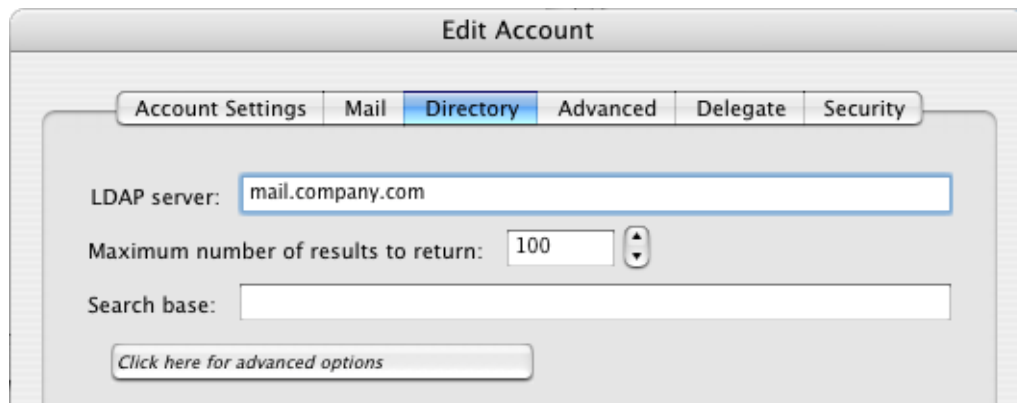


Figure 33.9 Manual account setting — LDAP server

Note: *MS Entourage* supports only the main private contact folder. It does not support for displaying of shared (unless delegation is set) and public contact folders nor it supports private contact subfolders created in *Kerio WebMail* (unless they are shared and connected by delegation). However you can add addresses from these other Contact folders through an LDAP search when creating a new email (see chapter 33.2).

On the *Advanced* tab, it is possible to enter a URL address to the *Free/Busy* server. The *Free/Busy* server is a public calendar that displays the free/busy data for all users that have an account in *Kerio MailServer*, and work with the calendar in *MS Entourage*, in *MS Outlook* or in the *Kerio WebMail* interface. For detailed information on usage of this feature, refer to chapter 33.3.

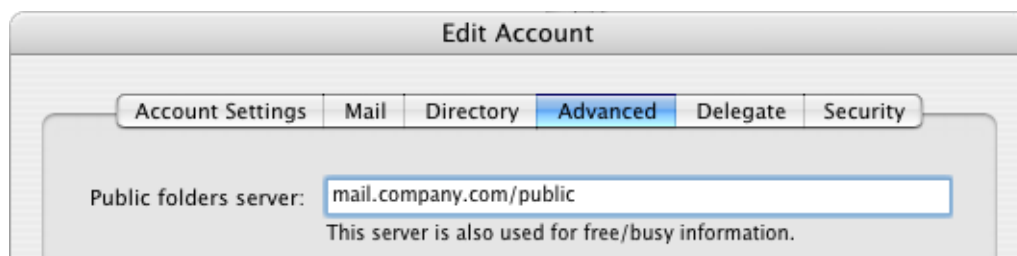


Figure 33.10 Manual account setting — Free/Busy server connection

MS Entourage 2004 sp2

Whenever a new profile is created or right upon a successful installation of the application, the *Entourage Setup Assistant* is started automatically. It is recommended not to use this wizard to create a KMS account.

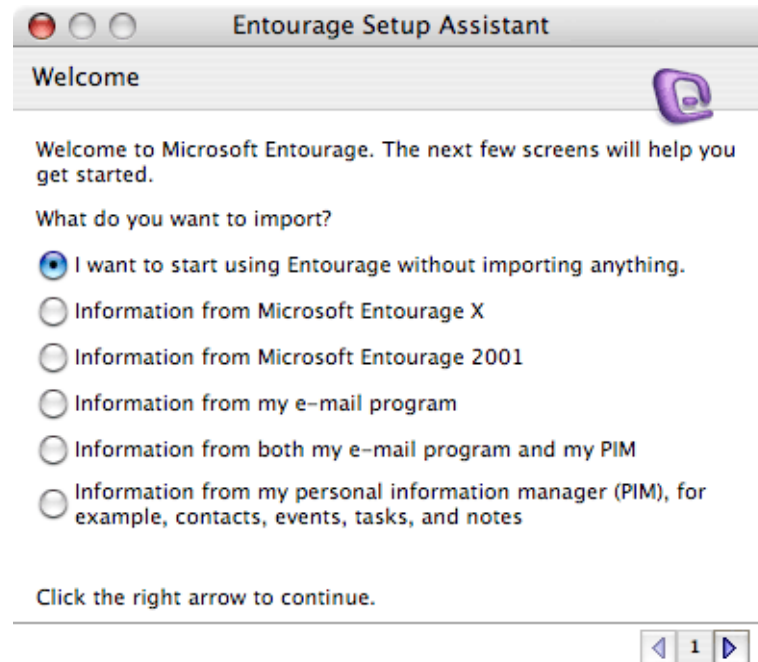


Figure 33.11 Entourage Setup Assistant

To set the account in *MS Entourage*, use *Tools* → *Accounts* menu (see figure 33.12). On the *Exchange* tab. Click *New* to open the *Edit Account* dialog where parameters of the new account need to be specified manually by using the *Configure account manually* button.

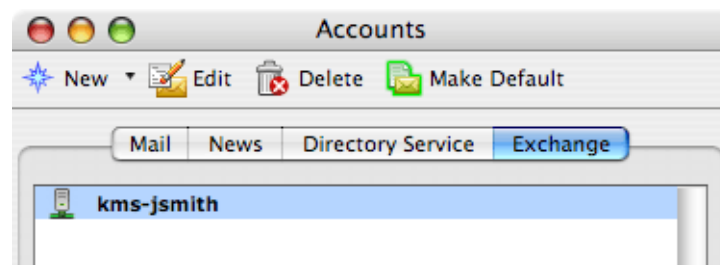


Figure 33.12 Accounts

There are several tabs available in the *Edit Account* window. Two tabs are used to specify the account settings:

On the *Account Settings* tab, the username and the server are defined:

The screenshot shows the 'Edit Account' window with the 'Account Settings' tab selected. The window contains the following fields and options:

- Account name:** kms-jsmith
- Personal information**
 - Name:** John Smith
 - E-mail address:** jsmith@company.com
- Server information**
 - Account ID:** jsmith
 - Domain:** company.com
 - Password:** masked with dots
 - ☒ Save password in my Mac OS keychain
 - Exchange server:** mail.company.com
- You can also enter Outlook Web Access server addresses, such as <http://mail.example.com/exchange>, into the Exchange server field. For more information, contact your Exchange server administrator.
- ☐ This DAV service requires a secure connection (SSL)
- ☐ Override default DAV port: 80

At the bottom right are 'Cancel' and 'OK' buttons.

Figure 33.13 Manual account configuration — Account Settings

Account name

The name of the email account.

Name

Any name (the first name and last name of the user is recommended) that will be displayed in the message header.

E-mail address

The email address of the user.

Account ID

Username used for login to *Kerio MailServer*. Username can be specified in two formats, either `user` or `user@domain`. If a user account is created in a domain which is not set as primary, use the `user@domain` pattern for specification of the username. Otherwise the user's attempts to connect to the LDAP database might fail.

Domain

Name of the email domain where the user has an account.

Password

The password used for accessing your account in *Kerio MailServer*.

Exchange server

DNS name or IP address of the machine where *Kerio MailServer* is running.

The traffic between *Kerio MailServer* and *MS Entourage* is usually maintained through the WebDAV interface (HTTP protocol) at port 80. If HTTP in *Kerio MailServer* is running on a non-standard port, it is necessary to enable the *Override default DAV port* option and change the port.

The traffic can also be secured by SSL. To encrypt the traffic, use the *This DAV service requires a secure connection (SSL)* option. When it is checked, the port in *Override default DAV port* is changed to port 443 (the default port for HTTPS). If another port number is specified, it is necessary to check also the *Override default DAV port* and change the port number to 443. Otherwise, connection to *Kerio MailServer* fails. It is also necessary to change the port if HTTP(S) protocol in *Kerio MailServer* communicates at a non-standard port. In such a case, it is necessary to specify the port number used by *Kerio MailServer* for HTTPS traffic.

The other tab to be filled out correctly is the *Advanced* tab where connection to the *Free/Busy* and to the LDAP server can be set:

Public folder server

In the entry, it is possible to enter a URL address to the *Free/Busy* server. The *Free/Busy* server is a public calendar that displays the free/busy data for all users that have an account in *Kerio MailServer*, and work with the calendar in *MS Entourage*, in *MS Outlook* or in the *Kerio WebMail* interface. For detailed information on usage of this feature, refer to chapter 33.3.

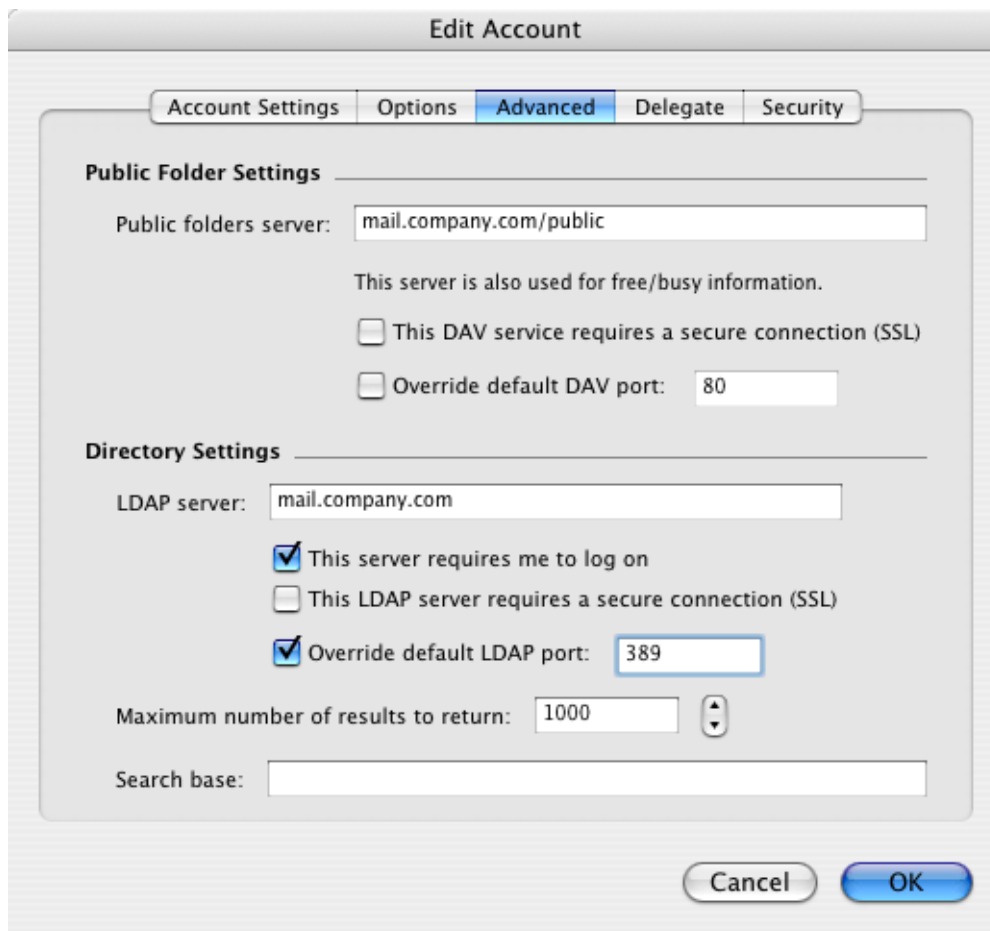


Figure 33.14 Manual account setting — Advanced

This DAV service requires a secure connection (SSL)

It is also possible to connect to the *Free/Busy* built in *Kerio MailServer* via secured SSL. If the HTTPS service in *Kerio MailServer* is running on a standard port, simply enable this option. The port in *Override default DAV port* is changed to 443 (see figure 33.27).

Override default DAV port

If *Kerio MailServer* communicates at a non-standard port, check this option and overwrite the port.

LDAP server

Enter DNS name or IP address of the LDAP server (typically the address of your *Kerio MailServer*) — see figure 33.14.

Note: *MS Entourage* supports only the main private contact folder. It does not support for displaying of shared (unless delegation is set) and public contact folders nor it supports private contact subfolders created in *Kerio WebMail* (unless they

are shared and connected by delegation). However you can add addresses from these other Contact folders through an LDAP search when creating a new email (see chapter 33.2).

This server requires me to log on

This option must be used if you want to use the LDAP database in *Kerio MailServer* since the LDAP server in *Kerio MailServer* does not allow anonymous connections.

This server requires a secure connection (SSL)

Communication with the LDAP server in *Kerio MailServer* can be secured by SSL. If this encryption is used, it is also necessary to change the port in *Override default LDAP port* (standard port for LDAPS is 636).

Override default LDAP port

By default, *MS Entourage* uses a non-standard port where the *MS Exchange* email client is run. Whenever a user connects to *Kerio MailServer*, they must change the port to the port on which the *Kerio MailServer's* LDAP service is running.

It is therefore necessary to check this option and enter the correct port number and every time. The standard port number for the non-secured LDAP is 389 and the standard port number for SSL-secured LDAP is 636. If the LDAP service in *Kerio MailServer* is running on a non-standard port, specify the port used by the LDAP(S) service in *Kerio MailServer*.

33.2 Connection to the LDAP server

MS Entourage enables connection to any number of LDAP databases for contact look-ups. New LDAP can be added on the *Directory Service* tab in *Tools* → *Accounts*.



Figure 33.15 LDAP settings

Account name

Name of the account, used for reference only.

LDAP server

DNS name or IP address of the computer where LDAP server is running (e.g. mail.company.com or 192.168.1.10).

This server requires me to log on

This option must be used if you want to use the LDAP database in *Kerio MailServer* since the LDAP server in *Kerio MailServer* does not allow anonymous connections.

- *Account ID* — user name. When connecting to the *Kerio MailServer's* LDAP database, it plays a role whether the user is created in the primary domain. If the user is created in a domain which is not primary, the username must include the domain for the specification. This implies that the *Account ID* pattern will be as follows: user@domain (jwayne@company.com). If the user is created in the primary domain, simply use the user (jwayne) pattern for the specification.
- *Password* — user password

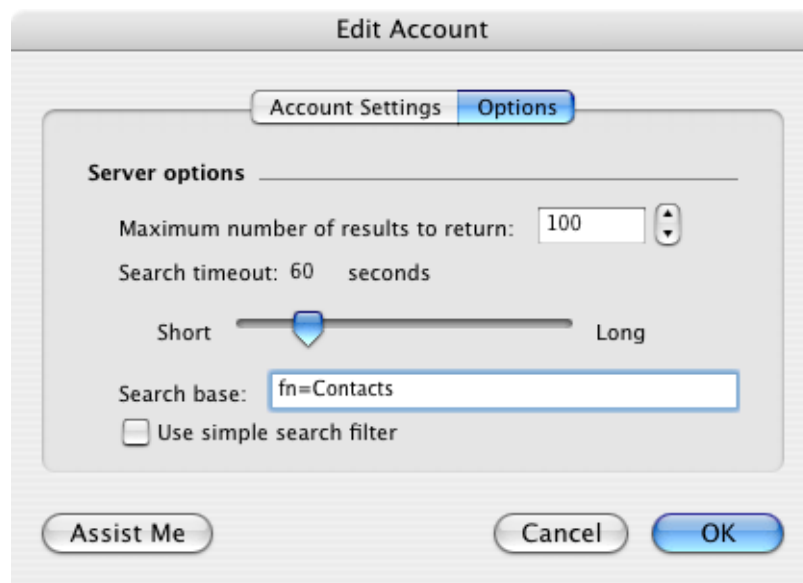


Figure 33.16 LDAP settings

Search base

Specify a location of contacts in the LDAP database (see above). If the entry is not specified, all subscribed contact folders will be searched through.

If you want to access all private and subscribed shared and public folders, leave the entry blank or enter

`fn=ContactRoot`

More precise specification of searched section of the LDAP database enables to access only some types of contacts. To better understand various alternatives, read the following examples:

- `cn=jsmith@company.com,fn=ContactRoot`
(the look-up will be performed only in folders of the `jsmith@company.com` user)
- `fn=personal,fn=ContactRoot` (only folders of the user currently connected to the LDAP server will be searched through. This option is identical with the previous one, however, it is not necessary to specify username (or email address) of the user. This option may be helpful for example when configuring multiple clients, etc.)
- `fn=public,fn=ContactRoot`
(only public contact folders will be searched through)
- `fn=Contacts,cn=jsmith@company.com,fn=ContactRoot`
(only the Contacts folder of the `jsmith@company.com` user will be searched through)
- `fn=PublicContacts,fn=public,fn=ContactRoot`
(only the public PublicContacts folder will be searched through)

33.3 Usage of the Free/Busy server

Kerio MailServer includes a built-in *Free/Busy* server. The *Free/Busy* server provides a public calendar showing information about free and busy time of users involved.

The *Free/Busy* calendar does not show what events are taking place. It only displays when and for how long a particular user is busy. This calendar helps user find out when everyone involved has time for a business meeting, however, it is not possible to find out what is the event that makes the meeting impossible at a certain time. The only information that can be found is that the user is either busy or free at a particular moment.

This implies that this type of calendar is perfect for planning of meetings and sessions. The user who adds a new meeting can view when the people involved are free or busy. It is therefore not necessary to ask individual users when they are free. However, the following conditions must be met to enable this function:

- all users must have an account in *Kerio MailServer*,
- the users involved must manage their events by a calendar in *MS Entourage*, in *MS Outlook* (with the *Kerio Outlook Connector*) or in *Kerio WebMail*.

The *Free/Busy* calendar displays all meetings and events included in the main calendar folder and its subfolders. If you want that some events (e.g. items of a private calendar) are not shown in the *Free/Busy* calendar, create a new calendar folder out of the branch of the main calendar and its subfolders.

Using the Free/Busy calendar for meetings

If the *Free/Busy* server is enabled for an account in its configuration (see chapter 33.1), users can easily choose the best time for their meetings. The *Scheduling* tab provides a list of all members of a particular meeting (with the *Invite* option) and time they are free or busy. The busyness of individual users is shown by different tints of blue. The *Free/Busy* server marks users for whom no information is available with grey (users who do not have an account on the mailserver, do not use a *Free/Busy* calendar, etc.).

Warning: It is necessary to specify each user by their usernames and domains (username@domain). Aliases cannot be used to display *Free/Busy* information.

The purple box represents the meeting suggested. The window can be moved, extended or narrowed by the mouse pointer.

Warning: For a successful connection to the *Free/Busy* server, it is necessary to specify the *Subject* entry on the *Appointment* tab.

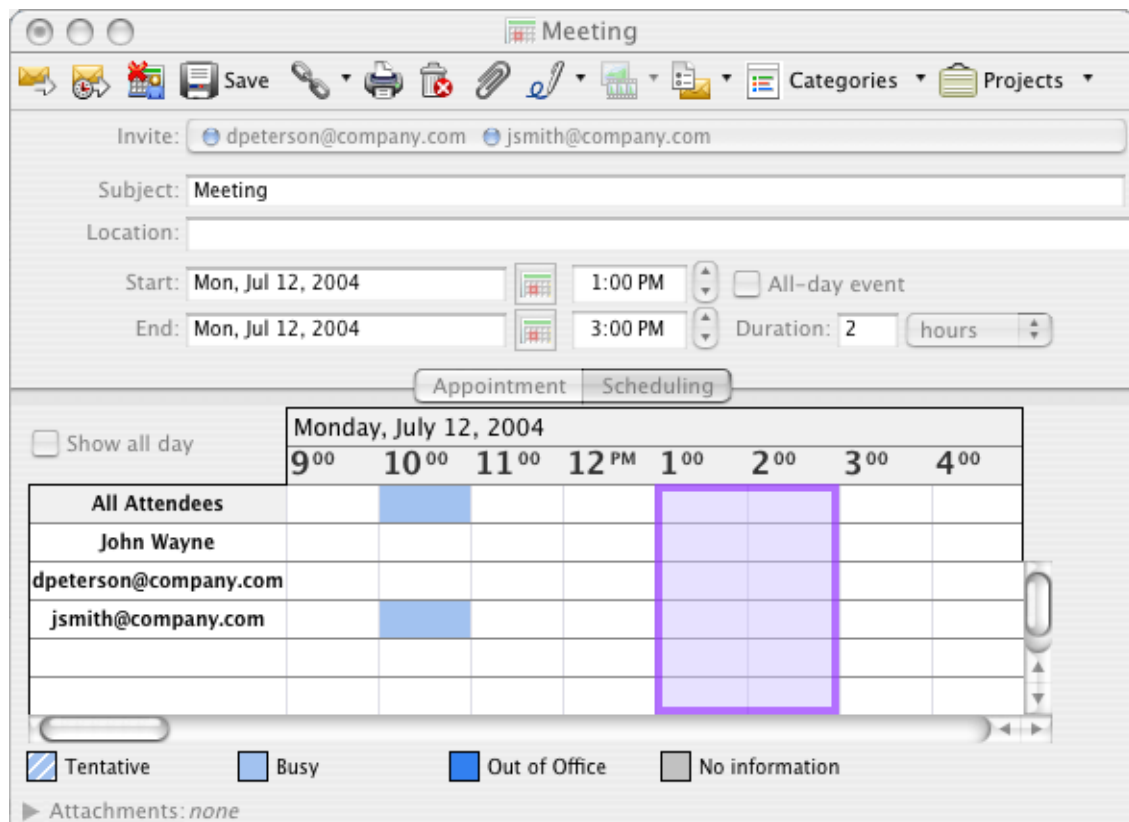


Figure 33.17 Usage of the Free/Busy calendar

33.4 Delegating folders and their connection in MS Entourage 2004

Delegating is similar to sharing which allows for assigning access rights (reading, writing, administration) for selected folders to any user of the same domain. These two types differ in method of their connection. In case of sharing, user has to connect folder by folder, whereas in case of delegation, user connects the entire account where he/she can see only folders enabled by appropriate rights. The main advantage of delegation is more transparent viewing of connected folders, especially when one user delegates multiple folders for another users.

The following folder types can be delegated:

- mail
- calendars
- contacts

In *MS Entourage*, folders can be delegated only in the version with service pack version2. If *MS Entourage* does not include the appropriate service pack update, it is necessary to set sharing via the *Kerio WebMail* interface or in *MS Outlook* extended by the *Kerio Outlook Connector*. Folders can be delegated simply by adding appropriate rights to a user. To see how to delegate folders in *MS Outlook*, go to chapter 31.9 and to learn how to do it in *Kerio WebMail*, read a separate user guide which is available at *Kerio Technologies* website.

When delegating folders, rights cannot be granted to folders of lower levels of the tree. It is necessary that the folders are shared up to the highest level (the highest folder must be saved right under the root folder). If folders which are save in a non-shared folder, the user to which the folders are delegated cannot see and access these folders in *MS Entourage*.

For security reasons, it is not recommended to delegate for example the *INBOX* folder. It is recommended to delegate a new folder created from the root folder instead. All folders to be delegated must be moved to the new folder. Now, it is secure to grant access rights (see figure 33.18).

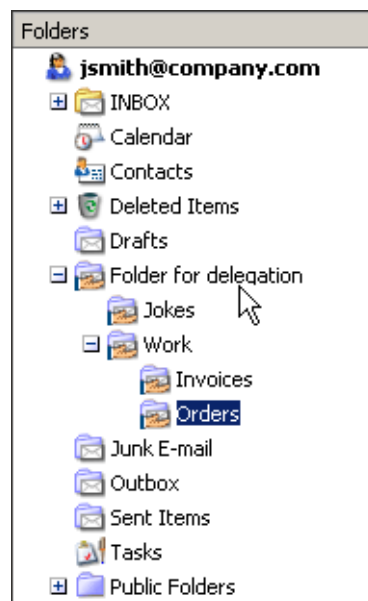


Figure 33.18 Tree structure in Kerio WebMail — an example of a correctly created structure of delegated folders

Delegated folders can be subscribed in *MS Entourage*:

Settings in MS Entourage 2004

The following conditions must be met to make the delegation and subscription work properly:

- Both users (delegator and subscriber) must use account in a single *Kerio MailServer* and they must belong to the same domain.
- Appropriate rights must be set for the folder in *Kerio WebMail* or *MS Outlook* by the delegator
- The subscriber's KMS account in *MS Entourage* must be set as primary
- The subscriber's LDAP service must be configured properly (server and port) in account settings
- The subscriber must have included the delegator in any of his/her contact folders (unless the contact is included in public contacts).

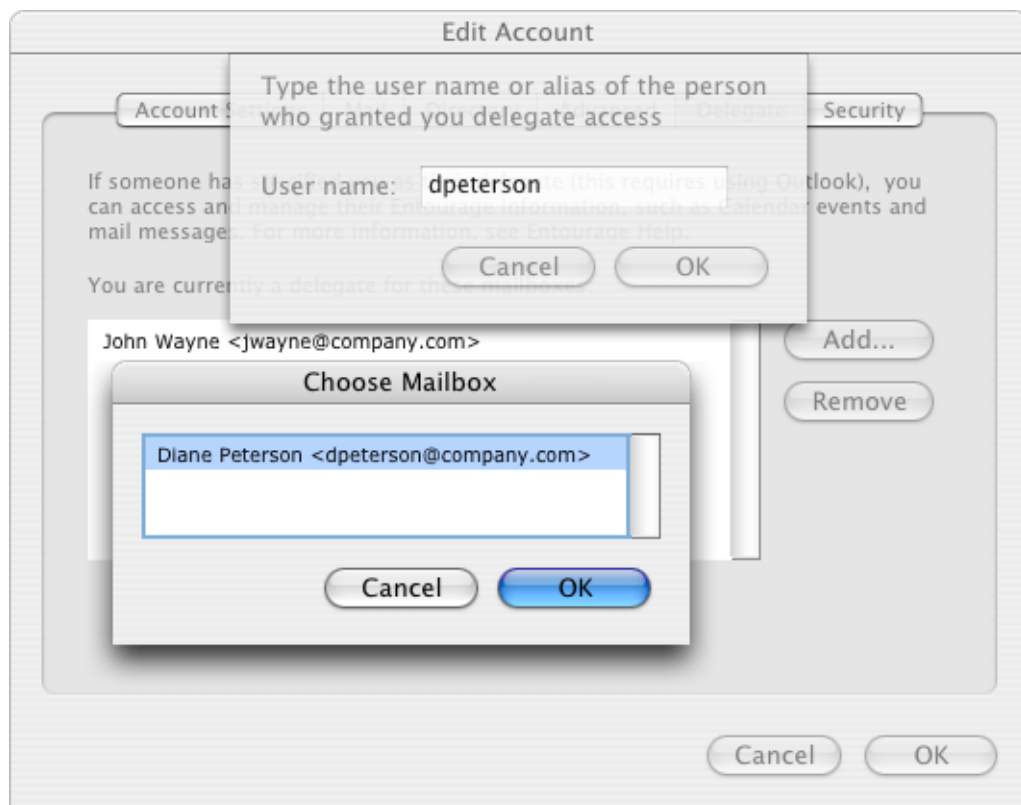


Figure 33.19 Connecting delegated folders

If the conditions are met, specify the username of the delegator on the *Delegate* (see figure 33.19) tab in the *Tools* → *Accounts*. From the box just opened, the delegating user can be selected.

If the delegation is set correctly, the mail folder added appears in the folder tree in the main *MS Entourage* (see figure 33.20) window and it can be used in accordance with the rights assigned.

If a calendar of a contact folder has been delegated, its items are shown in the standard calendar or contact folder. Items of the delegated folder will be marked by a different colour.

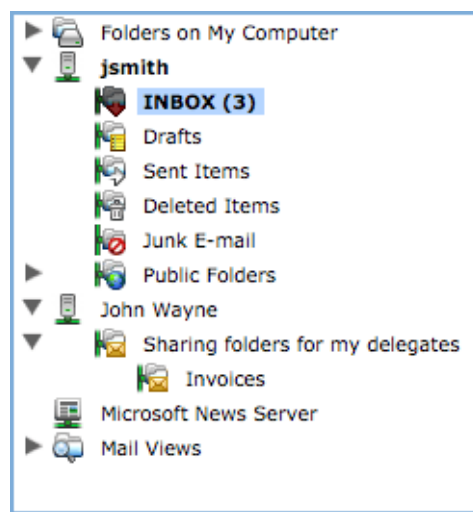


Figure 33.20 Delegated folders in the tree

If subscription of delegated folders does not work, check whether the configuration of the account meets all the conditions described above.

Settings in MS Entourage 2004 sp2

In *MS Entourage 2004* with service pack version 2, unlike in the previous version, it is possible to delegate folders right in *MS Entourage*. The standard delegation tool cannot be used in this case, however, it is possible to delegate folders by standard sharing (see figure 33.21).

In *MS Entourage*, it is possible to share any folder which includes at least one item (an email message, an event or a contact). To set this, follow this guidance:

1. Use the mouse pointer to select a folder to be shared with another user.
2. Open the folder's context menu (hold the *Ctrl* key and click on the folder) and select *Sharing*.

3. This opens a dialog where a user can be added and access rights for the folder can be assigned (see figure 33.21).

To allocate rights, use the *Permission level* menu. The menu includes multiple options, however, only three can be used for configuration of rights in *Kerio MailServer*:

- Owner = administration rights
- Editor = editing is allowed
- Reviewer = for reading only

It is recommended not to use the other options.

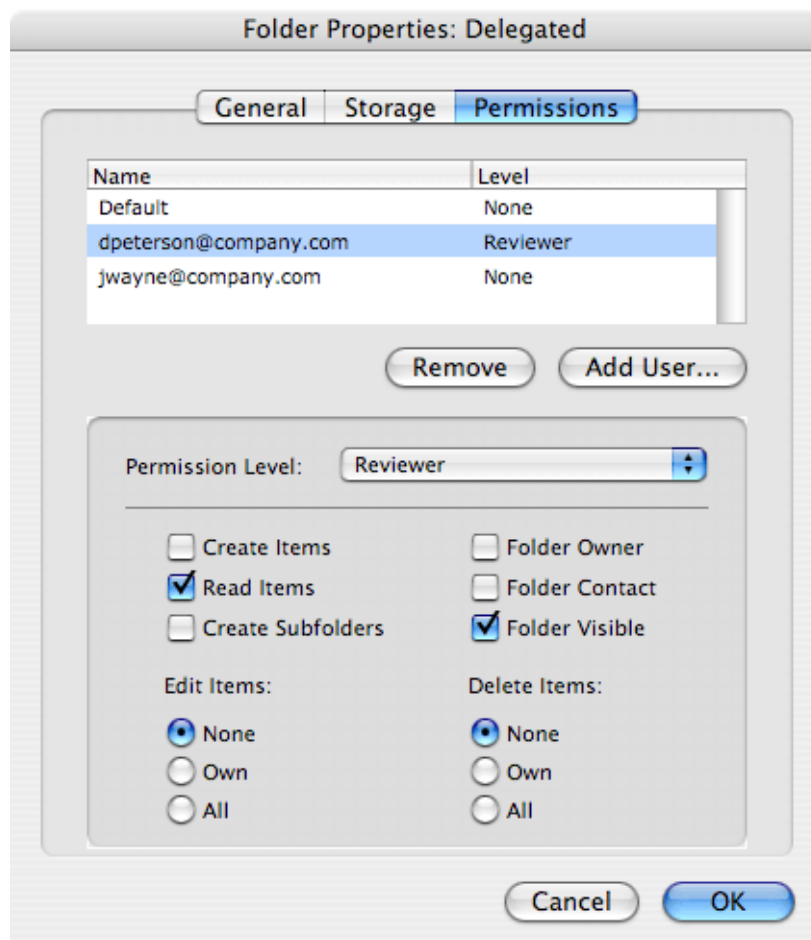


Figure 33.21 Sharing folders

The following conditions must be met for subscription of delegated folders:

- Both users (delegator and subscriber) must use account in a single *Kerio MailServer* and they must belong to the same domain.
- The delegator must set appropriate access rights for the folder in *MS Entourage* (by standard sharing methods), in *Kerio WebMail* or in *MS Outlook*.
- The subscriber's KMS account in *MS Entourage* must be set as primary

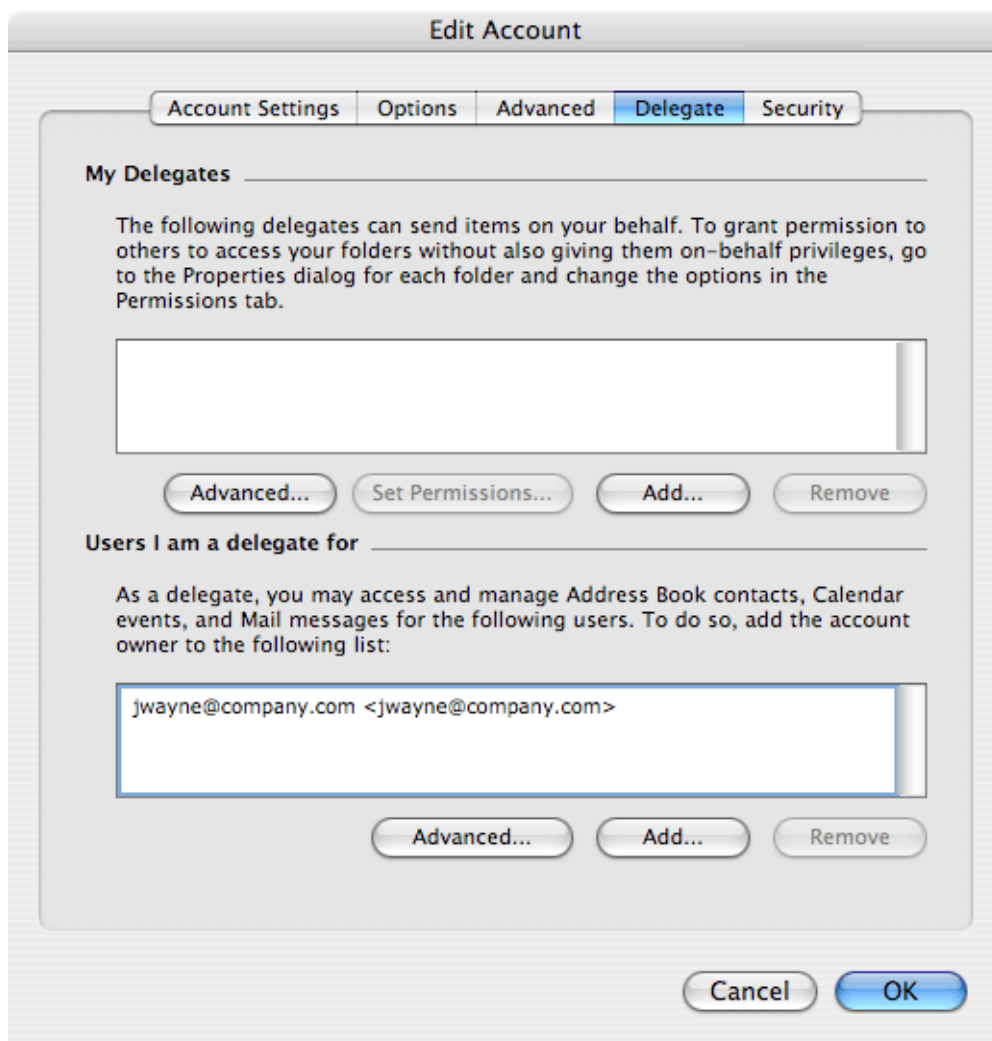


Figure 33.22 Connecting delegated folders

If the conditions are met, specify the username of the delegator on the *Delegate* (see figure 33.22) tab in the *Tools* → *Accounts*.

If the delegation is set correctly, the folders added appear in the folder tree in the main *MS Entourage* (see figure 33.23) window and it can be used in accordance with the rights assigned.

The way of displaying calendars and contacts differs from the previous version. If contacts or calendars were delegated, these folders will be displayed separately. Delegated calendar folders will be displayed in the calendars section, while delegated contact folders will be displayed in the contacts section.

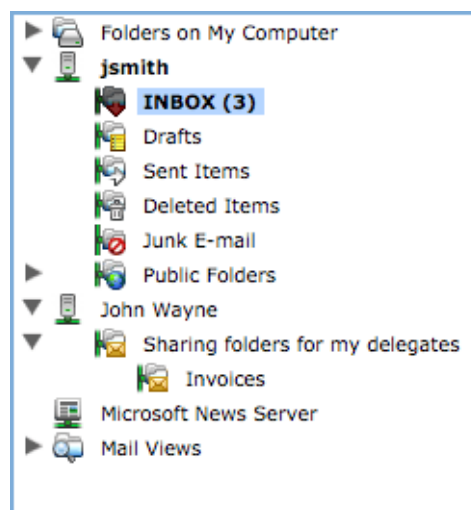


Figure 33.23 Delegated folders in the tree

If subscription of delegated folders does not work, check whether the configuration of the account meets all the conditions described above.

33.5 Secure communication of Kerio MailServer with MS Entourage

The communication between *Kerio MailServer* and *MS Entourage* can be protected by the standard SSL encryption protocol. It is possible to secure communication via the WebDAV interface as well as requests and responses between *MS Entourage* and the LDAP server built in *Kerio MailServer*. Settings differ for each version of *MS Entourage*. Here you can find description of both alternatives:

Settings in MS Entourage 2004

To set WebDAVS in *MS Entourage 2004*, follow these steps:

- On the *Advanced* tab in *Tools* → *Accounts* → *Entourage*, enable the *DAV service requires secure connection (SSL)* option.

Note: Enabling the *DAV service requires secure connection (SSL)* option also changes the standard port for HTTP service to the HTTPS port. Generally, it is therefore not necessary to change the port by hand.

- If the HTTPS service in *Kerio MailServer* is running on another port than the standard port 443, it is necessary to enable the *Override default DAV port* option and change the port by hand.

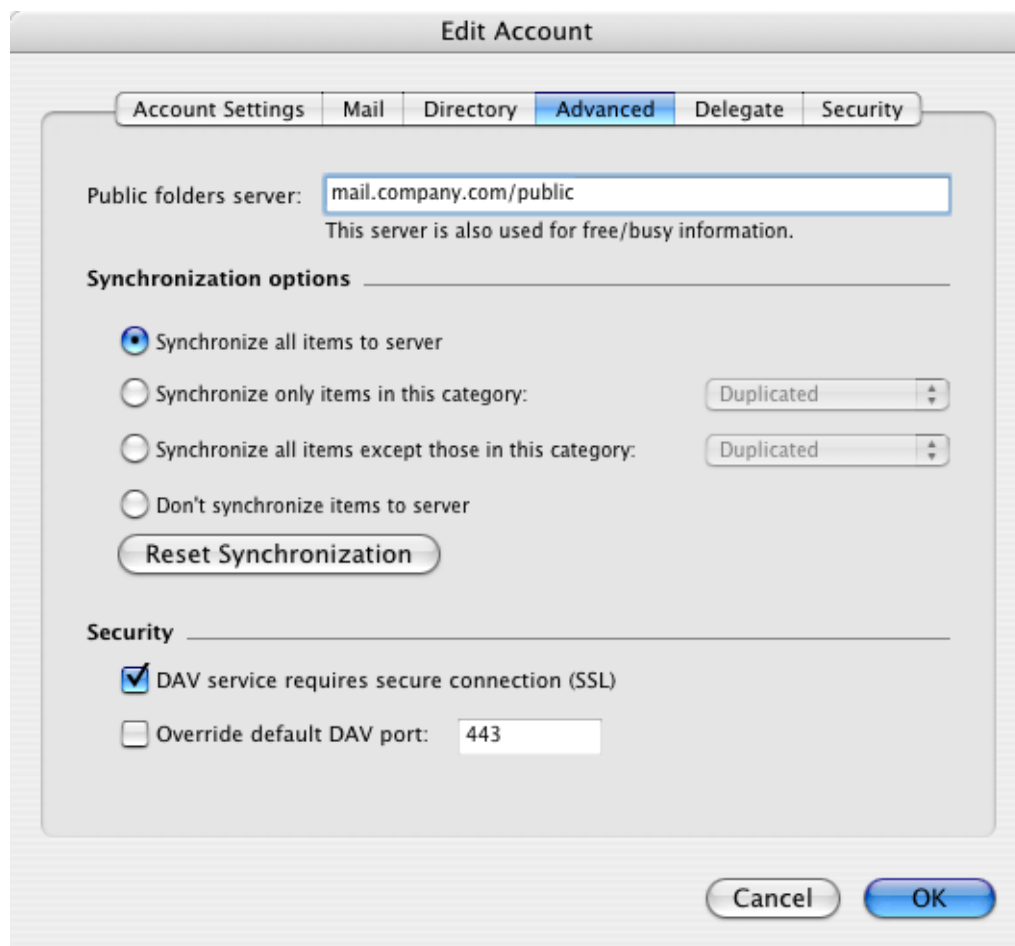


Figure 33.24 Setting the secure WebDAV

Setting of LDAPS in *MS Entourage* is also very simple:

- On the *Directory* tab in *Tools* → *Accounts* → *Entourage*,) click on *Click here for advanced options*.

- In the menu, check the *This LDAP server requires a secure connection (SSL)* option.

Note: Enabling the *This LDAP server requires a secure connection (SSL)* option also changes the standard port for LDAP service to the LDAPS port. Generally, it is therefore not necessary to change the port by hand.

- If the LDAPS service in *Kerio MailServer* is running on another port than the standard port 636, it is necessary to enable the *Override default LDAP port* option and change the port by hand.

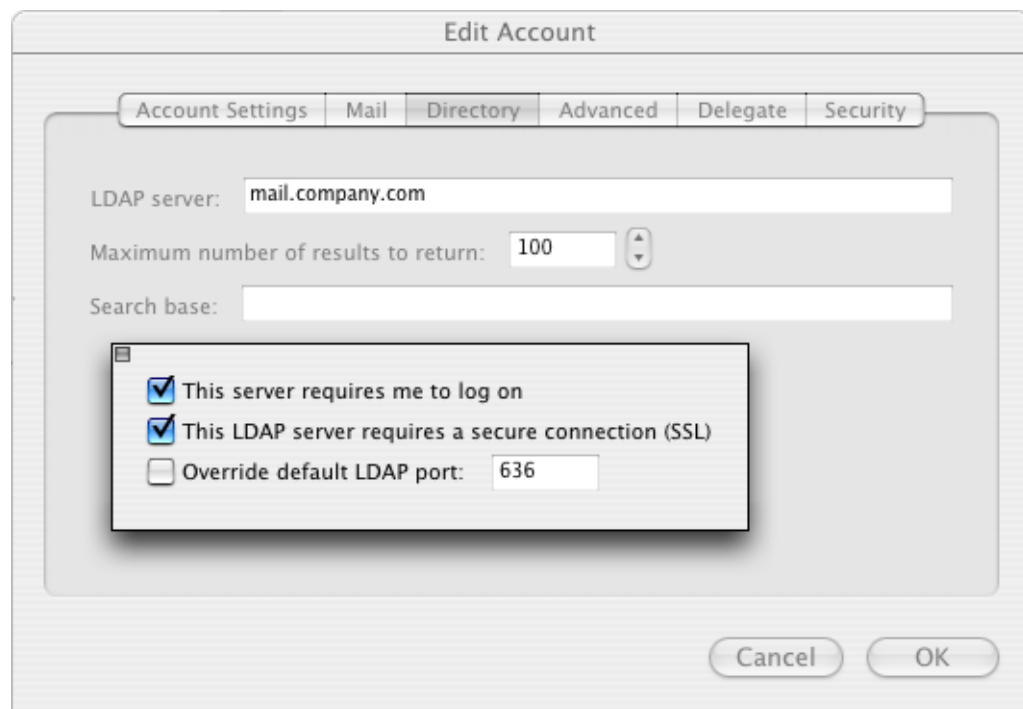


Figure 33.25 Setting the secure LDAP

Warning: It is not recommended to use SSL if the Internet connection is slow or if you intend to work with your email. When switched to SSL, the account will be synchronized with the server. The entire mailbox is downloaded within the first synchronization. Therefore, the synchronization may take quite a long time.

Settings in MS Entourage 2004 sp2

To set WebDAVS in *MS Entourage 2004 sp2*, follow these steps:

- On the *Account Settings* tab in *Tools → Accounts*, enable the *DAV service requires secure connection (SSL)* option (see figure 33.26).

Note: Enabling the *This DAV service requires a secure connection (SSL)* option also changes the standard port for HTTP service to the HTTPS port. Generally, it is therefore not necessary to change the port by hand.

- If the HTTPS service in *Kerio MailServer* is running on another port than the standard port 443, it is necessary to enable the *Override default DAV port* option and change the port by hand.

The screenshot shows the 'Edit Account' dialog box with the 'Account Settings' tab selected. The 'Account name' is 'kms-jsmith'. Under 'Personal information', the 'Name' is 'John Smith' and the 'E-mail address' is 'jsmith@company.com'. Under 'Server information', the 'Account ID' is 'jsmith', the 'Domain' is empty, and the 'Password' is masked with dots. The 'Exchange server' field is highlighted and contains 'mail.company.com'. Below this field, there is a note: 'You can also enter Outlook Web Access server addresses, such as http://mail.example.com/exchange, into the Exchange server field. For more information, contact your Exchange server administrator.' At the bottom, the checkbox 'This DAV service requires a secure connection (SSL)' is checked, and the 'Override default DAV port' checkbox is unchecked with the port number '443' in the adjacent field. The 'Cancel' and 'OK' buttons are at the bottom right.

Figure 33.26 Setting the secure WebDAV

Connection to the *Free/Busy* server built in *Kerio MailServer* can also be SSL-secured. The connection between a client and the *Free/Busy* server is handled via the WebDAV interface. Therefore, the traffic can be secured by setting of the secure version of the DAV protocol. To set this, go to the *Advanced* tab under *Tools* → *Accounts* and enable the *This DAV service requires a secure connection (SSL)* option.

Note: Enabling the *This DAV service requires a secure connection (SSL)* option also changes the standard port for HTTP service to the HTTPS port. Generally, it is therefore not necessary to change the port by hand.

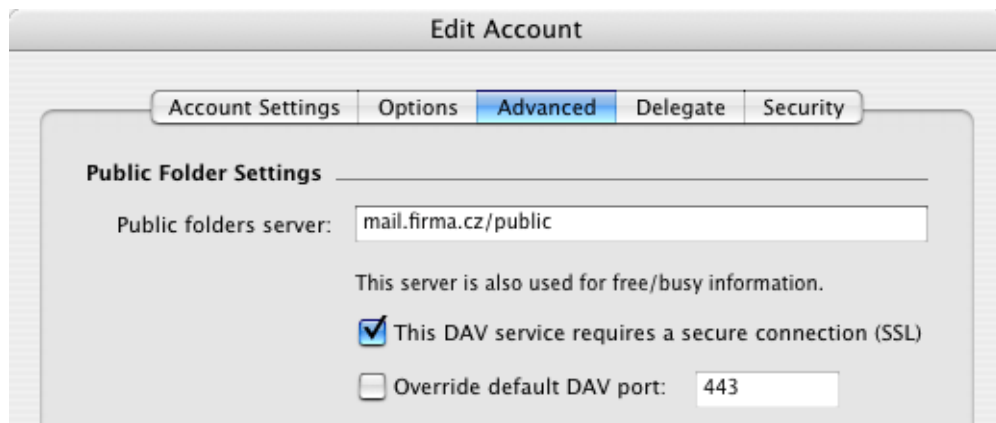


Figure 33.27 Setting secure version of WebDAV for connections to the Free/Busy server

Setting of LDAPS in *MS Entourage* is also very simple:

- On the *Advanced* tab in *Tools* → *Accounts*, enable the *This LDAP server requires a secure connection (SSL)* option.
- It is also necessary to enable the *Override default LDAP port* option and overwrite the port number to the port where the LDAPS in *Kerio MailServer* is running (standard port for LDAPS is port 636).

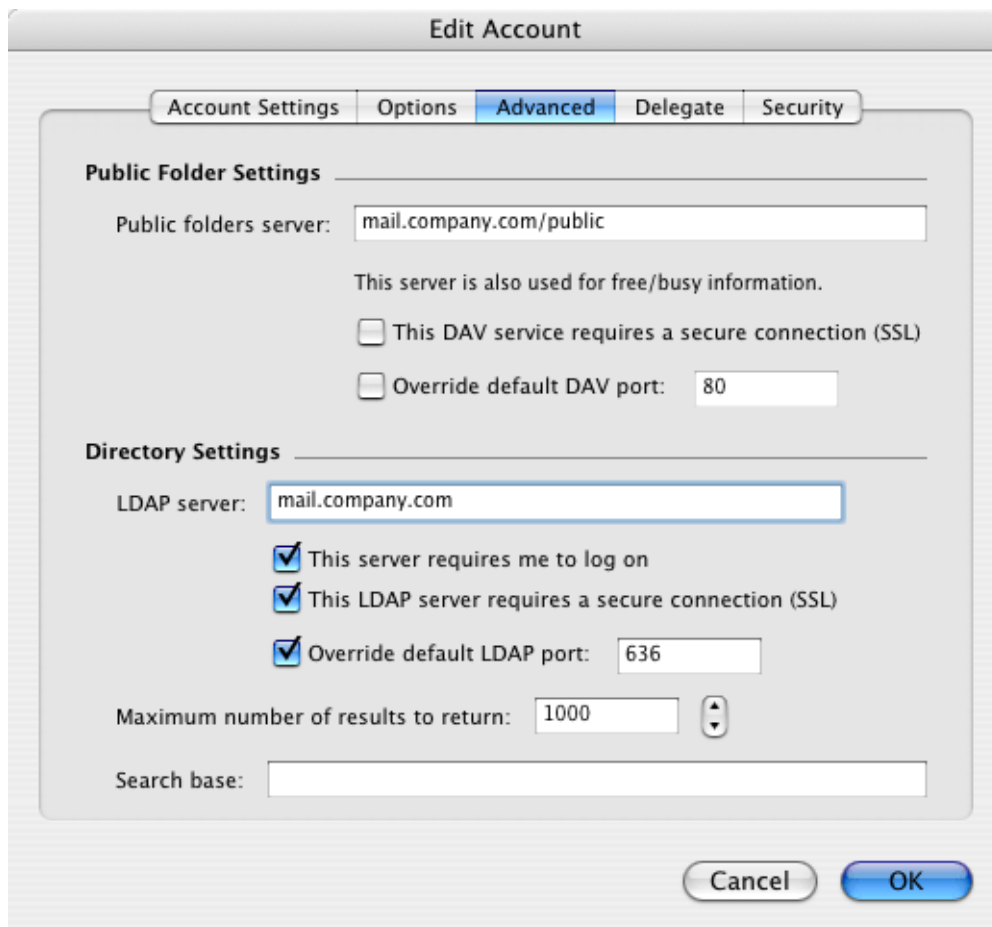


Figure 33.28 Setting the secure LDAP

Importing SSL certificate

This chapter describes the situation where *Kerio MailServer* uses a self-signed certificate and a user tries to connect to it via SSL (DAVS and LDAPS in *MS Entourage*).

The security system of MacOS X does not trust certificates which are not signed by a trustworthy certification authority (so called self-signed certificates — see chapter 11). *Kerio MailServer* uses the self-signed certificate by default. To make Mac OS X systems accept the *Kerio MailServer*'s self-signed certificate, do the following:

Exporting self-signed certificate from Kerio Administration Console

- In the *Kerio Administration Console*, go to the *SSL certificates* section.
- Select the active certificate and click *Export*. In the menu, choose *Export certificate*.
- Save the certificate on the desktop (if the client is installed on the same computer as the server) or to another directory available to client station where the certificate will be imported.

Importing certificate

- Open the key store at the client station by the *Applications → Utilities → Keychain access* option
- Look up the exported file and double-click it.
- In the *Add Certificates* dialog box (see figure 33.29), select the *X509Anchors* store type in the *Keychain* menu. The *X509Anchors* store includes saved certificates which can sign and thus make trustworthy other certificates. It also stores all trustworthy certificates.¹



Figure 33.29 The Add Certificates dialog box

- Administration password is required if you are not logged in as a root user or as an administrator.
- Now, find the certificate on the desktop or in a file and drag it to the *Keychain Access* window. The certificate should appear in the certificate list.
- Click OK

Update of *MS Entourage* for version 11.1.0.

- Check the *MS Entourage* version in the *About Entourage* section
- If your version is not up-to-date, update it by the *Entourage Help → Check for updates* option
- Check whether *MS Entourage* was updated successfully in the *About Entourage* dialog box

¹ Certificates work only if they are in the X509 format, encoded by Base64. If a certificate does not meet these conditions, it is possible to convert it by a special application, *Microsoft Cert Manager*. This application can be found under *Applications → Microsoft Office → Office → Microsoft Cert Manager*. However, in this case usage of the application would be irrelevant. *Kerio MailServer* creates certificates in the X509 format, encoded by Base64.

Note: If the SSL communication still fails, try to create a new self-signed certificate in *Kerio MailServer* and retry to establish the connection.

If your certificate is certified by a trustworthy certification authority, import it to the *X509Anchors* store in the *Keychain access* directory.

Chapter 34

Apple iCal Support

Apple iCal is an application used for management of *AppleComputer's* calendars. Developed by *Apple Computer*, it is designed for *Mac OS X* operating systems. This application enables to view events of multiple calendars in a single schedule and thus quickly identify conflicts in the time schedule.

These calendars may be either located at the disc or at a web server (in *Kerio MailServer* in this case).

It is possible to subscribe to various calendars as well as to publish calendars at web servers (such as *Kerio MailServer*). Subscription and publishing are performed by HTTP (in this case, it is not possible to use HTTPS). This implies that it is necessary that the HTTP service is running in *Kerio MailServer*.

As suggested by the name, the *iCalendar* (called *iCal* in this document) format is applied to calendar management. *iCal* is a standard format used for exchange of calendar data. The cooperation of *Apple iCal* and *Kerio MailServer* is actually based on *iCal*.

The support for *iCalendar* in *Kerio MailServer* enables subscription and publishing of *Apple iCal* calendars.

Notes:

- The support for *iCalendar* in *Kerio MailServer* enables various applications which can handle the format (such as *MS Outlook*, *Mozilla Calendar*, *Lotus Notes* and *Ximian Evolution*) to publish and subscribe to calendars via *Kerio MailServer*.
- If calendars are published as subfolders of the *Calendar* folder (the main calendar), all events will be also shown in the *Free/Busy* calendar (see chapters 31.17 and 33.3).

34.1 Setting Apple iCal in Mac OS X 10.3

Subscription to calendars

Calendars can be subscribed through the *Calendar* → *Subscribe* menu. This option opens a dialog (see figure 34.1) where URL address can be specified and detailed authentication and refreshing parameters can be set (the entire calendar is downloaded for each refresh):

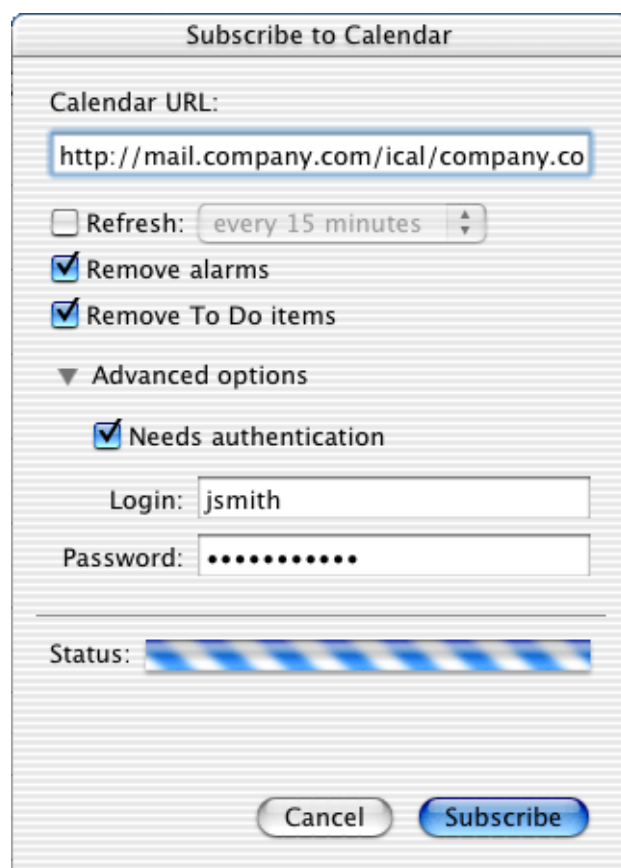


Figure 34.1 The Calendar Subscription dialog

Calendar URL

To subscribe a calendar in *Kerio MailServer*, a valid URL is required. The address must follow this pattern:

`http://server_name/ical[format]`

To subscribe the default calendar folder which belongs to your mailbox in *Kerio MailServer*, enter the URL in the following format:

`http://server_name/ical`

It is also possible to subscribe another user's calendar, if the user shares it for you.

For the login URL, use the following pattern:

`http://server_name/ical/user@domain`

or

`http://server_name/ical/domain/user_name`

It is also possible to subscribe another user's calendar, if shared. The following URL format must be used:

`http://server_name/ical/public`

or

`http://server_name/ical/public/calendar`

When a calendar is being subscribed, it is possible to edit name of the folder. If no name is entered, the Calendar folder will be used automatically.

Warning: It is not possible to subscribe calendars via SSL connection. Therefore, use only the non-secured HTTP version for this purpose. This means that URLs of calendars must not start with `https://`.

Refresh

The calendar will be refreshed in the interval set.

Remove alarms

Alarms will be disabled for the calendar (pop-up reminders).

Remove To Do items

The calendar will not include To Do items.

Advanced options

Username and password for a corresponding user account in *Kerio MailServer* is required for a calendar subscription.

The calendar is available only for reading.

Calendar publishing

In *Kerio MailServer*, any calendar in the *iCal* format can be published. URL for publishing in one of the following forms is required:

`http://server_name/ical[format]`

To publish a calendar in the root folder (of a particular mailbox), enter URL in the following format:

`http://server_name/ical`

To publish a calendar in the calendar folder (of your mailbox), enter URL in the following format:

`http://server_name/ical/calendar`

To publish a calendar to the mailbox of another *Kerio MailServer* user, enter URL in the following format:

`http://server_name/ical/user@domain/folder_name`

When published, the calendar will be available at the server for reading only. This means that the calendar cannot be edited in *Kerio WebMail* or *MS Outlook* extended by *Kerio Outlook Connector*.

Calendars can be published through the *Calendar* → *Published* menu. This opens a dialog (see figure 34.2), where URL address can be specified and other publishing parameters can be set. It is also possible to set that the calendar is re-published upon each change (the entire calendar is always published, not just changes):

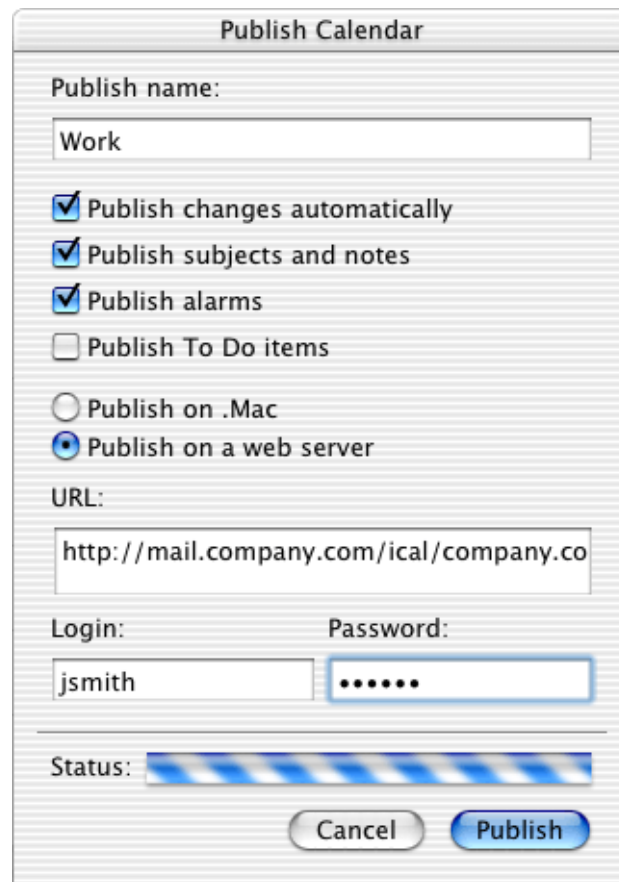


Figure 34.2 The Publish Calendar dialog

Publish name

Specify a name for the calendar. It is not recommended to use special symbols and characters in calendar names.

Publish changes automatically

If this option is checked, the calendar will be re-published upon each change.

Publish subjects and notes

If it is desirable that events' subjects and bodies are displayed on the server, enable this option.

Publish alarms

Alarms will be published with the calendar.

Publish To Do items

This data will not be displayed in *Kerio MailServer*.

It is necessary to switch the dialog for *Publish on to Private Server* mode:

URL

Publishing URL (see above).

Login, Password

Name and password used for authentication at the server where the calendar will be published. In this case, specify username and password for the corresponding *Kerio MailServer* user account.

34.2 Setting Apple iCal in Mac OS X 10.4

Subscription to calendars

As in the previous case, calendars can be subscribe in the *Calendar* → *Subscribe* menu. This opens a dialog (see figure 34.3), where URL address can be specified and more detailed publishing criteria can be set. The address must follow this pattern:

`http://server_name/ical[format]`

To subscribe the default calendar folder which belongs to your mailbox in *Kerio MailServer*, enter the URL in the following format:

`http://server_name/ical`

It is also possible to subscribe another user's calendar, if the user shares it for you. For the login URL, use the following pattern:

`http://server_name/ical/user@domain`

or

`http://server_name/ical/domain/user_name`

It is also possible to subscribe another user's calendar, if shared. The following URL format must be used:.

`http://server_name/ical/public`

or

`http://server_name/ical/public/calendar`

When a calendar is being subscribed, it is possible to edit name of the folder. If no name is entered, the *Calendar* folder will be used automatically.

Warning: It is not possible to subscribe calendars via SSL connection. Therefore, use only the non-secured HTTP version for this purpose. This means that URLs of calendars must not start with `https://`.

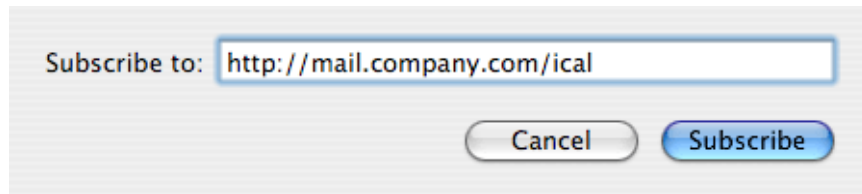


Figure 34.3 URL calendar definition

When the URL is specified, the application attempts to connect to the server. If authentication is required, the dialog where username and password can be specified is opened (i.e. typically the username and password used for connection to your email account).

Once connected to *Kerio MailServer*, a dialog where other details can be specified is opened (see figure 34.4):

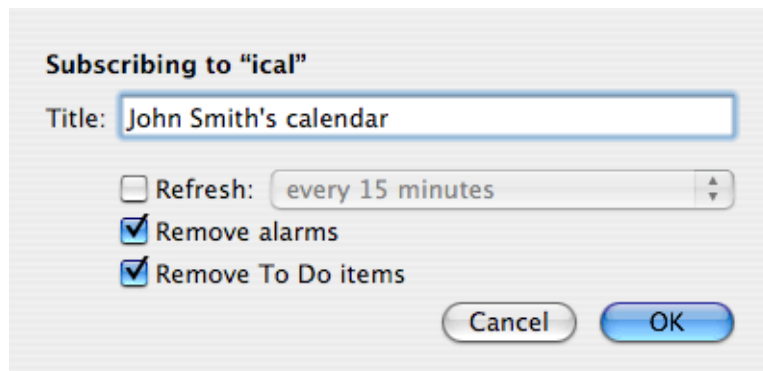


Figure 34.4 Setting details

Title

Any name used for the calendar in *Apple iCal*.

Refresh

The calendar will be refreshed in the interval set. Unless the user has a fast Internet connection, it is not recommended to set the interval too short (calendar is completely reloaded upon each refresh).

Remove alarms

Alarms will be disabled for the calendar (pop-up reminders).

Remove To Do items

The calendar will not include To Do items.

Calendar publishing

The calendar is published in similar way like in case of the previously described version. Calendars can be published through the *Calendar* → *Publish* menu. This opens a dialog (see figure 34.5), where URL address can be specified and other publishing parameters can be set. It is also possible to set that the calendar is re-published upon each change (the entire calendar is always published, not just changes).

When published, the calendar will be available at the server for reading only. This means that the calendar cannot be edited in *Kerio WebMail* or *MS Outlook* extended by the *Kerio Outlook Connector*.

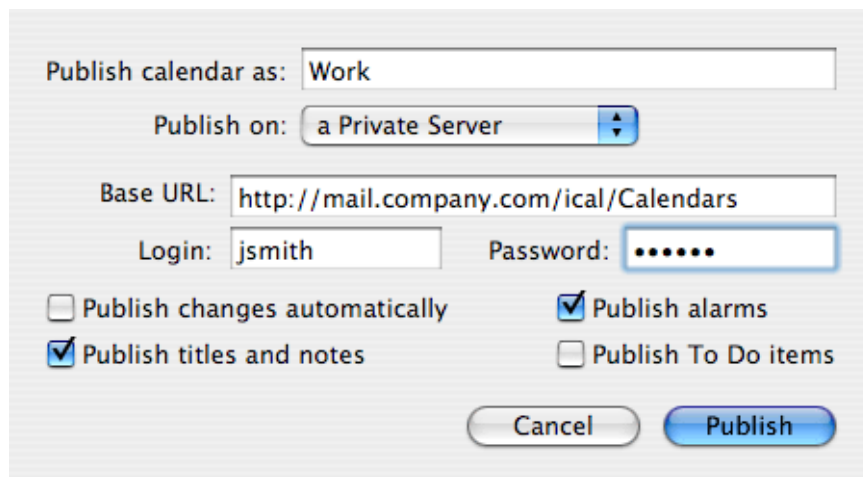


Figure 34.5 The Publish Calendar dialog

Publish calendar as

By default, the entry includes the name used by this calendar in *Apple iCal*. The title can be edited.

Publish on

In the menu, set the *a Private Server* option.

Base URL

URL address of the server where the calendar would be published. The URL address must follow this pattern:

`http://server_name/ical[format]`

To publish a calendar in the root folder (of a particular mailbox), enter URL in the following format:

`http://server_name/ical`

To publish a calendar in the calendar folder (of your mailbox), enter URL in the following format:

`http://server_name/ical/calendar`

To publish a calendar to the mailbox of another *Kerio MailServer* user, enter URL in the following format:

`http://server_name/ical/user@domain/folder_name`

Login, Password

Name and password used for authentication at the server where the calendar will be published. In this case, specify username and password for the corresponding *Kerio MailServer* user account.

Publish changes automatically

If this option is checked, the calendar will be re-published upon each change.

Publish titles and notes

If it is desirable that events' subjects and bodies are displayed on the server, enable this option.

Publish alarms

Alarms will be published with the calendar.

Publish To Do items

This data will not be displayed in *Kerio MailServer*.

Chapter 35

Apple Address Book Support

Kerio MailServer supports standard Mac OS X *Apple Address Book*.

For proper functionality of the *Apple Address Book* support, it is necessary that the LDAP(S) service is running in *Kerio MailServer*.

Kerio MailServer supports *Apple Address Book* in Mac OS X 10.2 *Jaguar*, Mac OS X 10.3 *Panther* and Mac OS X 10.4 *Tiger*. Setting options are different for these versions — therefore, they will be focused in separate sections:

35.1 Apple Address Book for Mac OS X 10.2 (Jaguar)

This version supports only search in the *Kerio MailServer*'s LDAP database. Settings can be made under *Address Book* → *Preferences* (the LDAP tab). Specify the *Server* item with the DNS name or the IP address of the host where *Kerio MailServer* is running and the LDAP port for *Kerio MailServer*.

SSL-secured LDAP can be used for the traffic. However, in such a case it is necessary to authenticate by a trustworthy certificate (for details, refer to chapter 33.5). *Apple Address Book* connects to *Kerio MailServer* by encrypted connection using the LDAP Start TLS (RFC 2830) extension. It is necessary to follow these steps when setting the encrypted communication on the *Address Book* → *Preferences* → *LDAP* tab:

1. enable the *Use SSL* option,
2. change the default port 636 to the port used in *Kerio MailServer* for the non-secured LDAP service (typically port 389). In case that you want to use SSL-secured connection to the server (*Use SSL*), a trustworthy certificate installed is required.

Note: In this version, searching is available only for public contact folders with anonymous read access (the “anyone” user).

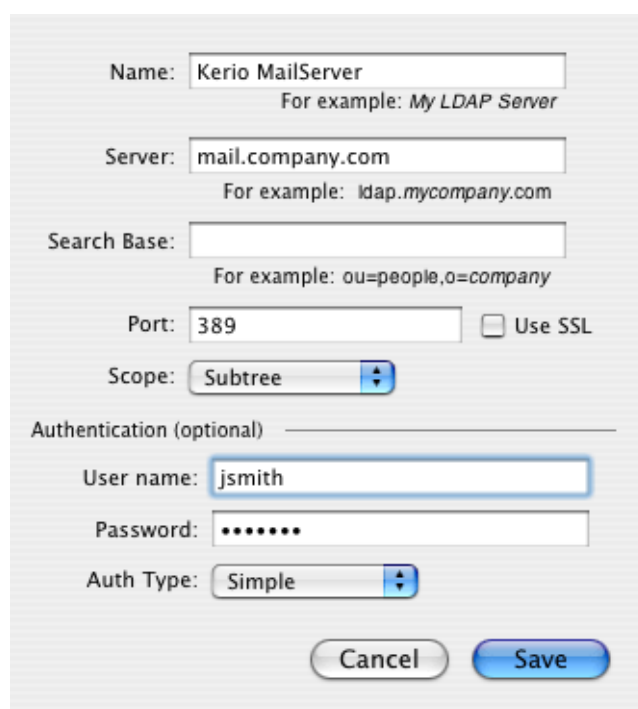
35.2 Apple Address Book for Mac OS X 10.3 (Panther) and 10.4 (Tiger)

This version of the address book is newer and, besides searching through the LDAP database, it provides additional features, as follows:

- user authentication at *Kerio MailServer* — private contact folders of the user will be available
- synchronization of contacts by iSync

LDAP searching settings

Apple Address Book parameters can be set under *Address Book* → *Preferences*. This option opens a dialog providing several tabs (refer to figure 35.2). Specification of the LDAP tab is required (see figure 35.1).



The screenshot shows the 'LDAP' tab in the 'Address Book Preferences' dialog. The fields are as follows:

- Name:** Kerio MailServer (with example: My LDAP Server)
- Server:** mail.company.com (with example: ldap.mycompany.com)
- Search Base:** (empty, with example: ou=people,o=company)
- Port:** 389 (with a checkbox for 'Use SSL' which is unchecked)
- Scope:** Subtree (with a dropdown arrow)
- Authentication (optional):** (header for the following fields)
- User name:** jsmith
- Password:** (masked with dots)
- Auth Type:** Simple (with a dropdown arrow)
- Buttons:** Cancel and Save

Figure 35.1 Apple Address Book settings

Name

Server name.

Server

IP address or DNS name of the server where *Kerio MailServer* is running.

Search Base

Optional item.

Port

Port of the LDAP service. The same port as in *Kerio MailServer* must be set.

If you want to use the encrypted connection to the server (*Use SSL*), it is necessary that a trustworthy certificate is set (for details, see chapter 33.5).

Apple Address Book connects to *Kerio MailServer* by encrypted connection using the LDAP Start TLS (RFC 2830) extension. It is necessary to follow these steps when setting the encrypted communication on the *Address Book* → *Preferences* → *LDAP* tab:

1. enable the *Use SSL* option,
2. change the default port 636 to the port used in *Kerio MailServer* for the non-secured LDAP service (typically port 389). In case that you want to use SSL-secured connection to the server (*Use SSL*), a trustworthy certificate installed is required.

Scope

This item defines which folders will be searched through. It is recommended to use the *Subtree* option where the system searches through all contact folders and subfolders.

Authentication

Authentication to *Kerio MailServer*. Set the *Simple* option for the authentication type to make it possible to specify username and password to the corresponding user account.

Synchronization

Address book synchronization can be set under *Address Book* → *Preferences*. To enable synchronization, use the corresponding option on the *General* tab (see figure 35.2).

Check the option *Synchronize with Exchange* to enable synchronization. Click *Configure* to open an advanced settings dialog (see figure 35.3):

User Name, Password

Username and password for the corresponding account.

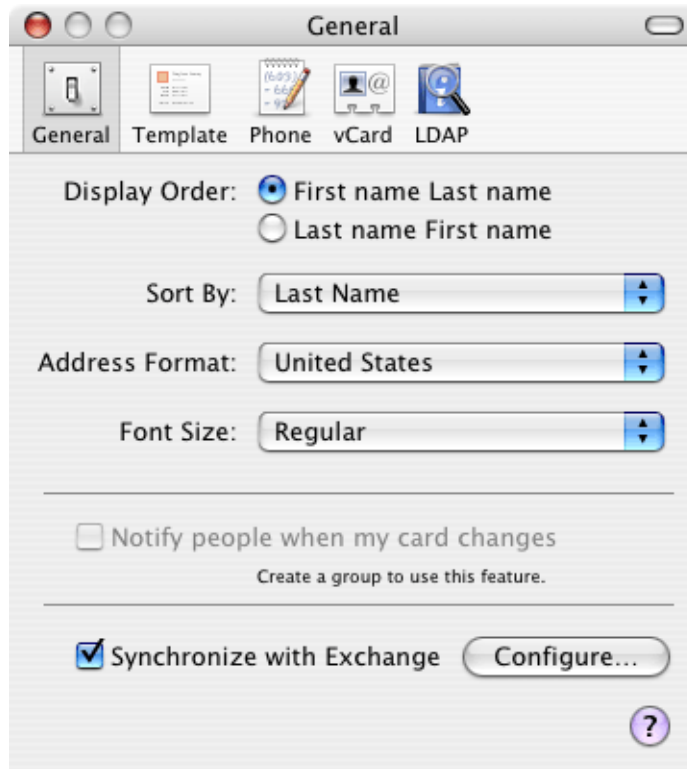


Figure 35.2 Enabling synchronization

Outlook Web Access Server

Synchronization is performed via the WebDAV interface. Therefore, it is necessary to specify this entry by the full path to the corresponding account in the following form:

`http://mail.company.com/exchange/jsmith`

Synchronize every hour

If this option is checked, synchronization is performed once an hour.

The synchronization uses *Apple iSync*. This application enables synchronization on various *Mac OS X* systems. In this application, synchronization can be started by hand any time (unless the every hour synchronization mode is set in the *Apple Address Book*). These settings are different for *Mac OS X 10.3 Panther* and for *Mac OS X 10.4 Tiger*:

Mac OS X 10.3 Panther

Follow these instructions:

1. Set *Apple Address Book* correctly (see above).
2. Run the *Apple iSync* application

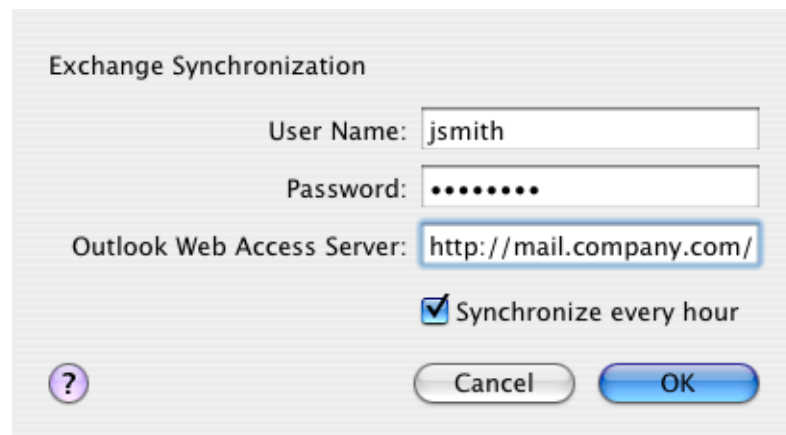


Figure 35.3 Synchronization setup

3. A dialog box with the *Exchange* icon is displayed. The window also includes the *Sync now* button.
4. Click *Sync now* to synchronize contacts.

Mac OS X 10.4 Tiger

Follow these instructions:

1. Set *Apple Address Book* correctly (see above).
2. Run the *Apple iSync* application
3. In the *iSync* menu, click on *Preferences*.
4. In the *iSync Preferences* dialog box, check the *Show status in menu bar* option (see figure 35.4).

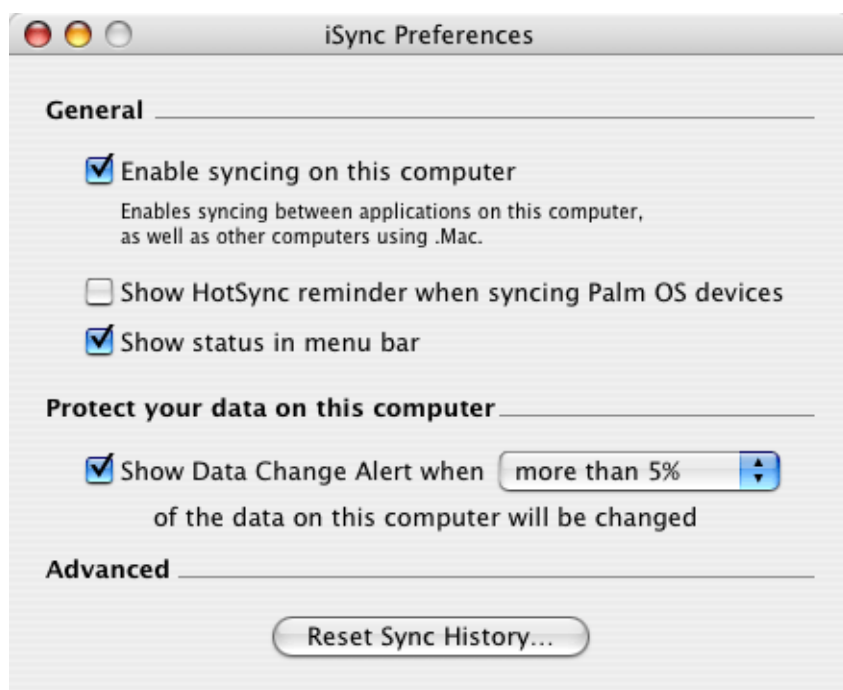


Figure 35.4 iSync Preferences

5. Now, it is possible to synchronize *Apple Address Book* whenever needed. A synchronization icon appears in the right top corner of the screen. Click this icon and select *Sync Now* in the menu (see figure 35.5).

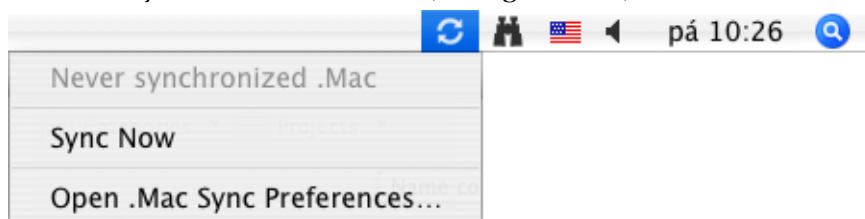


Figure 35.5 Starting synchronization

Chapter 36

Support for Apple Mail 10.4

Since version 6.1.2, *Kerio MailServer* supports some groupware features of IMAP and Entourage accounts in *Apple Mail 10.4*. The support enables to display events, contacts and task folders in the email client.

Cooperation of *Kerio MailServer* with *Apple Mail* is supported directly. This implies that it is not necessary to install any extensions to client stations. However, it is necessary to enable the support in the *Kerio MailServer's* configuration file:

1. Stop *Kerio MailServer* — before any manual edits in configuration files, it is necessary to stop *Kerio MailServer Engine* first.
2. In the directory where *Kerio MailServer* is installed, look up the `mailserver.cfg` file and open it.
3. Search the line including the `IMAPFullListing` value and rewrite the 0 digit with the 1 value.
4. Save the change and start *Kerio MailServer*.

Setting of the full support for IMAP in *Kerio MailServer* results in the situation where all users using IMAP to access their email share all types of folders and subfolders (email messages, calendars, contacts, tasks) in their email clients. However, these folders will be showed as email folders where any event, contact and task will be displayed as an email message with an attachment in the `.vcf` (contact) or `.ics` (event, task) format. For this reason, it is recommended to consider carefully whether the full support for IMAP in *Kerio MailServer* is really efficient.

For proper functionality of *Apple Mail* accounts, the following services must be running in *Kerio MailServer*:

- *HTTP(S)* — applied to Exchange accounts, if used.
- *IMAP(S)* — used both by IMAP and Exchange accounts.
- *SMTP(S)* — the protocol is used for email sending.

36.1 Exchange account in Apple Mail

Support for *Apple Mail* in Exchange accounts results in displaying of all calendar folders included in a particular user account in *Kerio MailServer*. *Apple Mail* does not support the calendar view mode and therefore each event is displayed as one email message. Such messages include an `.ics` attachment with all data associated with the corresponding event.

Thus, each event can be simply imported to *Apple iCal* (for details, see chapter 34) where it can be displayed easily.

36.2 IMAP account in Apple Mail

As well as plenty of other email clients, *Apple Mail* does not support displaying of calendars, contacts and tasks. Full support for IMAP accounts in *Kerio MailServer* enables to view any folder types in any client where IMAP is supported. Once the *Kerio MailServer* configuration file is set, all IMAP accounts will display these folder types:

- mail
- contacts
- calendar
- tasks

However, this support is limited by features of individual clients. Therefore, all events, contacts and tasks will be displayed only as email messages with an attachment where all data associated with the corresponding event, contact or task will be included. Events and tasks include attachments in the `.ics` format, contacts include attachments in `.vcf`.

If you use *Apple Mail* as an email application, it is possible to simply import each event to *Apple iCal* (for details, see chapter 34) where it can be viewed in a selected calendar.

Note: Although contacts are saved as `.vcf` attachments, it is not possible to import them to the *Apple Address Book*.

Chapter 37

Kerio Exchange Migration Tool

Kerio Exchange Migration Tool is a tool helping to convert mail accounts from *Microsoft Exchange* to *Kerio MailServer* 6.1 and later. *Kerio Exchange Migration Tool* migrates:

- of user
- mail folders
- contacts
- calendars
- tasks
- aliases

Kerio Exchange Migration Tool does not migrate:

- public folders
- rights to private folders — shared and mapped (when the migration is finished, it is possible to set sharing again both in *MS Outlook* and in the *Kerio WebMail* interface)

To establish connection with *Kerio MailServer* and *MS Exchange* server, the migration tool uses MAPI interface. MAPI (Messaging Application Programming Interface) is a versatile interface developed by *Microsoft*. It is helpful especially for developing various modules for *MS Outlook*. In this case, MAPI is used to copy contents of user folders from one server to another.

To connect to *MS Exchange*, *MS Outlook* also uses MAPI interface. *Kerio Exchange Migration Tool* connects to *MS Exchange* the same way as *MS Outlook*, i.e. via a standard MAPI interface.

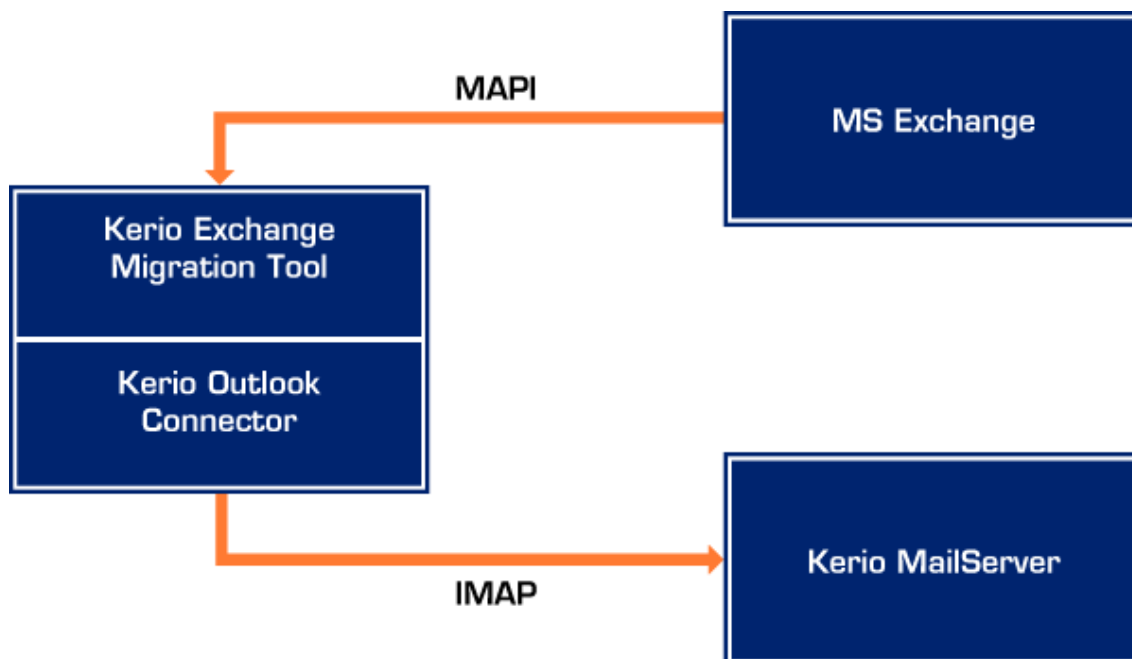


Figure 37.1 Kerio Exchange Migration Tool

The migration tool connects to *MS Exchange* only with read access rights. Therefore, the original *MS Exchange* accounts are kept intact and their functionality is not endangered. This implies that the migration cannot damage these account by any means.

During the migration, accounts are created in *Kerio MailServer* for which new passwords are generated automatically and where contents of *MS Exchange* are copied.

If you do not wish that passwords are generated for users of the migrated accounts, create user accounts in *Kerio MailServer* before the migration. This may be done either by their import or mapping to *Kerio MailServer*.

For user import or mapping from the Active Directory, users will use their original Active Directory passwords to connect to *Kerio MailServer*. User import from NT or Active Directory domain is described in chapter regarding *Kerio MailServer's* user accounts.

If the user accounts already exist in *Kerio MailServer*, new mailboxes are not create nor new passwords are generated. In such a case, the migration tool only copies contents of *MS Exchange* user accounts to *Kerio MailServer*. Users login to their mailboxes by their original password.

The *Master Password* is used to create new accounts and to login to them. It is necessary to set this password in *Kerio MailServer* before the migration is started (refer to chapter 37.3).

The migration can take even several hours, depending on the volume of migrated data. When the migration process is completed successfully, an automatic installation of *Kerio*

Outlook Connector on users' client devices is offered by the wizard (see chapter 37.1) so that users can access their *Kerio MailServer* accounts as soon as possible. This part of the migration is described in detail in chapter 37.7.

The migration supports the following versions of *MS Exchange*:

- MS Exchange Server 5.5
- MS Exchange Server 2000
- MS Exchange Server 2003

Performed by a standard wizard accompanied with explanatory hints, the migration is easy and almost fully automated.

The *Kerio Exchange Migration Tool* for migration from *MS Exchange* to *Kerio MailServer* is available charge-free at the *Kerio Technologies* web site.

37.1 About Kerio Outlook Connector

Kerio Outlook Connector is a MAPI provider enabling to use *MS Outlook* as a client of *Kerio MailServer*. *MS Outlook* with *Kerio Outlook Connector* installed can handle groupware data (contacts, calendars, tasks) saved in *Kerio MailServer's* store. The main benefit of the shared data store is that the data is available via the Internet anywhere necessary.

37.2 Kerio Exchange Migration Tool Installation

Kerio Exchange Migration Tool can be installed at the following *Windows* operating systems:

- Windows NT 4.0 with Service Pack 6a — if this operating system is used, Microsoft Internet Explorer 4.01 with the update 2 or later of Service Pack is required (this browser includes necessary libraries, missing in earlier versions of MSIE versions).
- Windows 2000
- Windows XP
- Windows 2003

Installation wizard is used for *Kerio Exchange Migration Tool* installation. The installation process includes automatic installation of a special version of *Kerio Outlook Connector* (*MS Outlook* is not required for the installation) which is necessary for accessing *Kerio MailServer* via the MAPI interface.

To enable smooth installation process, the following conditions must be met: Installation can be started on a computer where *MS Exchange* from which accounts will be migrated to *Kerio MailServer* is running or on any other host belonging to the same domain as the *MS Exchange* (refer to section [37.5](#))

37.3 Migration requirements

MS Exchange settings

Settings to be done at *MS Exchange* are as follows:

1. It is strongly recommended to backup all data that will be migrated.
2. *MS Exchange* and *Kerio MailServer* must be running.
3. The correct configuration of the administrator's account. The administration account must be set properly, as to enable smooth migration, it is necessary to login at the domain as an *MS Exchange* administrator. This administration account must have a user mailbox in the domain accounts of which will be migrated. It is necessary that the mailbox has the same name as the administrator's username.

It is also necessary that appropriate *MS Exchange* administration rights are set for the administrator's account. The rights must allow accessing user accounts (*Service Account Admin*).

4. It is strongly recommended to block delivery of new mail to user accounts during the migration (to stop the SMTP service).
5. It is also recommended to disable accessing user accounts by their users during the migration.
6. If *MS Exchange* and *Kerio MailServer* are running at the same host, the IMAP service at default port 143 must be stopped at *MS Exchange* before the migration is started. This service at port 143 is used by *Kerio MailServer* for the migration.

Settings of Kerio MailServer

Settings to be done at *Kerio MailServer* are as follows:

1. The IMAP service at default port 143 must be enabled and running. If *Kerio MailServer* is located outside the local network, it is necessary to check whether the service at the default port is enabled at the firewall and whether it is available.
2. *Master Password* must be set and defined in *Kerio MailServer*. *Master Password* is a special password used for creating new accounts in *Kerio MailServer*. This password can be set in the *Configuration* → *Advanced Options* section in the administration console (on the *Master Authentication* tab).
3. If Active Directory is being used, it is recommended to interconnect the domain in *Kerio MailServer* with the Active Directory, or to import Active Directory accounts to *Kerio MailServer*. This can be done in *Configuration* → *Domain Settings* → *User Accounts* by the *Import* button. If user accounts are imported, it is not necessary to generate new user passwords for the accounts.

37.4 Recommendations

Duration of the migration process

Migration of user accounts may take several hours. The more accounts migrated, the longer it takes (this is evident especially when all accounts are migrated). Therefore, it is recommended to divide accounts in groups and migrate them group by group in case that the volume of migrated data is too extensive.

Test User

If this is the first time you perform the migration, it is recommended to create a special test user at *MS Exchange* and perform a testing migration first.

This test checks whether there are not any problems, such as problems in communication of the migration tool with *MS Exchange* or *Kerio MailServer*.

Mail delivery during migration

For successful migration, it is necessary to minimize differences between *MS Exchange* accounts and accounts in *Kerio MailServer*. Therefore, it is recommended to:

- stop delivery via SMTP server,
- make sure that users cannot access their accounts and change their contents during the migration.

Note: It is recommended to perform migration on weekends or at night when the server is not used that much.

Addressing folders migration issue

During migration, problems with movement of folders may occur. These problems are usually caused by inconsistencies in folder names, as follows:

- Folder name includes characters or symbols that cannot be used for creating folders in *Kerio MailServer*. The following symbols are disallowed in folder names: \ (backslash), / (slash) and . . (parent directory). If any folder name includes any of these symbols, the folder will not be migrated and the migration will continue by migrating other items.
- A folder name is identical with a name of any *Kerio MailServer's* system folder — in this case, the folder is not migrated.
- A folder name is duplicated — this problem may occur if an account has already been migrated or when an *MS Exchange* user uses the same name for two or more folders. The migration tools solves this issue by indexing these folders by numbers.

37.5 Migration with full support for UNICODE

Under certain conditions, *Kerio Exchange Migration Tool* enables migration with full support for UNICODE. This means that all messages will be migrated correctly, regardless of localization set in *MS Exchange* or on client hosts.

Migration conditions

First, all conditions and recommendations mentioned in chapters 37.3 and 37.4 must be met.

In addition, this type of migration requires special conditions to be encountered:

- Migration in UNICODE is supported only from *MS Exchange 2000* and later (*MS Exchange 5.5* does not support UNICODE).
- The migration must be running at a third host which belongs to the same domain as *MS Exchange*.
- *MS Outlook 2003* must be installed on the host where the migration is running. *MS Outlook 2003* provides the MAPI subsystem which fully supports UNICODE.

MS Outlook 2003 must be installed before the migration tool.

- The parameter with DNS name (it is not possible to use IP address) of the server where *MS Exchange* is running must be included in the command which starts the migration tool. Two methods can be used to specify this parameter:

1. Using the command:

```
mgrwzrd exchange.company.com
```

2. By changing the path in the *Kerio Exchange Migration Tool's* shortcut (*context menu* → *properties*).

The path is changed by adding DNS name of the server with *MS Exchange* to the destination path of the application. The following format will be used for a standard path in the *Target* entry:

```
"C:\Program Files\Kerio\MailServer Migration\MigrWzrd.exe"  
exchange.company.com
```

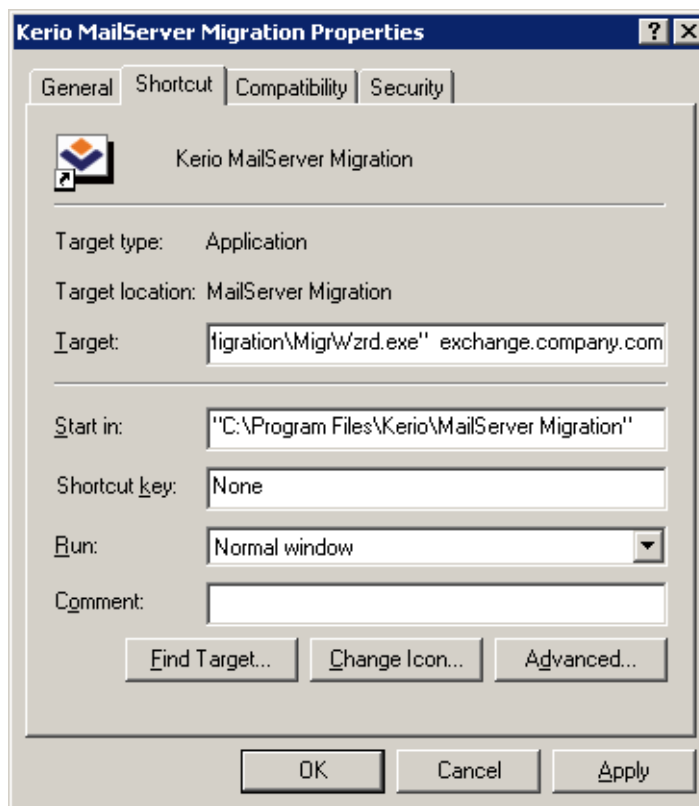


Figure 37.2 Changing the path

3. Migration can be started only by users with administration rights for *MS Exchange* (see Step Three in chapter 37.3).

37.6 Migration Wizard

The migration wizard helps you migrate accounts:

The first two dialogs provide basic information for starting the migration. Please, read carefully all comments and instructions provided by the migration wizard.

The third dialog checks and informs whether it is possible to run the migration (see figure 37.3). This may takes several minutes.

MAPI detection

The migration tool checks whether it is possible to communicate with the *MS Exchange* server via the MAPI interface.

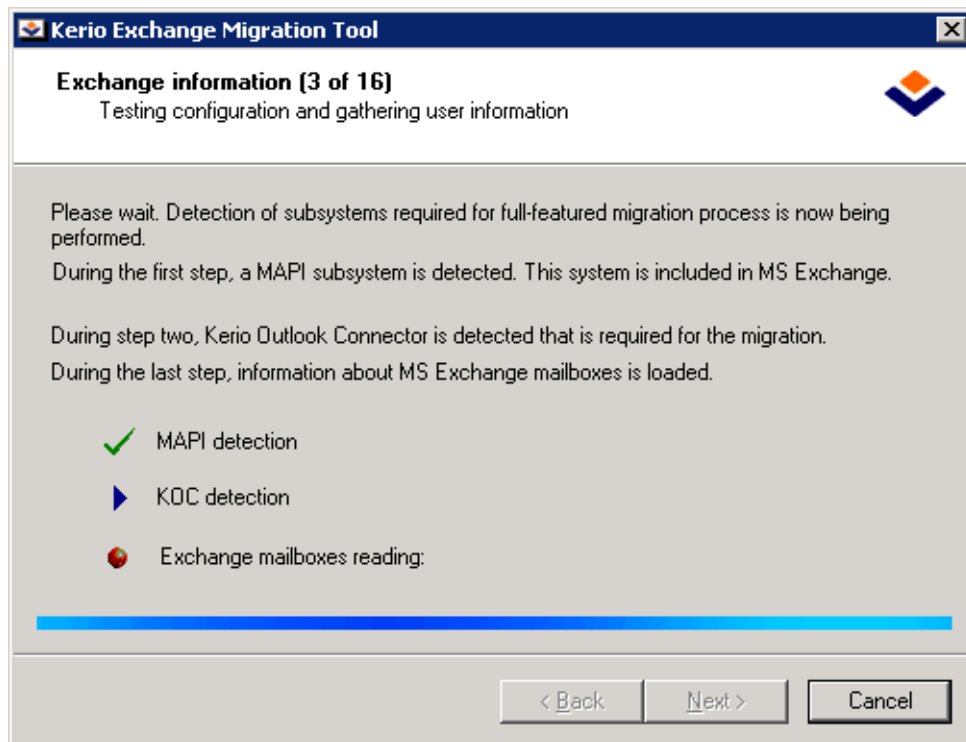


Figure 37.3 Migration Wizard — connection check

KOC detection

The migration tool also checks whether installation of *Kerio Outlook Connector* was completed successfully. *Kerio Outlook Connector* enables connection to *Kerio MailServer*.

Exchange mailboxes reading

In addition, the migration tool checks connection to *MS Exchange* and imports basic information about mail accounts.

Results of this step are logged in `MigrWzrd.log` (for details, check chapter 37.9).

In the step four (see figure 37.4), a list of users downloaded from the *MS Exchange* server is provided. Check boxes next to usernames for users to be migrated.

All accounts can be checked by the *Select All* button.

The *Invert selection* option checks unchecked items and vice versa (this option is helpful especially if almost all accounts are to be migrated except few ones).

The fifth dialog window informs about *Kerio MailServer* settings that are necessary to be taken before the migration is started.

In step six (see figure 37.5), specify IP address or name of the destination server and the *Master* password:

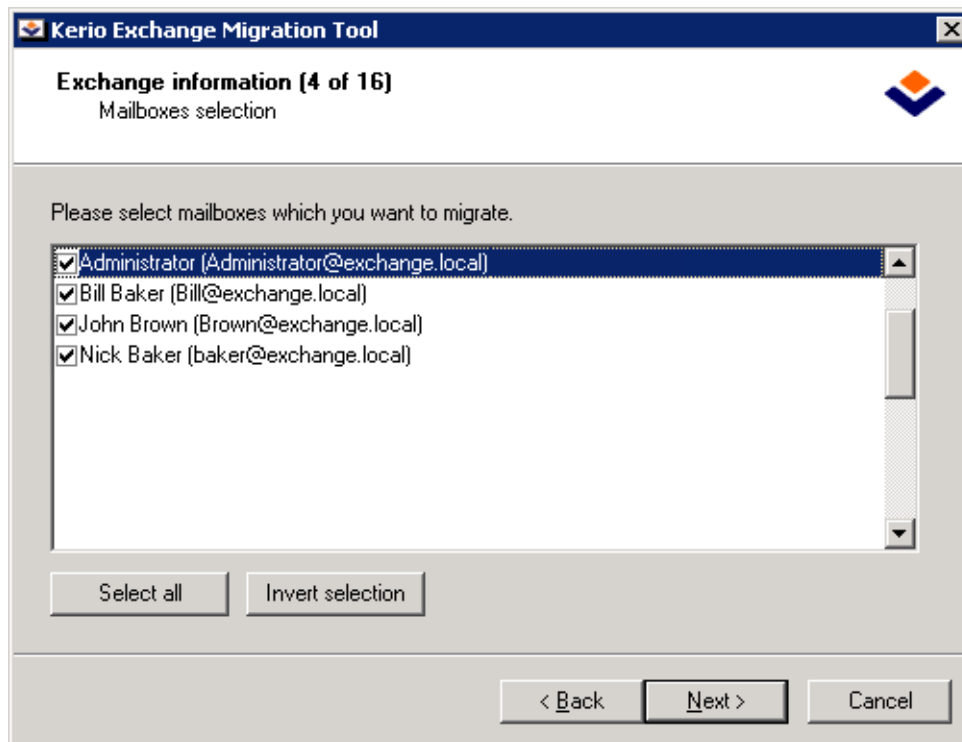


Figure 37.4 Migration Wizard — selection of user accounts

Kerio MailServer

Name or IP address of the destination *Kerio MailServer* where the data will be copied.

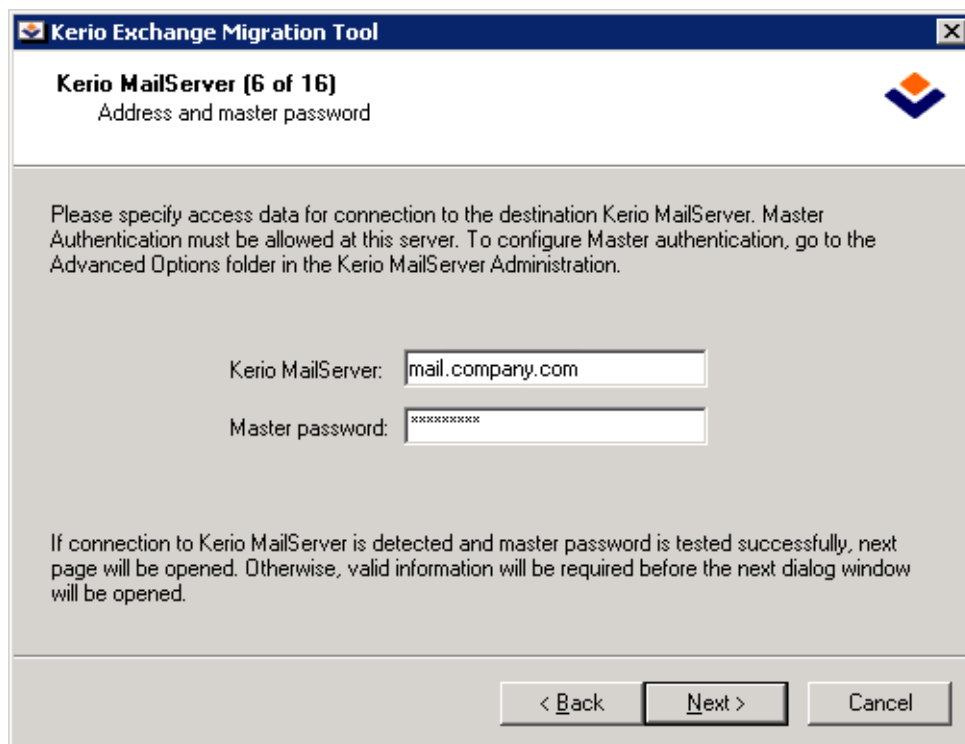


Figure 37.5 Migration Wizard — destination server address and Master Password

Master password

Master Password is a special password used for simultaneous access to multiple accounts without corresponding user passwords. Master password is used for creating new *Kerio MailServer* accounts and setting of new passwords.

Master Password can be set in *Kerio MailServer*, in the *Configuration* → *Advanced Options* section of the administration console (on the *Master Authentication* tab).

In step seven (see figure 37.6), accounts to be migrated can be checked. The *START* button runs migration of the accounts. The process may take several hours, therefore, it is recommended to migrate user accounts at night or on weekends.

The eighth window (see figure 37.7) displays the migration process status.

migration can be cancelled by the *Cancel* button, if necessary.

If the migration process is stopped and cancelled, accounts already migrated to *Kerio MailServer* will be available and functioning. For the account where the migration was stopped, only the part already migrated is available. The smallest indivisible item is a message. This means that just the last message (and all messages not having been migrated yet) where the process is stopped is not migrated.

Warning: If the migration is repeated once it is cancelled, it is recommended not to

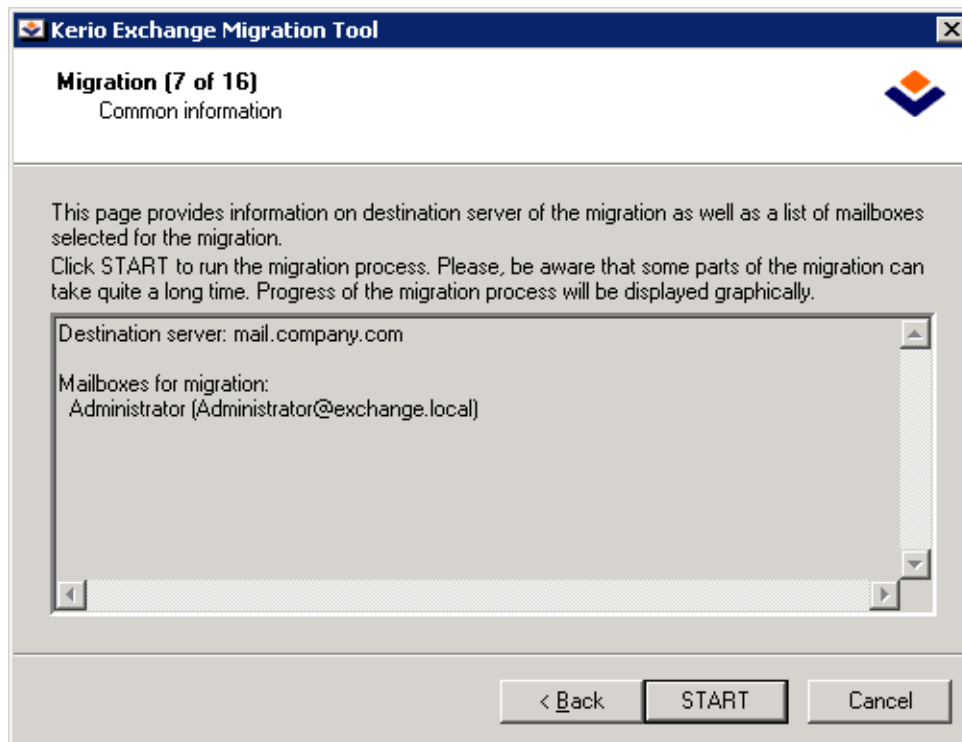


Figure 37.6 Migration Wizard — destination server information

include accounts already migrated. This might cause the following consequences:

- Duplicity of folders created by the same user — if folder names collide (there already exists a folder with the same name), the copied folder is stored and marked by an index number. All such folders will be duplicated.
- Duplicity of items in default folders (*Inbox*, *Sent Items*, *Deleted Items*, *Contacts*, *Calendar*, *Tasks*, etc.) — although these folders are not duplicated, during repeated migration, all items (mail, contacts, tasks, events) are copied again to the folders (all items are duplicated in the particular folders).

Mailbox

Name of the account currently being migrated.

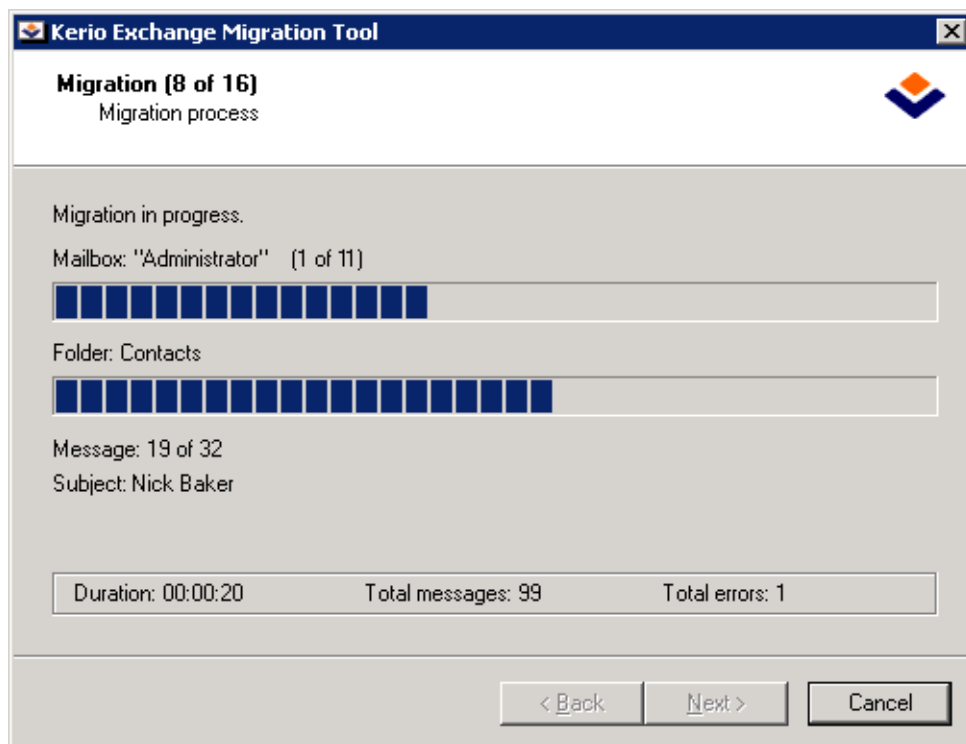


Figure 37.7 Migration Wizard — migration process status

Folder

Name of folder currently being migrated.

Message

Number of messages (of the total count in the corresponding folder) already having been migrated.

Subject

Subject of the message currently migrated.

During the migration, messages may be displayed incorrectly even if the migration with the full support for UNICODE was used (refer to chapter 37.5). All these messages should be migrated correctly, they are displayed incorrectly only in the migration wizard since it does not support for UNICODE.

Step nine (see figure 37.8) informs whether the migration has been completed successfully. It also includes the migration process log. It is recommended to check this information carefully to make sure that all accounts have been migrated to *Kerio MailServer*. This log is described in detail in chapter 37.9.

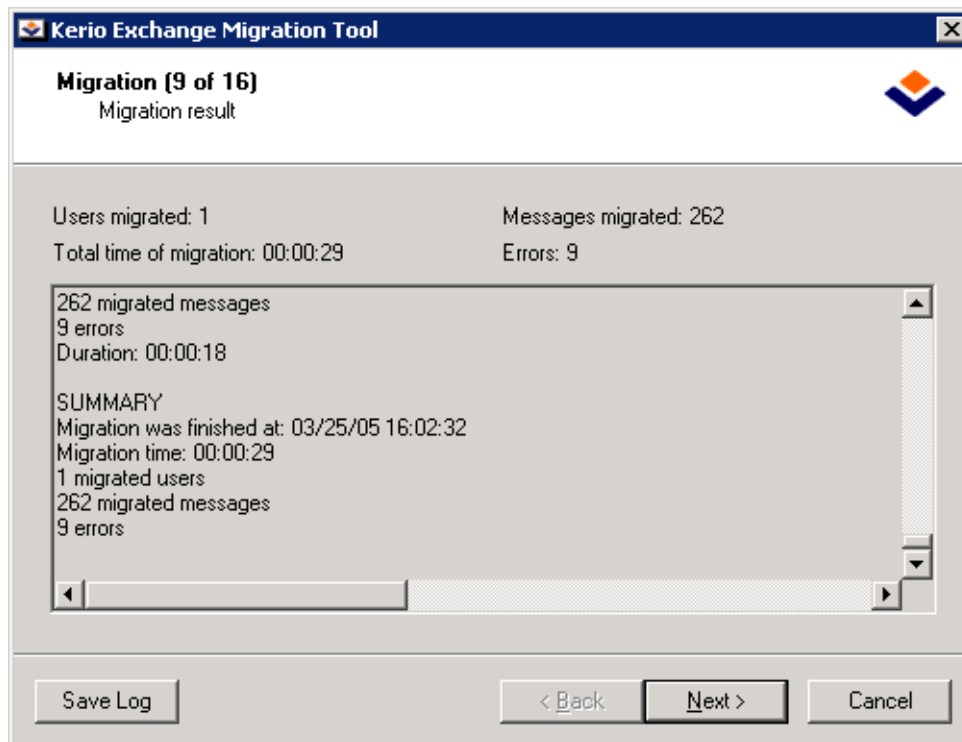


Figure 37.8 Migration Wizard — information about the migration process

To make *MS Outlook* groupware functions fully available in users' accounts in *Kerio MailServer*, it is necessary to extend *MS Outlook* on client computers by *Kerio Outlook Connector*. In step ten (see figure 37.9), you can either prepare conditions for automatic installation of *Kerio Outlook Connector* (for detailed description on the automatic installation, check chapter 37.7) or decide to install the installation on client stations manually. In the second case, it is possible to close the wizard at this point.

Check *Start installation upload* to import *Kerio Outlook Connector* automatic installation files to the file server.

Click *More info* to view information on *Kerio Outlook Connector's* automatic installation requirements. To avoid possible problems, read this information carefully.

In the eleventh dialog (see figure 37.10), specify network path and administration password for the automatic installation:

Network path

Definition of the network path to the file server (or a location at any network disk) where *Kerio Outlook Connector* will be installed to the client station from. This location must be available for all local users. The network path can also be specified by hand in the *Network path* entry or it can be browsed using the *Browse for folder* dialog.

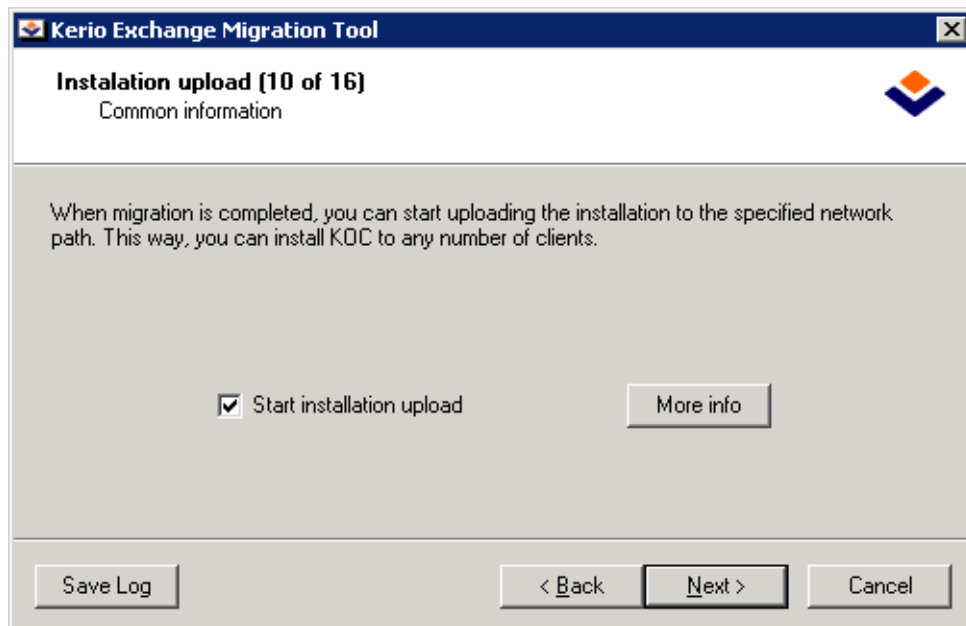


Figure 37.9 Migration Wizard — starting automatic installation

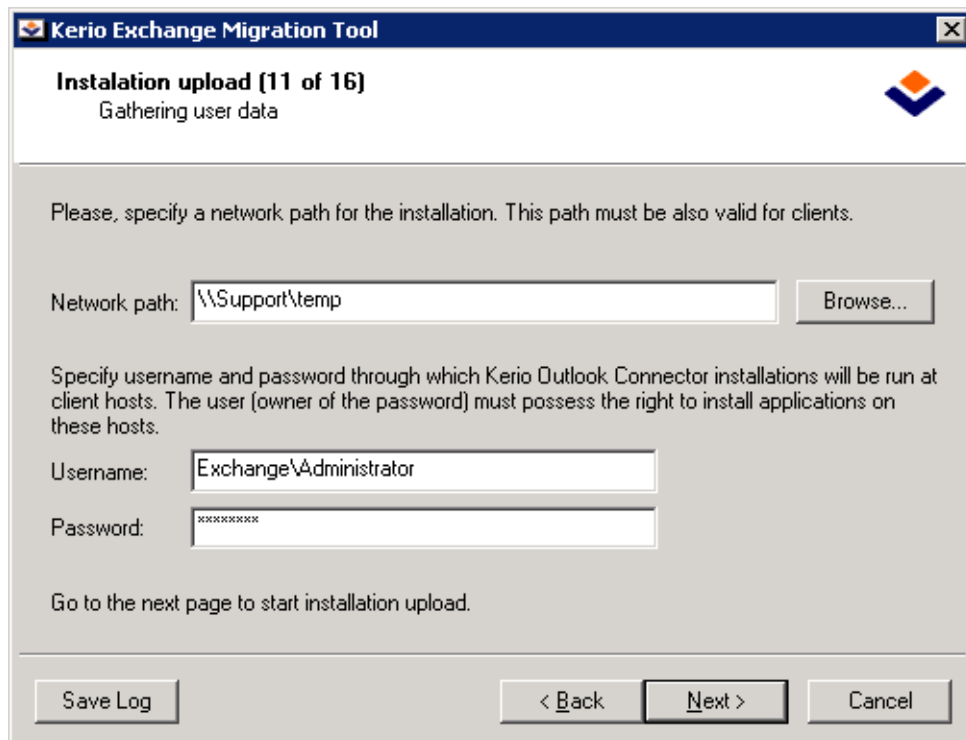


Figure 37.10 Migration Wizard — automatic installation settings

Username, Password

Administration username and password for the domain that will be used for installation at all the clients (under *Windows* operating systems, installations must be performed from an account with administration rights). This username and password will be secured by an encryption.

The next step of the wizard provides information about the installation process and results. If the installation was performed correctly and completed successfully, it is possible to tell users by automatically generated email messages. If you do not wish to inform users, uncheck the *Inform users* option in step thirteen (see figure 37.11) — in such a case, the wizard will be closed in the following step.

If you decide to inform users by an email message providing username, password and link to the *Kerio Outlook Connector* automatic installation, check the option and continue by switching to the following dialog box. The email body is described in chapter 37.8.

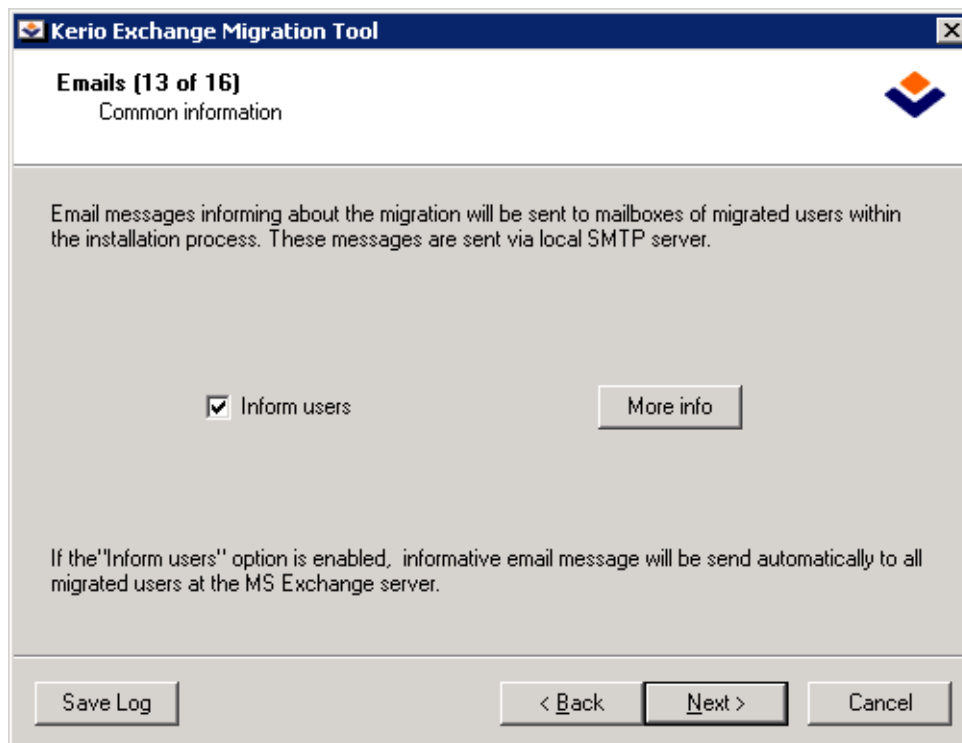


Figure 37.11 Migration Wizard — sending informative email to users

Inform users

This option sends automatic email to all users whose accounts were migrated to *Kerio MailServer*. If you do not wish to send an automatic email message including information about how to install *Kerio Outlook Connector* and handle the account in *MS Outlook*, disable the option. In the next step, close the wizard.

Click *More info* to view important information regarding automatically sent messages. To avoid unnecessary problems, read this information carefully.

Sending results are displayed when the automatic mail is sent.

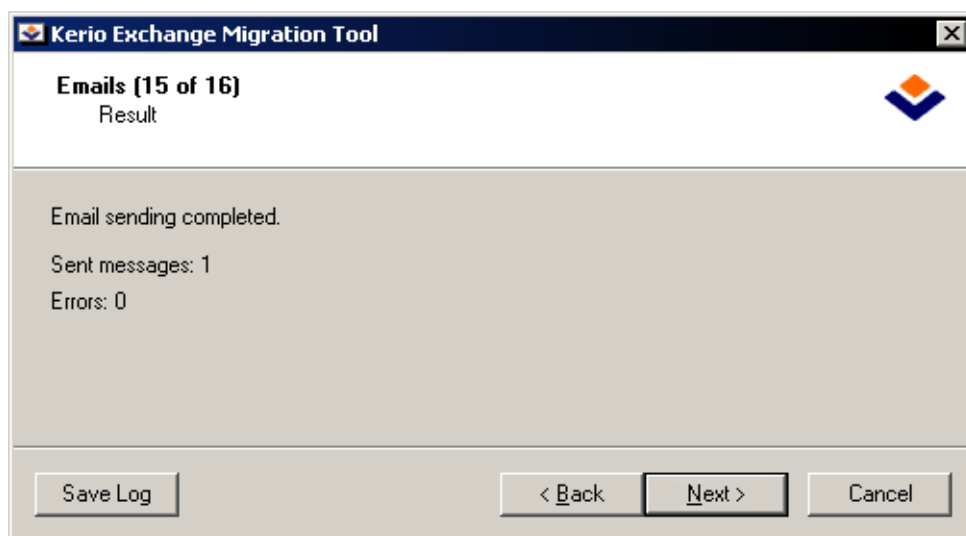


Figure 37.12 Migration Wizard — email sending results

Step sixteen (see figure 37.12) closes the migration.

37.7 Kerio Outlook Connector automatic installation

When the migration is completed successfully, the wizard offers automatic installation of *Kerio Outlook Connector* to users' client hosts. This feature enables users to connect to their *Kerio MailServer* accounts as soon as possible. To set the automatic installation, it is necessary to specify network path to the file server or to a location in the network which is available to all users.

It is also necessary to specify the domain administration username and password which can be used for installation at all clients (under *Windows* operating systems, installations must be performed by users with administration rights). This username and password will be protected by an encryption so that they cannot be read and misused. In spite of this fact, it is recommended to create a special administration account for the automatic installation purpose and to remove the account when the installation is completed.

During the installation, an installation package is saved in the location defined that includes *Kerio Outlook Connector*, encrypted username and password as well as the administration account password and a special script which starts the installation.

When the automatic installation is ready in the file server, the administrator can make server send automatic email informing users about the migration. This email is sent via *MS Exchange* to the original accounts (these accounts are still available). To ensure that this operation is performed smoothly, it is necessary to allow anonymous access at the local SMTP server.

The email message includes DNS name or IP address of the host where *Kerio MailServer* is running, login name and optionally also the password generated during the migration process. It also contains a short explanatory text and a link which starts the *Kerio Outlook Connector* installation.

The link runs *User Profile Creator*, an application which installs *Kerio Outlook Connector* at the client. If unable to run the installation, check the following issues:

1. Version of *MS Outlook*. In case of older versions, the recommended updates should be installed:
 - MS Outlook 2000 + version Service Pack 3 (if the service pack version is not installed, *Kerio Outlook Connector* installation cannot be started)
 - MS Outlook XP + version Service Pack 3 (the version of *MS Outlook XP* must have this format: 10.0.6515.xyz)
 - MS Outlook 2003 + version Service Pack 1 (if the service pack version is not installed, *Kerio Outlook Connector* installation cannot be started)
2. Check whether the user can access the network disc where the installation package is stored.

If none of these problems is detected, *User Profile Creator* starts a hidden installation (this implies that the user cannot control the installation). The profile settings issue is described in detail in chapter 37.8. In addition, *User Profile Creator* starts another application, called *makeprof*, which creates a new user profile at client hosts. This profile, called *Kerio*, includes their migrated MAPI account.

37.8 Creating profiles at user computers

If the automatic installation option was used, an email message regarding information about the accounts and installation is sent to users. The message has high priority and it is as follows:

This message was generated

The migration process completed successfully.

New server address: mail.company.com

Your login name: jsmith@company.com

Your new password: D4995F

To enable Microsoft Outlook with MAPI provider, Kerio Outlook Connector - a MAPI implementation developed by Kerio Technologies — must be installed first. Kerio Outlook Connector is an extension to MS Outlook. Kerio Outlook Connector can be installed on Microsoft Windows 2000 Family, Microsoft Windows XP, Microsoft Windows 2003 Family. It allows users to work with groupware data (contacts, calendar, tasks) stored in Kerio MailServer location.

MAPI (Messaging Application Programming Interface) is a universal open messaging interface that allows the MAPI client to work with any mailserver (e.g. Microsoft Outlook Kerio MailServer). Then, a profile for the Microsoft Outlook must be created. Follow this link to start an automatic installation of the Kerio Outlook Connector and to create a user profile. Run the installation. (\\Kms-exchange\temp\MAPI\install.bat)

If you want to use a standard IMAP or POP3 client (such as Microsoft Outlook, Microsoft Outlook Express, Mozilla, Eudora, etc.), create a special account and define its parameters, or contact your administrator.

If you want to access KMS via the WebMail interface, please follow this link

Should any issues arise, please contact your administrator.

Within the installation of *Kerio Outlook Connector*, basic configuration of the profile and user account is set.

Upon clicking on the link provided in the email message, a dialog is opened where it is necessary to specify email address and password for the particular mailbox (see figure 37.13).

The installation is started when these items are specified. If the installation is completed successfully, the new *Kerio* profile is created at client hosts. This profile includes user accounts connected via *Kerio Outlook Connector*.

Note: If *Kerio Outlook Connector* is installed in *MS Outlook 2000*, additional configuration of the profile created is necessary. The *Outlook Address Book* service must be added by hand in the profile.

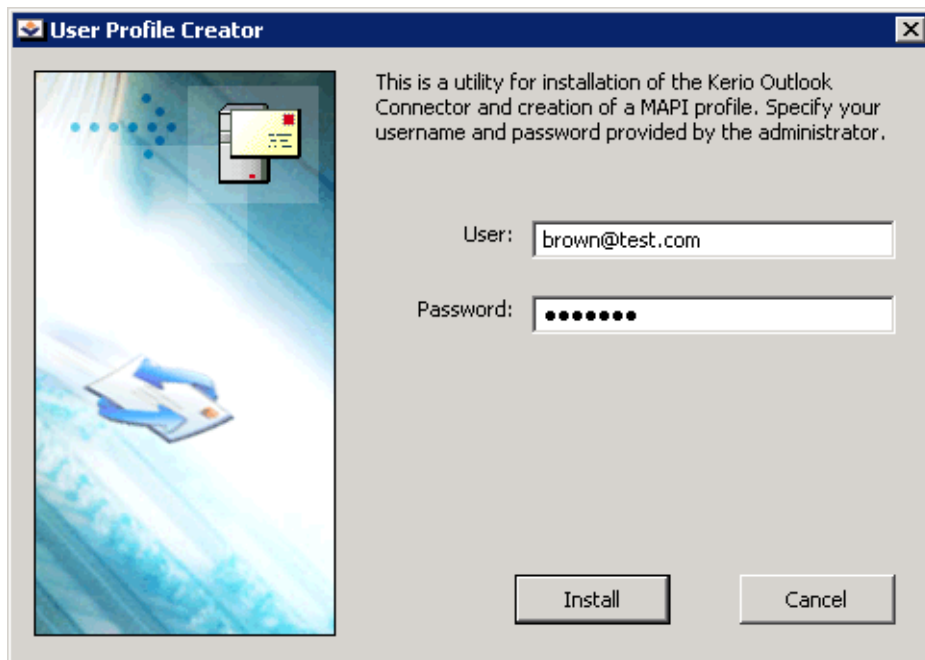


Figure 37.13 User profile creator

Warning: EachMS Outlook profile may be used only by one account connected via *Kerio Outlook Connector*. Functionality of POP3 and IMAP accounts located in the same profile is not affected by *Kerio Outlook Connector Store*.

37.9 Log

The migration process is logged in `MigrWzrd.log`. This log is stored in the directory where the migration tool is installed and where it can be run from.

The log is always saved in the same file. This implies that each migration log rewrites the previous one. Therefore, it is recommended to backup each log when the migration is completed.

`MigrWzrd.log` keeps information about the migration process as well as about the process of the automatic installation import and email distribution.

Migration process log

Creating a new account in *Kerio MailServer*:

User `jsmith@exchange.local` (password = 1F98AC) was created at the destination server.

The log informs that a new account was created and a new password was generated. If the accounts were imported to *Kerio MailServer* before the migration, the password generated will not be used. Even this information is provided in the log:

User `jsmith@exchange.local` already exists at the destination server. (The original password will be used).

Here is an example by a log of a user account completely migrated:

Migration of user adm@exchange.local in progress.

Copying folder hierarchy

Copying the Deleted Items folder

226 messages

Copying the Sent Items folder

625 messages

Copying the Outbox folder

1 messages

Copying the Inbox folder

15 messages

Folder: Signed

12 messages

Folder: Work

522 messages

Copying the Calendar folder

260 messages

Copying the Contacts folder

496 messages

Copying the Drafts folder

5 messages

Copying the Journal folder

0 messages

Copying the Notes folder

0 messages

Copying the Tasks folder

124 messages

Copying other folders

0 messages

2286 migrated messages

0 errors

Duration: 00:20:37

The migration log also provides the complete count of users and messages migrated.

Log for the installation package import and informative mail delivery

When the migration is completed, it is possible to continue by importing the *Kerio Outlook Connector* installation package to the file server (refer to chapter 37.7).

The information about this process is also logged in `MigrWzrd.log`. Here is an example of the installation import log:

Uploading installation.

Copying process completed successfully.

The `\\Kms-exchange\temp\MAPI\install.bat`

installation file has been created successfully.

The last section of this log includes information about sending of informative messages:

An email message was sent to `baker@exchange.local`.

An email message was sent to `smith@exchange.local`.

An email message was sent to `wayne@exchange.local`.

It is also possible to save the log in another, user-defined location. This can be done by using the *Save log* button at the bottom of each installation wizard step.

Chapter 38

Technical support

Kerio Technologies provides free email and telephone support for *Kerio MailServer* to registered users. For contacts, see the end of this chapter. Our technical support staff is ready to help you with any problem you might have.

You can also solve many problems alone (and sometimes even faster). Please perform the following before you decide to contact *Kerio Technologies* technical support:

- Try to look up the answer in this manual. Its chapters describe the functions of *Kerio MailServer* and how to use them for optimizing server settings in detail.
- If the answer cannot be found in this manual, refer to:
 1. the *Kerio MailServer* website (<http://www.kerio.com/kms>)
 2. our technical support website (<http://www.kerio.com/support>)
- Another useful information source is the discussion forum of *Kerio MailServer* users — go to <http://forum.kerio.com/> and the knowledge base that can be found on <http://support.kerio.com/>.
- Specific issues can be asked via a special technical support form at <http://support.kerio.com/>.

38.1 Contacts

USA

Kerio Technologies Inc.

2350 Mission College Blvd., Suite 400

Santa Clara, CA 95054

Phone: +1 408 496 4500

Email technical support is available at <http://support.kerio.com/>.

<http://www.kerio.com/>

United Kingdom

Kerio Technologies UK Ltd.

Sheraton House

Castle Park

Cambridge, CB3 0AX

Phone: +44 1223 370 136, +44 8707 442 205

Email technical support is available at <http://support.kerio.com/>.

<http://www.kerio.co.uk/>

Czech Republic

Kerio Technologies s. r. o.

Anglicke nabrezi 1/2434

301 49 PLZEN

Phone: +420 377 338 902

Email technical support is available at <http://support.kerio.cz/>.

<http://www.kerio.com/>

Appendix A

Used open-source libraries

This product contains the following open-source libraries:

libiconv

This library provides support for conversions between different encodings through Unicode conversion.

Copyright ©1999-2003 Free Software Foundation, Inc.

Author: Bruno Haible

Kerio MailServer for *MS Windows* includes a customized version of this library.

Customized source code of the *libiconv* library is available as patch at

<http://download.kerio.cz/dwn/iconv-patches>

The patch is designed for *libiconv 1.9.1* which can be downloaded at

<http://ftp.gnu.org/pub/gnu/libiconv/libiconv-1.9.1.tar.gz>

myspell

Spellcheck library.

Copyright 2002 Kevin B. Hendricks, Stratford, Ontario, Canada And Contributors.

All rights reserved.

OpenLDAP

Freely distributable *LDAP (Lightweight Directory Access Protocol)* implementation.

Copyright ©1998-2004 The OpenLDAP Foundation.

OpenSSL

An implementation of *Secure Sockets Layer (SSL v2/v3)* and *Transport Layer Security (TLS v1)* protocol.

This product contains software developed by *OpenSSL Project* designed for use in *OpenSSL Toolkit* (<http://www.openssl.org/>).

PHP

PHP is a widely-used scripting language that is especially suited for Web development and can be embedded into HTML.

Copyright ©2001-2004 The PHP Group.

zlib

General-purpose library for data compressing and decompressing.

Copyright ©1995-2003 Jean-Loup Gailly and Mark Adler.

Glossary of terms

Application protocol

Application protocols are conveyed by packets of the TCP or the UDP protocol. It is used to transfer user (application) data. There are many standard application protocols (e.g. SMTP, POP3, HTTP, FTP, etc.), however, it is possible to develop a custom (non-standard) communication method.

DoS attack

DoS (Denial of Service) is a type of attack when too many concurrent requests overload the system; the server is no more able to respond to the requests of authorized users or fails.

DSN

DSN (Delivery Status Notification) is an information about the email message delivery status. There are a couple of different types of delivery status notification. Unless otherwise specified, users receive only the error messages from the mailserver (deferred, failure).

Email Address

An email address determines the sender and recipient of a message in electronic communication. It consists of a local part (before the @ character) and a domain part (after the @ character). A domain specifies where email be delivered to (a company), a local part specifies a particular recipient within this domain.

ETRN

If you receive email using the SMTP protocol and your server is not permanently connected to the Internet, email can be accumulated at another SMTP server (typically a secondary server for a given domain). When it is connected to the Internet, the SMTP server sends an ETRN command (command of SMTP protocol) and asks for stored emails to be transmitted.

If the given SMTP server doesn't have any messages stored, it doesn't need to reply at all. That's why it is necessary to define a timeout period. If the SMTP server doesn't receive any emails, it terminates the connection after the specified timeout.

Firewall

Software or hardware device that protects a computer or computer network against attacks from external sources (typically from the Internet).

IMAP

Internet Message Access Protocol (IMAP) enables clients to manage messages stored on a mail server without downloading them to a local computer. This architecture allows the user to access his/her mail from multiple locations (messages downloaded to a local computer would not be available from other locations).

It is possible under certain conditions to access the email account using both IMAP and POP3 protocols.

IP

IP (Internet Protocol) is a protocol which uses its data part to convey all the other protocols. The most important information in its header is the source and destination IP address, i.e. by which host the packet was sent and to which host it should be delivered.

IP address

IP address is a unique 32-bit number used to identify the host in the Internet. It is represented by four bytes in the decimal system (0–255) separated by dots (e.g. 200.152.21.5). Each packet includes the information on where the packet was sent from (source IP address) and to which host it should be delivered (destination IP address).

Kerberos

Protocol for secure user authentication in Windows 2000 environments. It was designed by MIT (Massachusetts Institute of Technology) within the Athena project. The protocol is based on such principles where the third side is trustworthy. Users use their passwords to authenticate to the central server (KDC, Key Distribution Center) and the server sends them encrypted tickets which can be used to authenticate to various services in the network.

LDAP

LDAP (Lightweight Directory Access Protocol) is an Internet protocol used to access directory services. Information about user accounts and user rights, about hosts included in the network, etc. are stored in the directories. Typically LDAP is used by email applications to search for email addresses and to delivery management (*Microsoft Active Directory*).

Mailbox Account

A place where email is stored on a server. Clients can download emails from an account (using POP3 protocol) or work with messages directly at the server (using IMAP or Webmail).

The account is physically represented by a directory on a disk. The directory is created in the *Kerio MailServer* directory (mail/domain/username). Other subdirectories representing individual folders are created in this directory.

Glossary of terms

Mailboxes are not created during the definitions of users, the concrete mailbox is created after the first email to this mailbox is received.

MAPI

MAPI (Messaging Application Programming Interface) is an application programming interface (API) designed by *Microsoft*. Any software that supports MAPI can communicate with any mailserver (*Kerio MailServer*) and send and receive data via this interface regardless of their type and software provider.

MX Records

One of the record types that might be saved in DNS. It includes the information about the mailserver for a particular domain (information about which SMTP server email for this domain should be sent to). Multiple MX records may be defined with different MX preference values to denote priority.

NNTP

NNTP (Network News Transfer Protocol) is a simple text protocol that allows for distribution, retrieval and posting of messages on the Internet.

Notifications

Short message (notification) about a particular event — e.g. new email. It is usually sent as a text message (SMS) to a cellular phone.

POP3

Post Office Protocol is a protocol that enables users to download messages from a server to their local computer. It is suitable for clients who don't have a permanent connection to the Internet.

Unlike Internet Message Access Protocol (IMAP), POP3 does not allow users to manipulate messages at the server. Mail is simply downloaded to the client where messages are managed locally. POP3 enables access only to the *INBOX* folder and it does not support public and shared folders.

Port

16-bit number (1–65535) used by TCP and UDP for application (services) identification on a given computer. More than one application can be run at a host simultaneously (e.g. WWW server, mail client, FTP client, etc.). Each application is identified by a port number. Ports 1–1023 are reserved and used by well known services (e.g. 80 = WWW). Ports above 1023 can be freely used by any application.

RFC

Request For Comments. RFC is a set of deliberately recognized standards. It is a set of indexed documents where each document focuses a particular area of network communication.

SMTP

Simple Mail Transfer Protocol is used for sending email between mail servers. The SMTP envelope identifies the sender/recipient of an email.

Spam

Unwanted, usually advertisement email. Spam are usually sent in bulk and the recipient addresses are obtained by illegal means (e.g. by tapping the network communication).

SSL

A protocol used to secure and encrypt the TCP connection. Secure Socket Layer was originally designed by Netscape to secure transmission of web pages using HTTP protocol. Today it is supported by almost all standard internet protocols — SMTP, POP3, IMAP, LDAP, etc.

At the beginning of communication, an encryption key is requested and transferred using asymmetrical encryption. This key is then used to encrypt (symmetrically) the data.

Subnet mask

Subnet mask divides an IP address in two parts: network mask and an address of a host in the network. The mask has the same format as IP addresses (e.g. 255.255.255.0), but it is displayed as a 32-bit number with certain number of left-to-right oriented ones and zeros (mask cannot include other values). Number one in a subnet mask represents a bit of the network address and zero stands for a host's address bit. All hosts within a particular subnet must have identical subnet mask and network part of IP address.

TLS

Transport Layer Security. A later version of SSL, in fact it may be considered as SSL version 3.1. This version is approved by the IETF and it is accepted by all the top IT companies (i.e. Microsoft Corporation).

WAP

Wireless Access Protocol uses a streamlined formatting language called Wireless Markup Language (WML), which allows wireless devices to view Internet content.

WebDAV

Using WebDAV (Web Distributed Authoring and Versioning), users can group-edit and organize files located on servers.

WebMail

Interface used by *Kerio MailServer* to enable access to email through a web browser. Several user settings (such as message filtering, password, etc.) can be also changed using *Kerio WebMail*.

Index

A

Active Directory [108](#)
 user import [109](#)
Active Directory Extensions [270](#)
 installation [271](#)
alias
 control [133, 227](#)
 definition [132](#)
 groups [116, 131](#)
 of user [13, 97, 131](#)
antivirus [169](#)
 attachment filtering [174](#)
 McAfee Anti-Virus [169, 170](#)
 supported external antivirus programs [173](#)
Apple Address Book [382](#)
 synchronization [384](#)
Apple iCal [374](#)
 calendar publishing [376](#)
 settings [374](#)
 subscription to calendars [374](#)
Apple Mail
 groupware support [388](#)
 mailserver.cfg settings [388](#)
archiving [177](#)
authentication methods [143](#)

B

back-up [180](#)
 kmsrecover [185](#)
 recovery [185](#)

C

conflicting software [19](#)

D

deployment examples [234](#)
domain mailbox [123](#)
 X-Envelope-To: [124](#)
domains [60](#)
 aliases [60](#)
 footers [61](#)
 forwarding [61](#)
 primary [26, 57](#)

E

ETRNs [62, 75, 122, 140](#)

F

firewall [142, 232](#)

G

groups
 IP address [51, 85, 89, 90, 126](#)
 user groups [99, 116](#)

H

HTTP [51](#)
HTTP Proxy [149](#)

I

IMAP [13, 51, 226, 230, 231, 232](#)
import
 user groups [108](#)
installation [19](#)
 Linux [22](#)
 MAC OS X [23](#)
 MS Windows [20](#)
Internet connection [71](#)

K

- kerberos [69, 96](#)
 - authentication [280](#)
- Kerio Administration Console [42, 45](#)
- Kerio Exchange Migration Tool [390](#)
 - automatic installation [406](#)
 - installation [392](#)
 - log [409](#)
 - wizard [397](#)
- Kerio MailServer Engine [42](#)
- Kerio MailServer Monitor [42, 42](#)
- Kerio Open Directory Extensions [276](#)
 - authentication settings [277](#)
 - installation [276](#)
 - settings [277](#)
- Kerio Outlook Connector [301](#)
 - contacts forwarding [332](#)
 - data file settings [311](#)
 - folder mapping [318](#)
 - folder sharing [317](#)
 - free/busy [333](#)
 - initial settings [305](#)
 - installation [302, 312](#)
 - MAPI [301](#)
 - Outlook 2000 [313](#)
 - password change [333](#)
 - profile [303](#)
 - rules for incoming messages [320](#)
 - spam filter [328](#)
- Kerio Synchronization Plug-in [337](#)
 - installation [338](#)
 - settings [340](#)
 - synchronization [338](#)
- Kerio WebMail [14, 82](#)
- Kerio Webmail logo [70, 82](#)
- KMS Web Administration [250](#)
 - access rights [251](#)
 - aliases [267](#)
 - groups [261](#)
 - supported browsers [250](#)
 - user accounts [254](#)

L

- LDAP [63, 226](#)
 - Active Directory [63](#)
 - Apple Open Directory [66](#)
 - client settings [187](#)
 - server [187](#)
 - service [51](#)
- logs [214](#)
 - config [217](#)
 - debug [225](#)
 - error [223](#)
 - mail [218](#)
 - security [221](#)
 - settings [214](#)
 - spam [223](#)
 - warning [223](#)

M

- mailing lists [192](#)
- master authentication
 - master password [148](#)
- messages in queue [204](#)
 - queue viewing [205](#)
- Microsoft Entourage [343](#)
 - free/busy [359](#)
 - LDAP [355](#)
 - LDAP settings [357](#)
 - settings [344](#)
- Microsoft Entourage 2004
 - delegating folders [360](#)
 - free/busy [351](#)
 - settings [348](#)
- Microsoft Entourage 2004 sp2
 - free/busy [354](#)
 - settings [352](#)
- Microsoft Entourage X
 - free/busy [347](#)
 - settings [345](#)
- MX Records [121](#)

N

NNTP [13, 51](#)
NT domain [69](#)
 user import [109](#)

O

Open Directory [277](#)

P

PAM [68, 96](#)
performance monitor [228](#)
POP3 [13, 50, 226, 230, 232](#)
port [52](#)
ports [232](#)
product registration [33](#)
 importing license key [38](#)
 licensing policy [41](#)
 registration of the full version [35](#)
 registration of the trial version [34](#)
 registration via web [33](#)
 registration with the administration
 console [33](#)
 subscription [41](#)

R

RAS [72](#)
reindexing mail folders [246](#)
relaying [122](#)
remote POP3 mailboxes [134](#)

S

scheduling [74](#)
 time ranges [15, 75, 86, 87](#)

services [50](#)
skins [82](#)
 cascading stylesheet [82](#)
SMTP [13, 50, 121, 124, 226](#)
spam [155](#)
 Bayesian filter [155](#)
 Caller ID tab [162](#)
 internet spammer databases [159](#)
 SMTP greeting delay [167](#)
 SpamEliminator [155, 327](#)
 SPF [164](#)
SSL [77](#)
SSL certificate [77](#)
store directory [147](#)
system requirements [18](#)

T

technical support [413](#)
 contacts [413](#)

U

update [150](#)
user accounts [91](#)
 quota [101](#)
 templates [113](#)

W

WAPmail [96](#)

X

X-Envelope-To: [143](#)

