Kerio MailServer 6™

Administrator's Guide

Kerio Technologies

Printing Date: February 5, 2008

This guide provides detailed description on *Kerio MailServer*, version *6.5.0*. All additional modifications and updates reserved.

For current versions of the product and related manuals, check `http://www.kerio.com/kmsdwn`.

Information regarding registered trademarks and trademarks are provided in appendix A.

Contents

Chapter 1

Introduction

1.1 Basic features

Kerio MailServer 6.5 is designed as a "secure mail server accessible from anywhere". Here is a brief list of its main functions and features.

SMTP server

A full-featured SMTP server which allows multiple independent local domains, 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 client to download mail from a server and store it on the 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 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

NNTP (Network News Transfer Protocol) is a protocol used to transfer news messages and display public news folders for users. An 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. *Kerio WebMail* is address in a stand-alone document, *Kerio MailServer, User's Guide*.

Personal and Public Contact Lists

In *Kerio MailServer* 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.

Free/Busy server

The *Kerio MailServer's* built-in *Free/Busy* server is a server using HTTP to provide information on busyness and free time of other *Kerio MailServer* users without details of individual events being displayed.

Calendars, tasks and notes

Kerio MailServer includes tools for keeping and administration of private and public folders with calendars, tasks and notes. In the *Kerio WebMail* interface and the *MS Outlook* application with *Kerio Outlook Connector*, calendar, task and note folders can be managed (see chapter 32.2).

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 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 *SpamAssassin* 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 *Spam Eliminator* 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.
Kerio MailServer has a highly configurable mailing list archive feature.

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, tasks and notes) at the server. It is also possible to share and map folders, as well as set up message sorting rules.

Kerio Outlook Connector (Offline Edition)

Kerio Outlook Connector (Offline Edition) 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, tasks and notes) at the server. It is also possible to share and map folders, as well as set up message sorting rules.

Kerio Outlook Connector (Offline Edition) allows offline users to work with their email, calendar and other groupware tools in offline mode.

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.

Support for Windows Calendar

Kerio MailServer provides support for the *Windows Calendar* application. Users can subscribe and publish calendars in *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 allows use of the *Kerio MailServer's Free/Busy* server .

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

Support for groupware features in Apple Mail 10.4

Kerio MailServer supports certain groupware features in *Apple Mail 10.4*.

Support for subscription and publishing of calendars in Apple iCal

Kerio MailServer supports subscription and publishing of iCalendar calendars. This support enables subscription of *Kerio MailServer* calendars to *Apple iCal* as well as publishing of *Apple iCal* calendars in *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.

Kerio Sync Connector for Mac

Kerio Sync Connector for Mac is a special application which enables synchronization of local data between *Kerio MailServer* and the *Apple iCal* or the *Apple Address Book* application.

CalDAV protocol support

Support for the CalDAV protocol enables subscription and viewing of calendars saved *Kerio MailServer* in email or calendar clients supporting CalDAV (e.g. *Apple iCal*). The protocol also supports meeting scheduling (Free/Busy and invitations) and subscription of delegated calendars.

Apple iPhone

Kerio MailServer provides support for *Apple iPhone* devices. This support allows to send and receive email and synchronize calendars and contacts with the desktop mail client.

Kerio MailServer supports running of *Kerio WebMail* on *Apple iPhone* in both the full version and the simplified version designed for PDA and mobile devices.

BlackBerry support

- *Kerio MailServer* supports synchronization of email, calendars, contacts and tasks with *NotifyLink* (for details, see `http://www.notifycorp.com/`).
- *Kerio MailServer* enables wireless access to email by using the *BlackBerry Internet Service*.

Support for ActiveSync

Support for the *ActiveSync* protocol allows to synchronize email, contacts, calendars and tasks between *Kerio MailServer* and mobile devices (PDA, Smartphone). Synchronization can be performed between the server and a mobile device (only if an application is installed on the mobile device that provides synchronization over *ActiveSync*).

The support also applies to synchronization between a desktop application (*MS Outlook*) and mobile devices. The synchronization will be performed between the desktop application and a mobile device.

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*.

Support for RoadSync

Kerio MailServer supports *RoadSync*, an application which allows direct synchronization of email, contacts and calendar in mobile devices via *ActiveSync*. The application and the mobile devices settings are focused at `http://www.dataviz.com/`.

Migration Tools

Kerio MailServer allows simple migration of user accounts from various types of email servers to *Kerio MailServer* (e.g. from *4D* or *MS Exchange Server*). Migration is performed by special utilities available on demand at *Kerio Technologies*.

1.2 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 6.1.

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 7.

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 13 for more details.

5. If necessary, create groups (to create group addresses, for instance; under *Domain Settings/Groups*) and assign users to them. For more information refer to chapter 14.

6. Define aliases for users and user groups if necessary (*Domain Settings/Aliases*). More details can be found in chapter 15.3.

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 8.

8. If the modem is installed on the same computer as *Kerio MailServer*, choose the correct RAS line. Again, see chapter 8 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 9.

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 15.4.

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 15.5 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 17 for more information.

13. If *Kerio MailServer* is running behind a firewall, map appropriate ports. See chapter 26.3 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 16.

15. Set up email backup/archiving of mail folders and configuration files if necessary. See chapter 18.2 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 10.

Chapter 2

Installation

2.1 System requirements

The minimum hardware configuration recommended for *Kerio MailServer* (basic license for 20 users):

- CPU 1 GHz
- 512 MB RAM
- 50 MB free disk space (for the installation)
- 40 GB free disk space for user mailboxes and backups
- 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 20 — 100 active users

- CPU 2 GHz
- 1 GB RAM
- 160 GB free disk space for user mailboxes and backups

For 100 and more active users

- CPU 2.8 GHz Dual Core
- 2 GB RAM
- 200 GB and more free disk space for user mailboxes and backups

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. *Kerio MailServer* is supported on 32-bit operating systems.

2.2 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 disk. Antivirus might damage the disk or the system. To prevent your computer from such failure, configure your antivirus to not scan the folder (or the disk) where *Kerio MailServer* data is kept (refer to chapter 17).

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 6.

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 6 and 26.3 for more detail).

2.3 Firewall configuration

Kerio MailServer is usually installed in a local network behind a firewall. In addition to the mailserver's configuration, it is also necessary to perform corresponding additional settings of the firewall.

If the MailServer is to be accessible from the Internet, certain ports have to be opened (mapped) in the firewall. Each mapped port might introduce security problems. Therefore, map ports only for those services which you want to make available from the Internet.

If server is supposed to deliver email directly by DNS MX records, it is necessary to map port 25 (standard port for SMTP service). This setting is required for cases where an MX record for the particular domain is addressed to the server. Any SMTP server on the Internet can connect to your SMTP server to send email to one of its domains.

Now, it is necessary to map ports that will be used for connections out of the local network. Since the security risk is higher here, it is recommended to map only SSL/TLS-secured services. Settings are shown in table 2.1.

Service (default port)	Outgoing connection	Incoming connection
SMTP (25)	allow	allow
SMTPS (465)	allow	allow
POP3 (110)	allow	deny
POP3S (995)	allow	allow
IMAP (143)	allow	deny
IMAPS (993)	allow	allow
NNTP (119)	allow	deny
NNTPS (563)	allow	allow
LDAP (389)	allow	deny
LDAPS (636)	allow	allow
HTTP (80)	allow	deny
HTTPS (443)	allow	allow

Table 2.1 Services to be allowed on the firewall

2.4 Installation

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

Microsoft Windows

It is recommended to perform the upgrade to *Kerio MailServer 6.5.0* from *Kerio MailServer* 6.3 or 6.4.

Kerio MailServer supports the following versions of *Microsoft Windows* operating systems:

- Windows 2000 (SP4)
- Windows XP (SP2 or SP1)
- Windows 2003 (SP2 or SP1)
- Windows Vista (Business, Enterprise or Ultimate edition)

It is necessary that *Kerio MailServer* is installed under a user with administration rights for the system.

Kerio MailServer is supported on 32-bit operating systems.

Kerio MailServer is installed by using the *Windows Installer*. Once the installation program is launched, a guide will take you through setting the basic server parameters. For details about this wizard, refer to chapter 2.5.

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

`C:\Program Files\Kerio\MailServer`

This setting can be changed during the installation process if necessary (see below).

For better reference when solving any problems, the *Kerio MailServer* installation process is logged in a special file (`C:\WINDOWS\kms_setup.log`).

To install *Kerio MailServer*, follow these instructions:

1. Double-click on the *Kerio MailServer's* installation file run it. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kmsdwn/`.

2. The installer asks user to select the installation language. In the menu, select a language (English, German, Italian, Russian and Czech localizations are available so far) and confirm settings by clicking on *OK*.

3. When the installation process is started, a welcome page is displayed (see figure 2.1). When the welcome page is opened, the installer scans the disk automatically to find out whether there is enough space for the installation on the target drive.

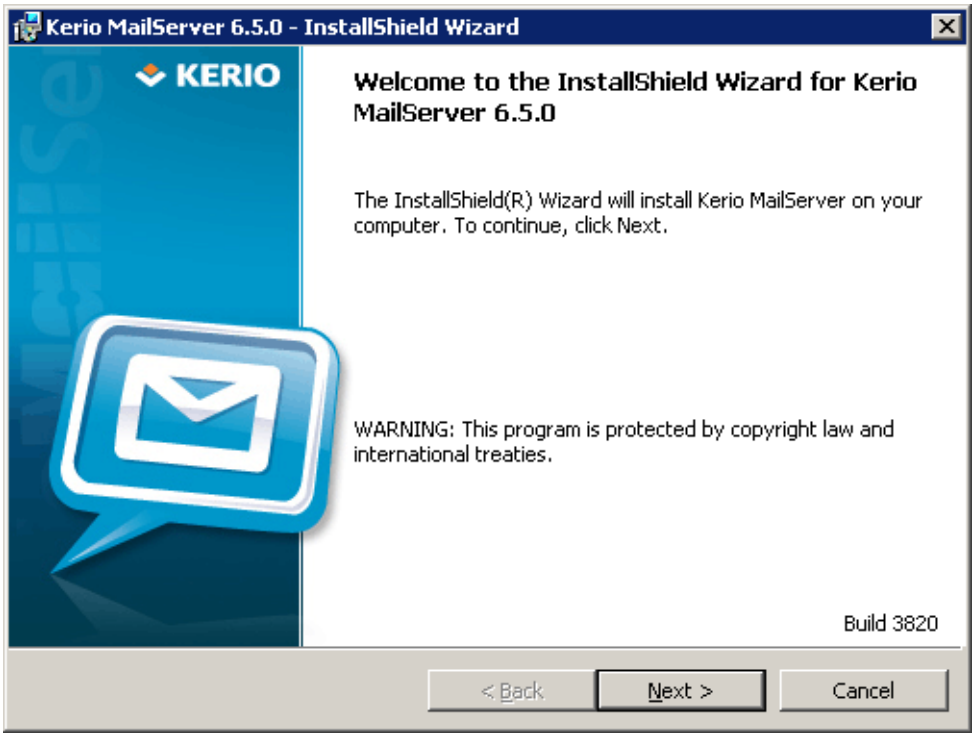

Figure 2.1 Installation wizard's welcome page

To install *Kerio MailServer*, click *Next*.

4. In the following dialog, all important changes and news since the last version of *Kerio MailServer* are listed.

   Read the change log and click on *Next*.

5. In this dialog, license terms for the product are displayed. To continue in the installation process, select the *I accept the terms in the license agreement* option (see figure 2.2).

   Once the terms are accepted, click *Next*.

6. In this dialog, select an installation type (see figure 2.3):

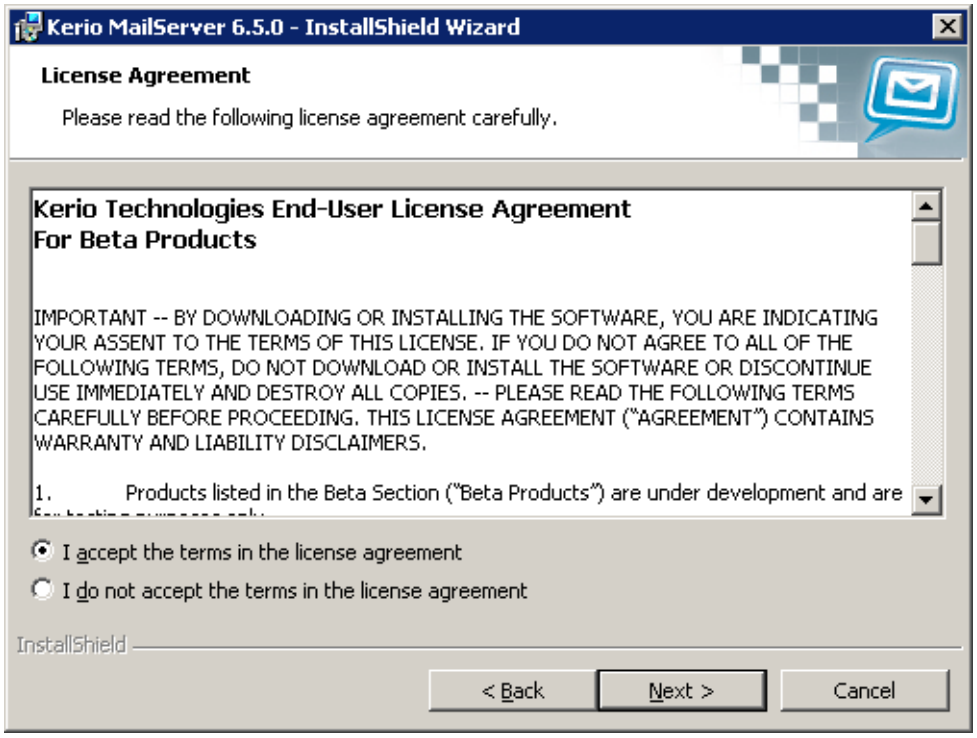

Figure 2.2 Licensing Policy

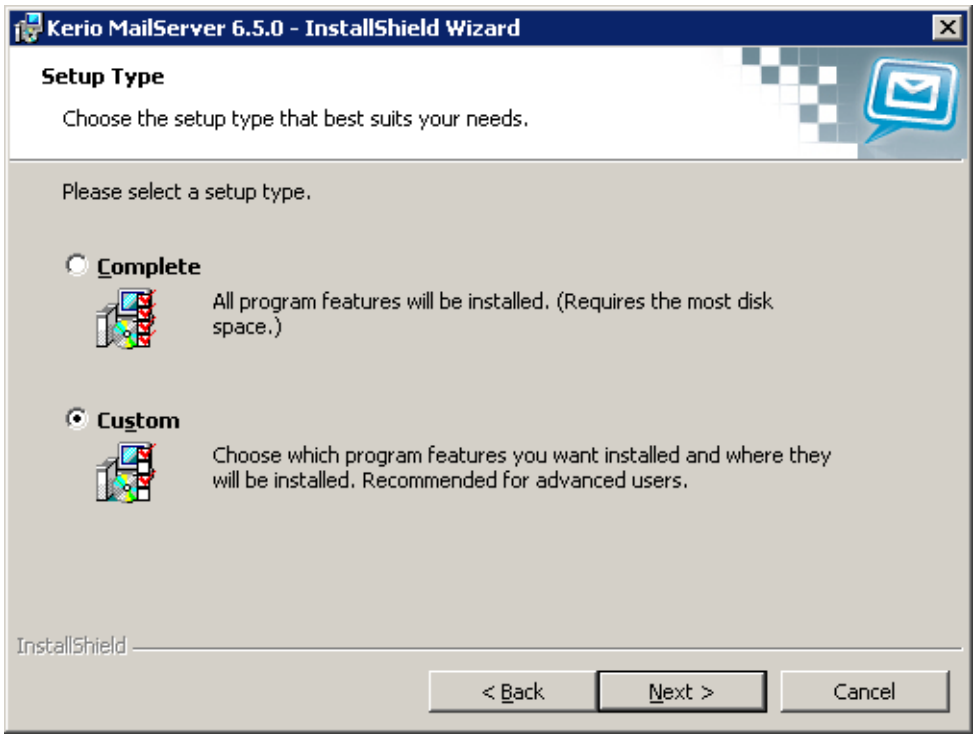

Figure 2.3 Installation type selection

- *Complete* — all parts and modules of *Kerio MailServer* including the product guide in two language versions will be installed.

  This option is recommended especially to users who are installing *Kerio MailServer* for the first time.

- *Custom* — selection of *Kerio MailServer* components which will be installed as well as of a language of the *Kerio MailServer's* help.

7. In this dialog, select a directory where *Kerio MailServer* will be installed. As shown at figure 2.4, by default, the mailserver is installed in

   `C:\Program Files\Kerio\`

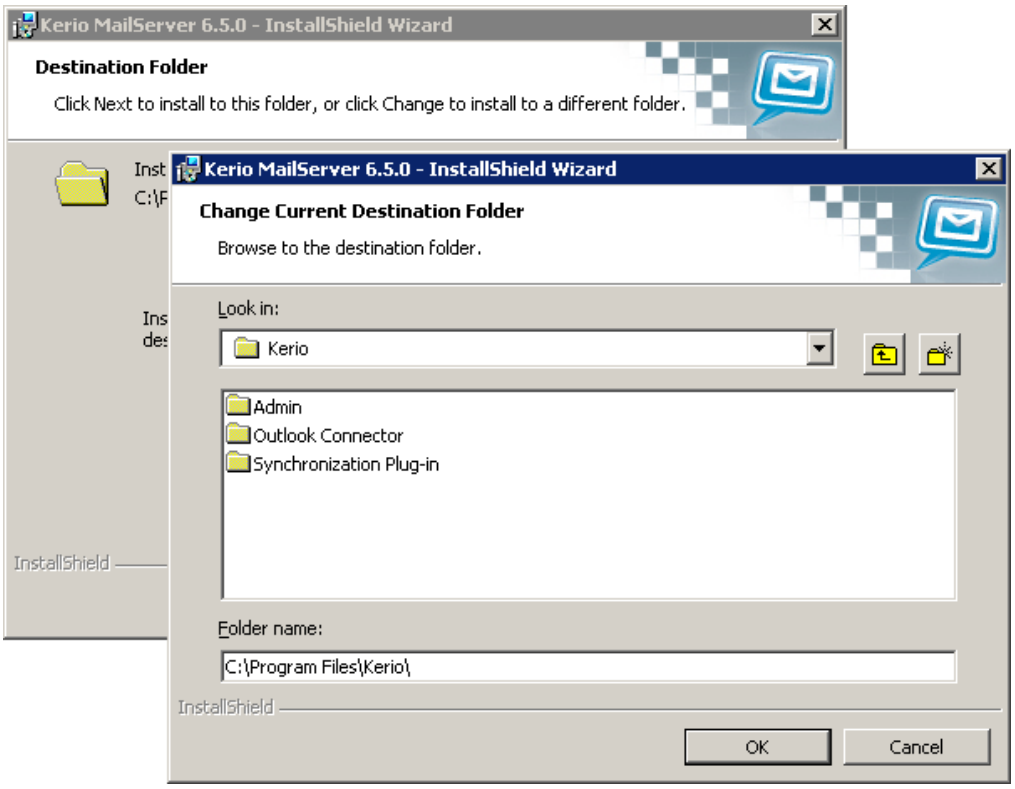

Figure 2.4 Kerio MailServer installation path selection

   Select a folder where the program will be installed and click on *Next*.

8. The following dialog is opened only if the *Custom* installation was selected. If you selected the *Complete* option, skip reading this section.

   In the *Custom* installation, it is possible to choose which *Kerio MailServer* components will be installed. This installation type is usually helpful if you need to spare your disk space by leaving for example the help file out of the installation or if you

need to install only the *Kerio Administration Console* on a host from which you will perform remote administration.

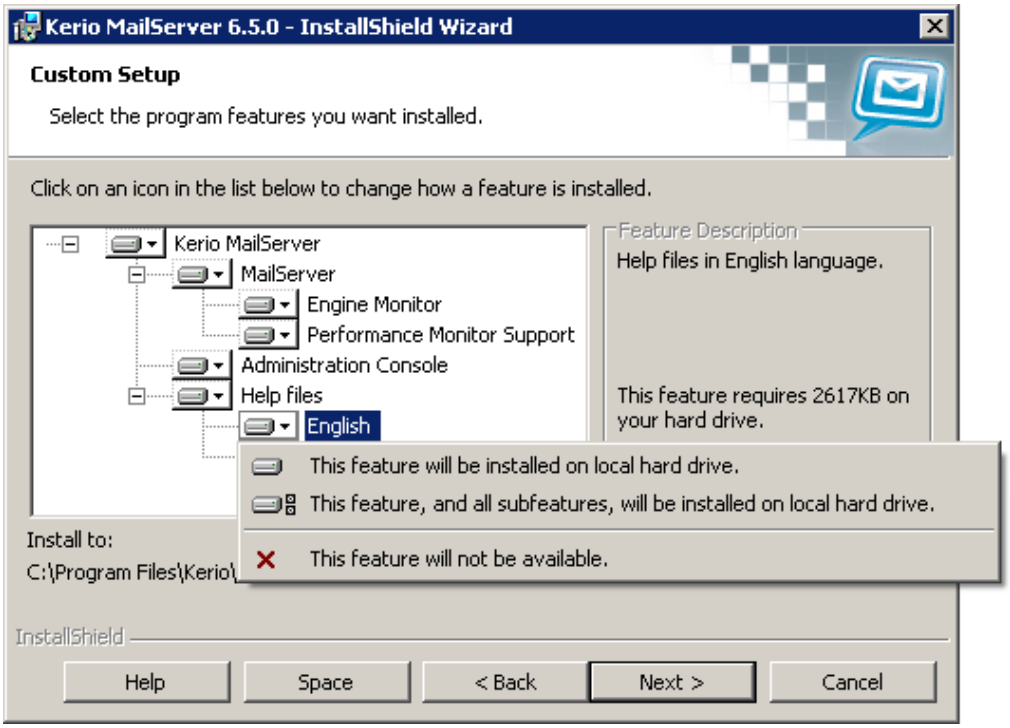

Figure 2.5 Custom installation

Components to be installed:

- *MailServer* — the executive core of the program (the *Kerio MailServer Engine*) which provides all services and functions. It runs as a background application (as a service on Windows 2000, Windows XP or Windows Vista, or as a daemon on Unix-based systems).

  Along with the *Kerio MailServer Engine*, it is recommended to install the following components:

  - *Engine Monitor* — to get more information about this component, see chapter 4.1.
  - *Performance Monitor Support* — to get more information about this component, see chapter 22.9.

- *Administration Console* — the *Kerio MailServer's* administration interface. It can be also installed separately and used for remote administration (more information in chapter 5).

- *Help files* — 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.

9. In the next dialog, automatic startup of *Kerio MailServer* upon completion of the installation can be enabled (the *Start the MailServer Engine service after the installation finishes* option).

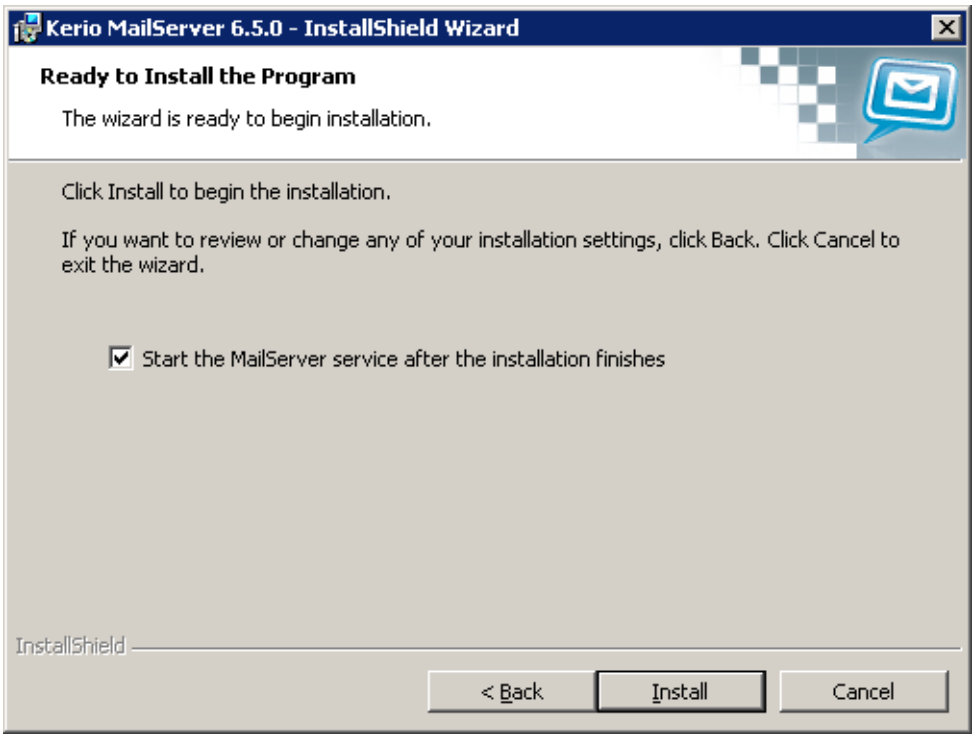

Figure 2.6 Confirmation of the installation startup

Click on *Install*. After this step, the installation continues (i.e. files are copied to a hard drive and all necessary system settings are performed).

10. Status of the installation process is showed during the installation. Please be patient, the installation may take several minutes.

    Once the installation is completed, click *Next*. At this moment, the wizard is started where basic server parameters can be set (see section 2.5). Be really attentive while setting these parameters.

11. Once the settings in the configuration wizard are done, the final dialog of the installation wizard is opened. Click on *Finish* to complete the installation (see figure 2.7).

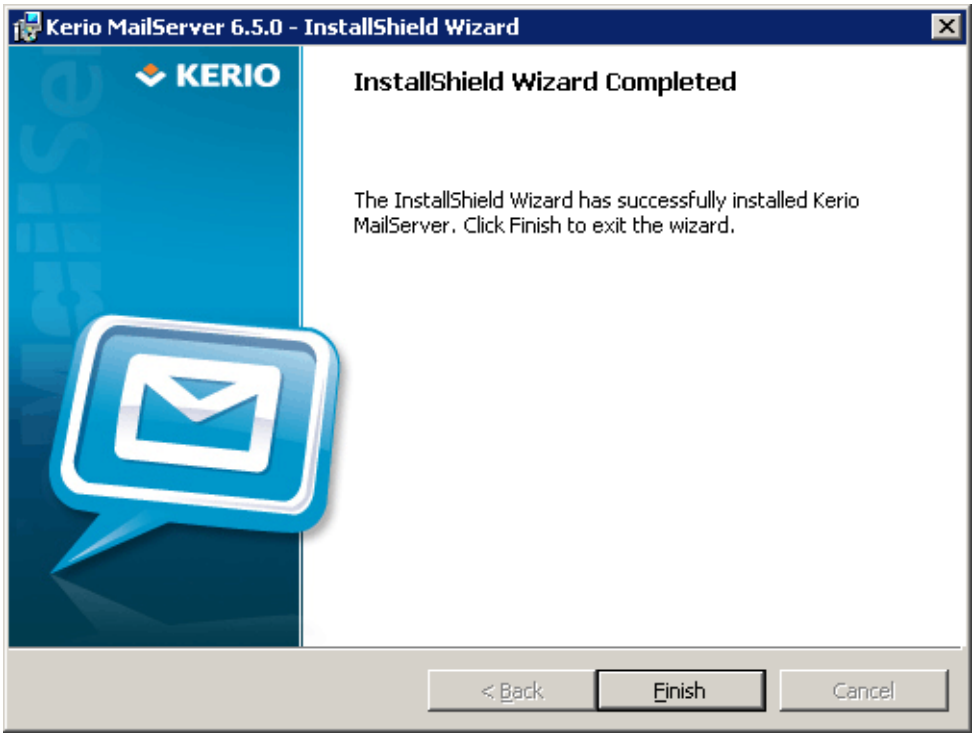

Figure 2.7 Installation on Windows: Final dialog of the wizard

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 (see figure 2.8).

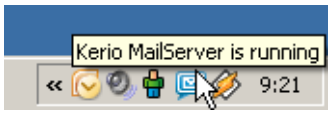

Figure 2.8 Kerio MailServer Monitor on Windows

Protection of the installed product

In order to ensure the maximum security 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 the first startup after each upgrade or installation: 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* disks.

Linux

Kerio MailServer supports the following distributions of the Linux operating system:

- *Red Hat 9.0*
- *Red Hat Enterprise Linux 3 / 4 / 5*
- *Fedora Core 4 / 5 / 6 / 7 / 8* (on 32-bit systems)

  Requires: libstdc++.so.5 (compat-libstdc++-33 RPM package)

  Fedora Core 5 requires: compat-gcc-32-3.2.3-56.fc5 and compat-libstdc++-33-3.2.3-56.fc5.
- *SuSE Linux* 10.0, 10.1, 10.2 and 10.3 (32-bit)

  Requires: libstdc++.so.5 (compat-libstdc++-33 RPM package)

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

Note: For installations, *Kerio MailServer* uses the RPM application. All parameters for RPM are supported by *Kerio MailServer*.

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_file_name>
```

Example:

```
# rpm -i kerio-kms-6.5.0-1070.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

/etc/init.d/keriomailserver restart
```

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

Administration

To run *Kerio Administration Console*, use the `kerioadmin` command in the `/usr/bin` directory (the path is set by default). The *X Window System* graphical interface is required.

Mac OS X

Since version 6.2, *Kerio MailServer* supports Mac OS X systems on both PowerPC and Intel processors. The *Kerio MailServer's* installation package is a universal binary file which can be run on both platforms.

The product supports the following systems:

- Mac OS X 10.3.9 Panther on G4 or G5, 512 MB RAM, Mac Intel Solo or Duo, 512 MB RAM
- Mac OS X 10.4 Tiger on G4 or G5, 512 MB RAM; Mac Intel Solo or Duo, 512 MB RAM
- Mac OS X 10.5 Leopard on G4 or G5, 512 MB RAM; Mac Intel Solo or Duo, 512 MB RAM

Recommended: G5, 1GB RAM Mac Intel Solo or Duo, 1GB RAM

`kerio-kms-6.5.0-1069.mac.dmg`

1. Double-click on the package icon to open the `kerio-kms-6.5.0-1069.mac.dmg` installation package.

2. This opens the *Finder* where the installation package is opened as a disk and where the *Kerio MailServer Installer* executable is available. Click on it to run the installer (see figure 2.9).

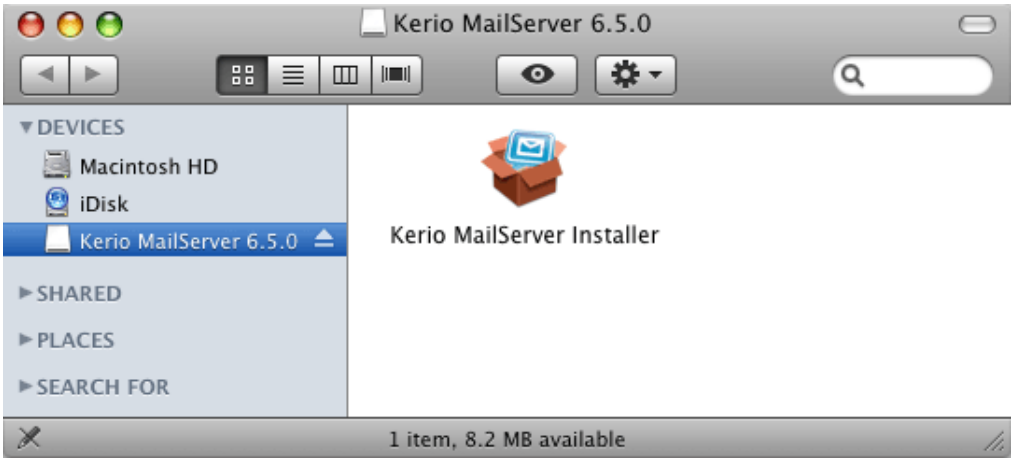

Figure 2.9 Kerio MailServer Installer

3. *Kerio MailServer* can be installed only by a user with administration rights for the system. To start the installation, username and password is required in a special dialog (see figure 2.10). Enter the username and password for a user who has administration rights for the system. Only users with appropriate rights (members of the *Admins* group) are allowed to install applications in the system.

   Administrators can allocate any users with these rights under *System Preferences* → *Accounts*.

4. The installation wizard is opened upon a successful authentication.

5. At the start, license terms are displayed. Click on *Continue* and confirm the terms by the *Agree* button.

Figure 2.10 User authentication

Figure 2.11 License terms

6. Once license terms are accepted, a dialog is opened where an installation type can be selected:

   - *Easy Install* — preset installation, all components will be installed automatically by the installer.

- *Custom Install* — you can select individual components that you would like to install (*Kerio Administration Console*, *Kerio MailServer Engine* and *Administrator's Guide* are available).
- *Uninstall* — this options uninstalls *Kerio MailServer*.

Select an installation type (the *Easy Install* option will install all available components) and click on *Install*.

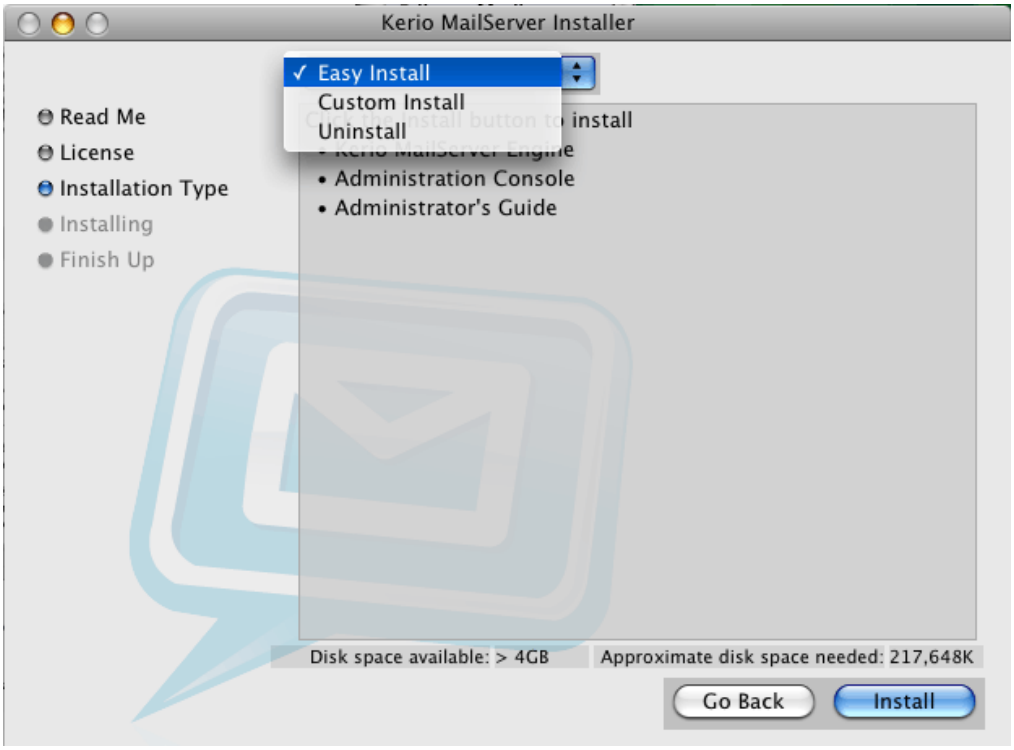

Figure 2.12 Installation — custom install

7. Now, the wizard runs the installation.

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

   The complete version of *Kerio MailServer* will be installed (*Kerio Administration Console*, *Kerio MailServer Engine* and *Administrator's Guide*).

8. Once the installation is completed, the configuration wizard is opened automatically. Set the primary domain name and the admin password which will be used for login to the *Kerio MailServer's* administration console (see chapter 2.5).

9. When the configuration wizard is finished, the final dialog of the installer is displayed. Finish the installation by the *Quit* button.

Click *OK* to open the *Kerio MailServer* folder which includes the `Administration Console` executable file, the administrator's guide (`Administrator's Guide`) in *PDF* and *Configuration Wizard* (refer to chapter 2.5).

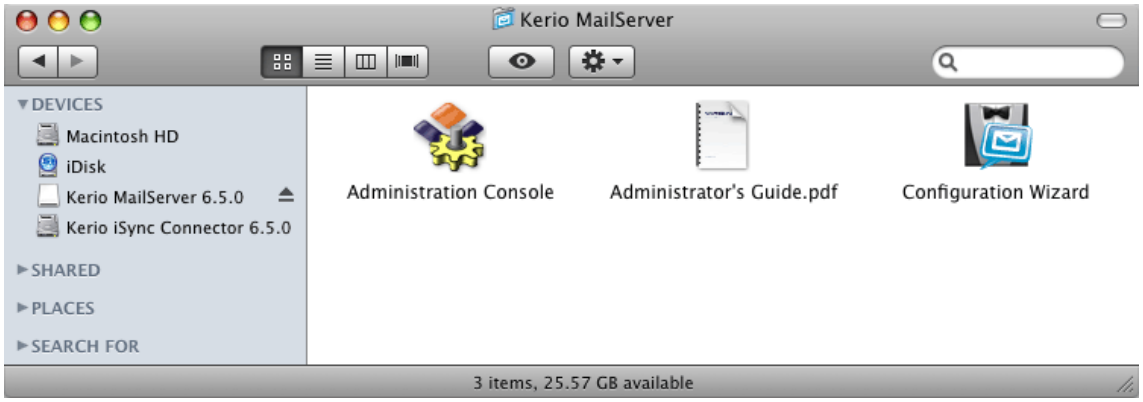

Figure 2.13 Kerio MailServer folder

Kerio MailServer will be run automatically after the operating system is booted. However, users must run *Kerio MailServer Monitor* (*System Preferences* → *Other* → *KMS Monitor*). Username which must belong to the `Admins` group and password is required for stopping or running of the service. Once authenticated, clicking *Stop Kerio MailServer* or *Start Kerio MailServer* 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
```

2.5 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 and internet name of the server

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 7).

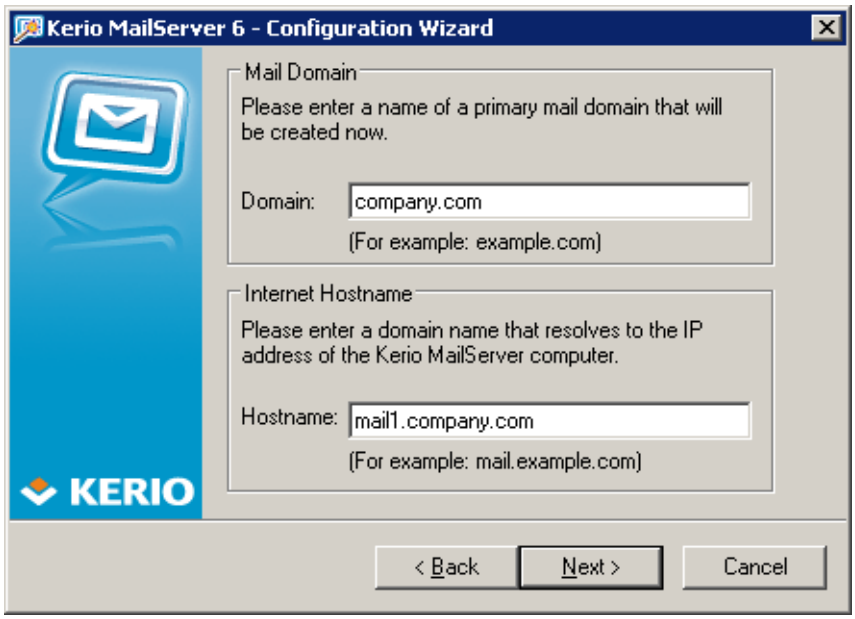

Figure 2.14 Configuration Wizard — creation of the primary domain

It is also necessary to insert the name of the server where *Kerio MailServer* is installed. In the *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 suggested by the configuration wizard). Server names are used for server identification while establishing SMTP traffic.

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.

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.

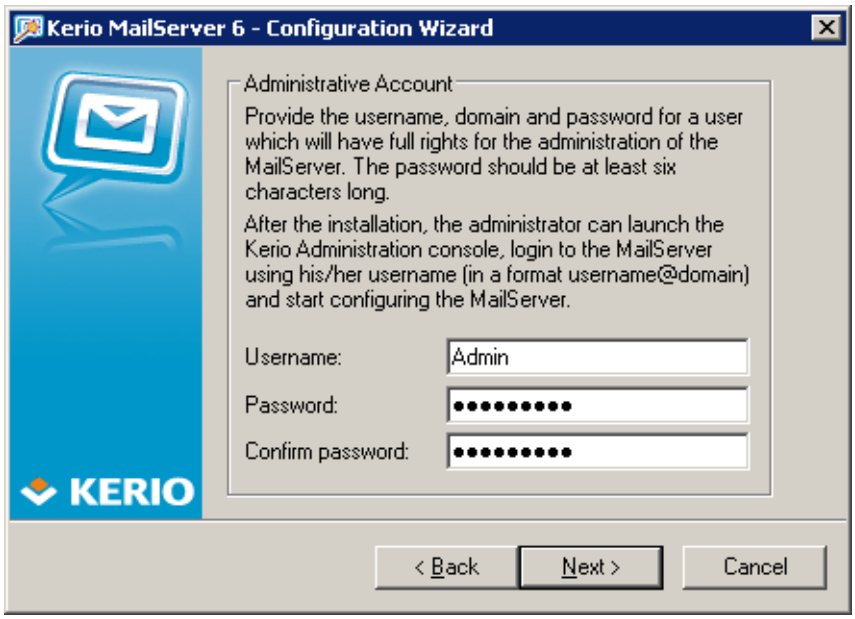

Figure 2.15 Configuration Wizard — user account creation

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 select a different location to store data (e.g. another disk partition, RAID etc.). The store directory can be changed anytime later through the *Kerio Administration Console* (see chapter 15.6). If the location is changed then it is necessary to move the files located in this directory to the new location. Prior to this potentially very time-consuming operation, the *Kerio MailServer Engine* must be stopped. Therefore it is recommended that you select a location with sufficient space for growth during the installation — using the configuration wizard.

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

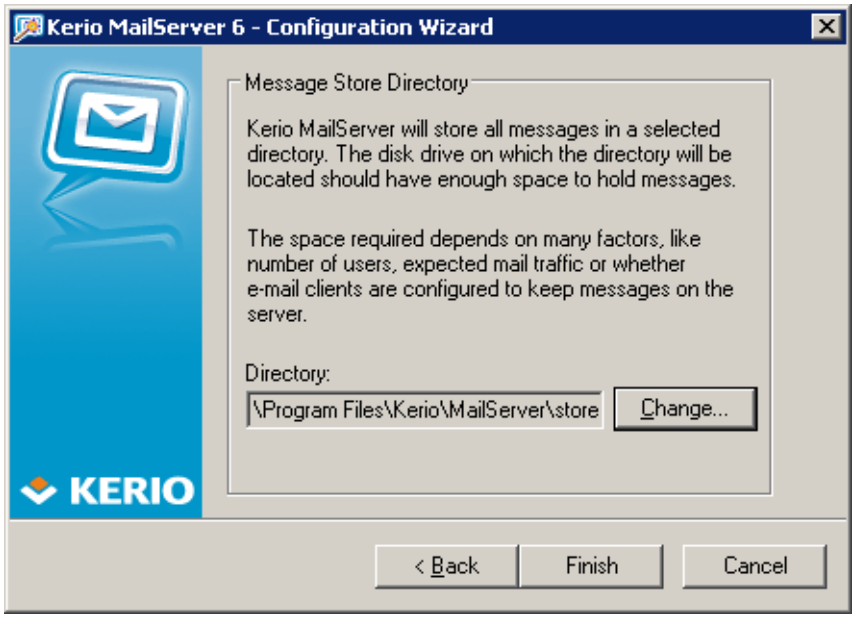

Figure 2.16 Configuration Wizard — folder selection

The last step of the initial configuration

The last dialog provides information about writing of the settings in the configuration files (on Windows only):

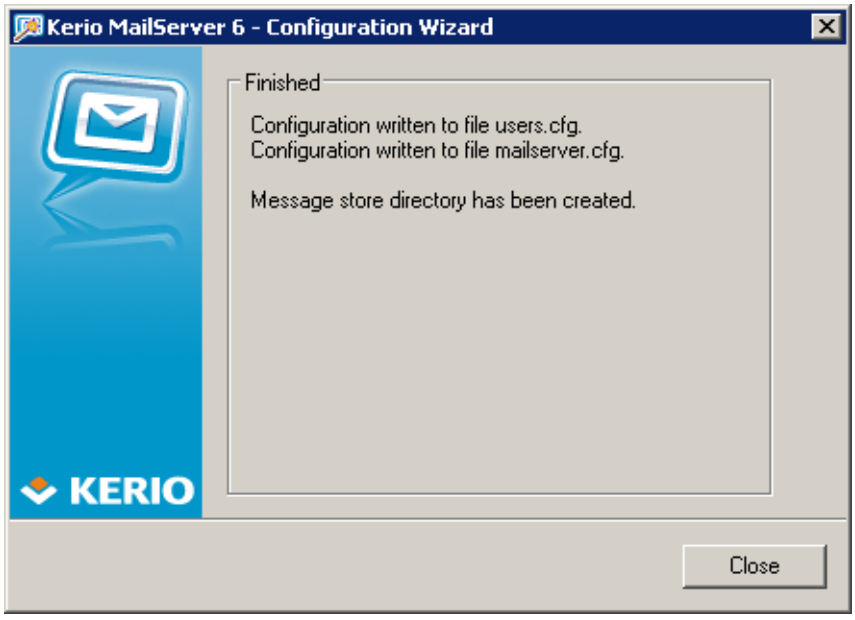

Figure 2.17 Information about successful completion of the primary domain configuration

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, Internet name of the server as well as the location of the message store was written.

2.6 Upgrade and Uninstallation

Windows Operating Systems

To upgrade this product (i.e. to install a newer version of the 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!

When upgrading *Kerio MailServer*, follow the same scheme as for the first installation of *Kerio MailServer* (see chapter 2.4).

Once the product is upgraded successfully, a backup of the configuration files of the previous *Kerio MailServer* version is saved in the directory where *Kerio MailServer* is installed (`C:\Program Files\Kerio` by default), under the `UpgradeBackups` directory.

Kerio MailServer can be uninstalled by using Uninstall from the Start menu using the *Add/Remove Programs* in the *Control Panels*:

1. Under *Add or remove programs*, select *Kerio MailServer* and click on *Remove*.
2. This runs the *Microsoft Installer* installation wizard.
3. In the first dialog, it is possible to choose whether *Kerio MailServer* will be removed completely, including the data store and configuration files (see figure 2.18):

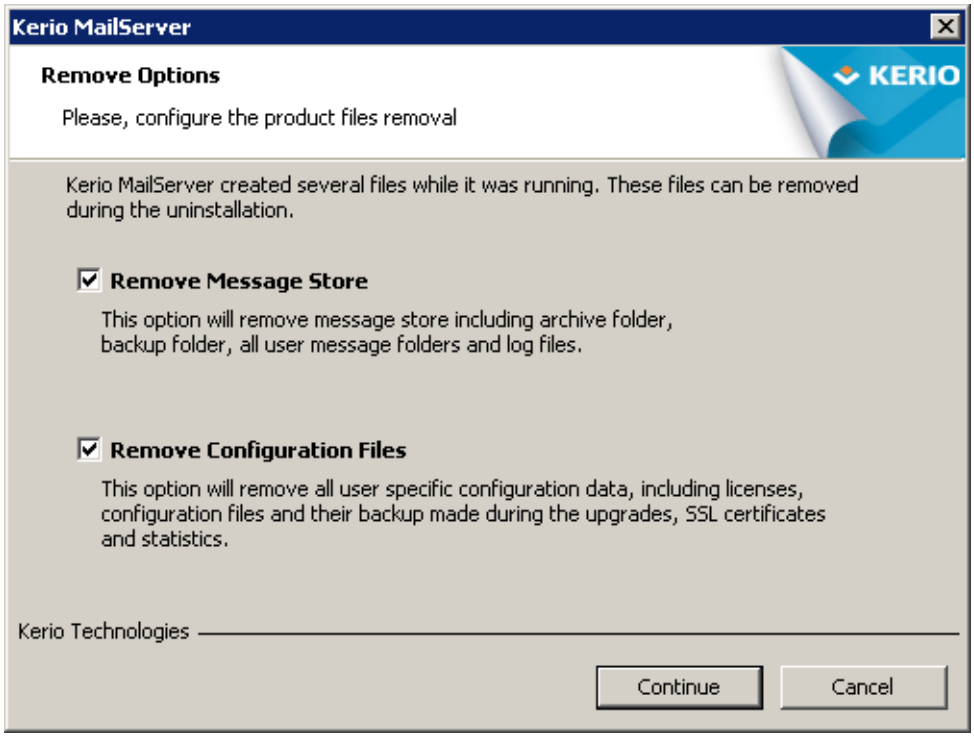

Figure 2.18 Removal of the data store and configuration files

- *Remove message store* — check this option to remove *Kerio MailServer's* data store including the archiving and the backup store.
- *Remove configuration files* — if this option is enabled, configuration files (`mailserver.cfg` and `users.cfg`) as well as the license file, SSL certificates, statistics and logs will be removed.

When sure that the settings are finished, continue by clicking on the *Next* button.

4. Progress of the uninstallation process is showed on the status bar. Please be patient, the process may take several minutes.

Linux Operating System

Upgrade

To upgrade, use the following command:

```
# rpm -U <installation_file_name>
```

Example:

```
# rpm -U kerio-kms-6.5.0-1070.linux.i386.rpm
```

Fix installation of the current version

To fix the current installation, use the following command:

```
# rpm -U --force <installation_file_name>
```

Example:

```
# rpm -U --force kerio-kms-6.5.0-1070.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.

Note: RPM allows using additional, advanced parameters. For description of these parameters, see the RPM guidance page. To open this page, use the following command:

```
man rpm
```

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 *Kerio MailServer's* installation program to uninstall this product. Simply click on the icon of the currently installed *Kerio MailServer's* installation package to run the installation and select *Uninstall* as the installation type.

Chapter 3

Product Registration and Licensing

Once purchased, *Kerio MailServer* must be registered. Registration may be performed in the *Kerio MailServer's* administration console (see chapter 3.2) or at *Kerio Technologies* website (refer to chapter 3.1).

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. This should be sufficient time (30 days) to test the product in the regular environment. It is not necessary to reinstall or reconfigure *Kerio MailServer* after registration.

3.1 Product registration at the website

Web registration can be performed at the *Kerio Technologies* website (`https://secure.kerio.com/reg`), 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 3.3.

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

3.2 Registration with the administration console

In *Kerio Administration Console*, the product can be registered at the main page of *Kerio MailServer* (see figure 3.7). The *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 5.2).

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 allow the customer to become familiar with the 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 3.1). The trial version can be registered at the product's main page (see figure 3.7). Just click the *Trial* link at the page to register the product using a registration wizard.

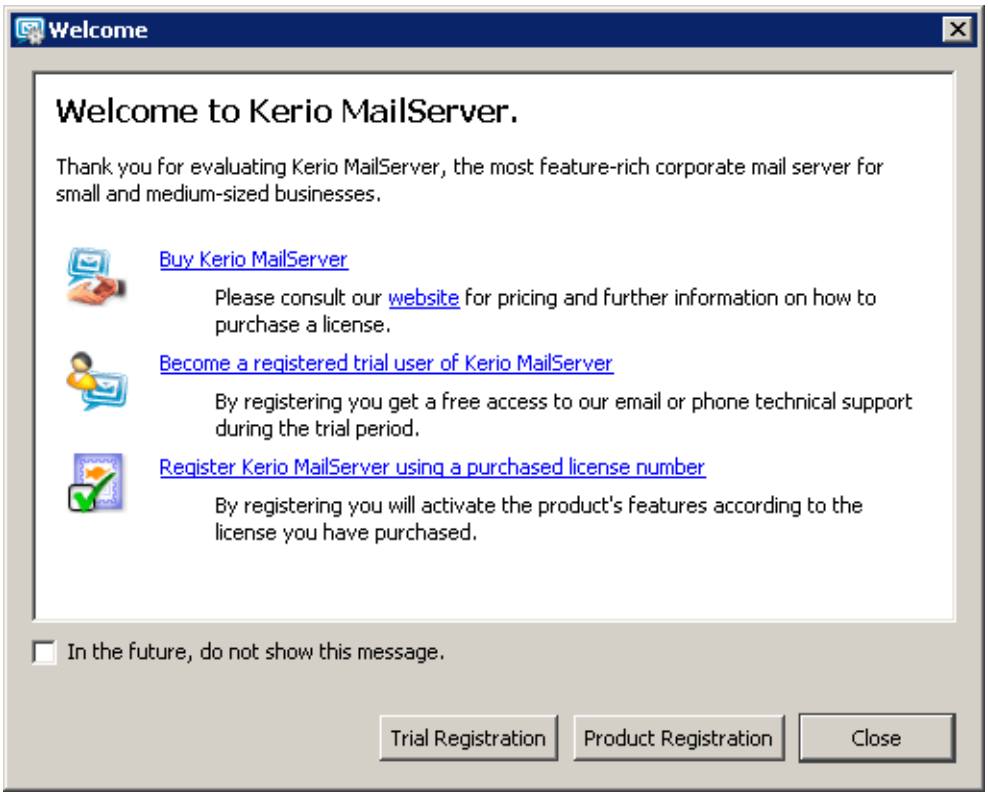

Figure 3.1 Product registration

You should pay careful attention during step five where a special identification code called *Trial ID* is generated. This ID is later required when contacting the technical support. After a successful registration, Trial ID can be found in the license information of the *Kerio Administration Console*.

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).

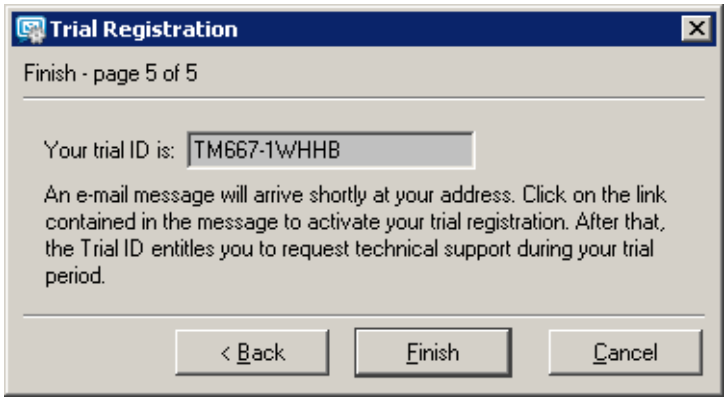

Figure 3.2 Trial ID

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 3.7):

- *Base product* — in step one, enter the license number you acquired upon purchasing the product (*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 a connection to the registration server and check validity of the number entered. If the number is invalid, the registration cannot be completed.

- *Subscription* — In this dialog you can specify add-ons and/or subscriptions numbers. If you have purchased only the base license so far (usually when registrating 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/subscr/`.

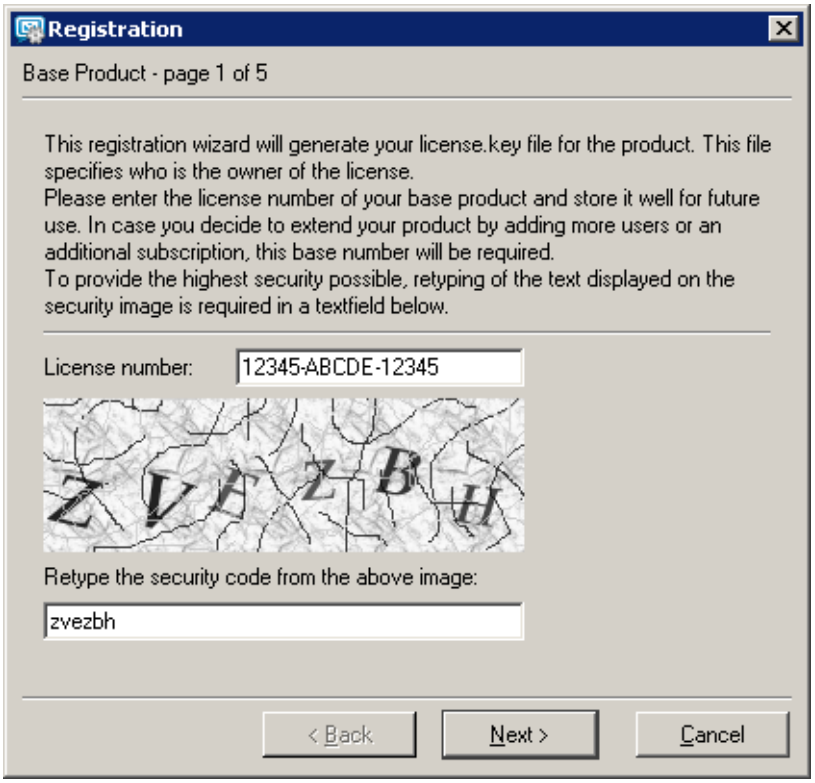

Figure 3.3 License number

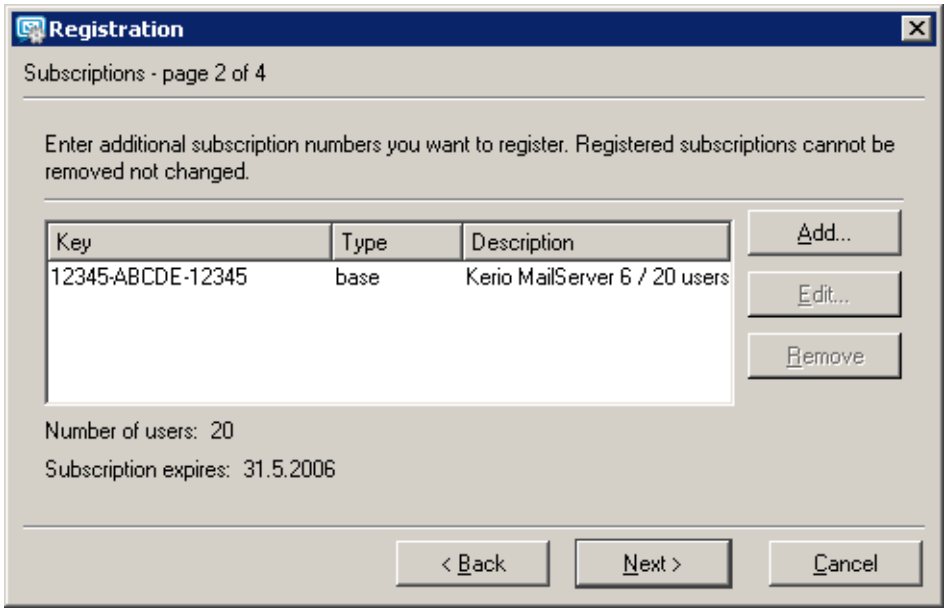

Figure 3.4 Subscriptions and add-ons numbers

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*.

- *Details* — at this page, registration information identifying the company (organization) to which the product is registered is required.

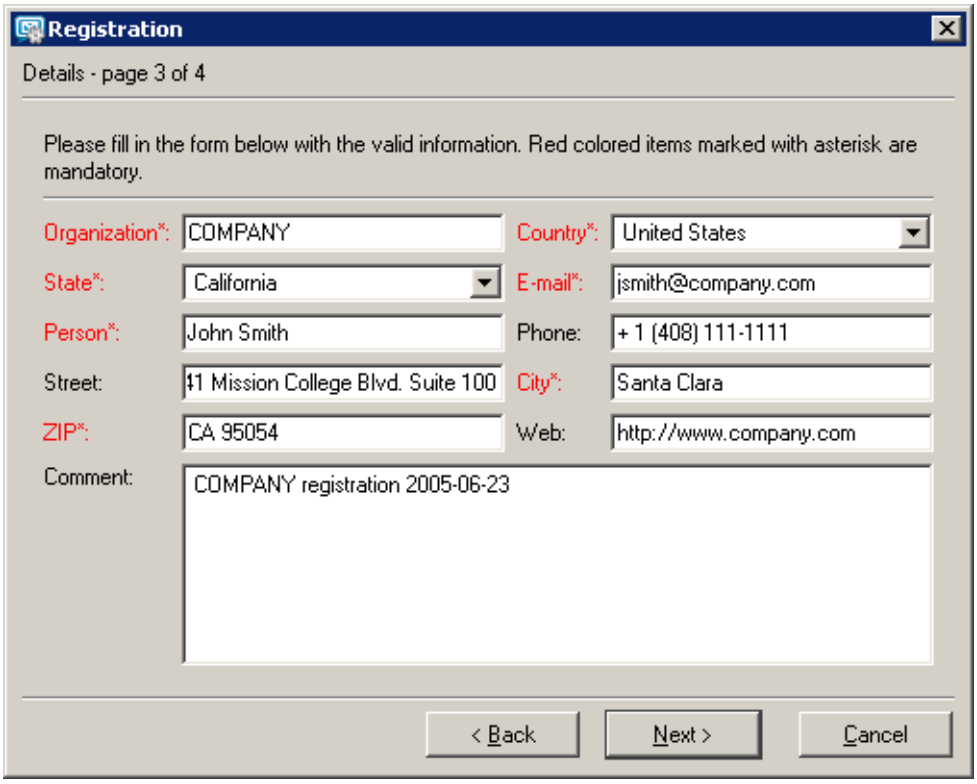

Figure 3.5 Registration form

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

- *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).

  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.

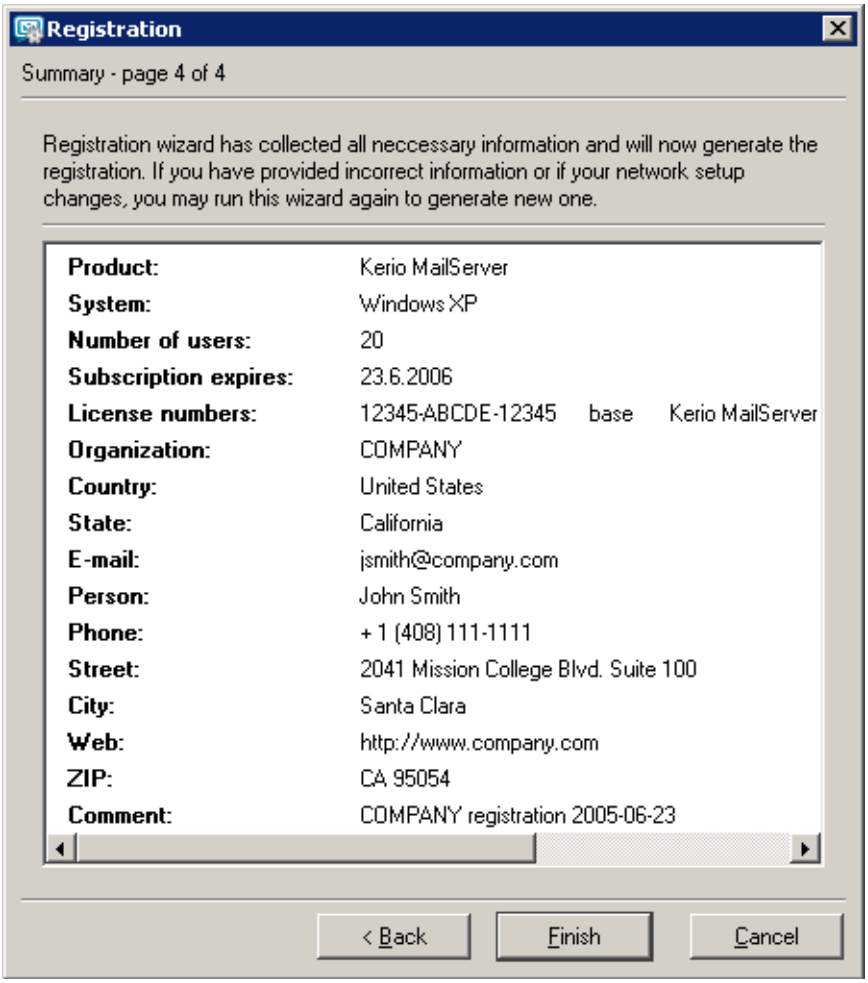

Figure 3.6 Registration data summary

3.3 License information and import of the license key

License information is provided at the main page of *Kerio MailServer*. The *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 5.2).

To run a full version of *Kerio MailServer*, a 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 3.2).

Figure 3.7 Viewing license information

- *Import via the context menu* — click the right mouse button at the main page (see figure 3.7) to open the context menu and select the *Install license* option (see figure 3.8). 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.

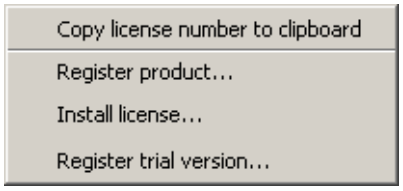

Figure 3.8 The main page's context menu

  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 licensed users
Number of licensed users. Number in parenthesis refers to total number of email accounts used in the *Kerio MailServer*. The number includes both mailboxes created locally as well as accounts mapped from a directory service.
If number of active mailboxes exceeds number of licensed users, the *Number of active mailboxes* line is coloured by red to alert user.

Number of active mailboxes
Number of users connected since the last restart of *Kerio MailServer*. This number includes all local users, all mailing lists (each mailing list stands for 1 licence) as well as all users mapped from the directory service.
Once number of licensed users is exceeded no other users will be allowed to connect to their 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`

3.4 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.

In case of users mapped from the LDAP database of the directory service, all users created in this database are counted as individual licences (all active users).

Once number of licensed users is exceeded no other users will be allowed to connect to their accounts.

Subscription

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

Chapter 4

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, or as a daemon on UNIX-like systems).
The *Kerio MailServer Engine* also includes the `avserver` and `spamserver` processes which run separately that maintain the antivirus plug-in and the*SpamAssassin* anti-spam module (details in section 4.2).

Kerio MailServer Monitor
: With this application you can monitor the *Engine* and *Monitor* applications, you can switch the engine's on/off status, edit startup preferences or launch the administration console. Details can be found in chapter 4.1.
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 5.

Performance Monitor
: This component allows for real time system performance monitoring of KMS components. For more details, see chapter 22.9. This module is available under *MS Windows* operating systems only.

4.1 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.

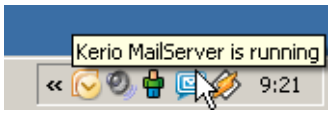

Figure 4.1 Kerio MailServer Monitor

If the mailserver 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.

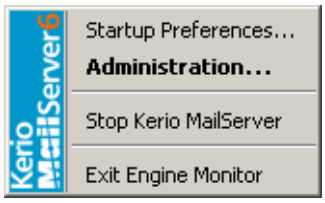

Figure 4.2 Kerio MailServer Monitor — menu

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

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 Engine Monitor
— 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

On *Mac OS X*, the *Kerio MailServer Monitor* is displayed in a new window (see figure 4.3) which can be opened from the *Other* section of *System Preferences*. The window includes the following options:

Figure 4.3 Kerio MailServer Monitor — Kerio MailServer Status

- *About Kerio MailServer* — the button opens the *About* window providing basic information on the product and its version number.
- *Stop/Start Server* — the button starts/stops the *Kerio MailServer Engine*.

  Username which must belong to the `Admins` group and password is required for stopping or running of the service.
- *Configure Server* — the button runs the *Kerio Administration Console*.

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]
```

4.2 Standalone processes of the server

`avserver` and `spamserver` are special processes used to maintain applications developed outside *Kerio Technologies*. These applications include any antivirus plugins (external and/or the built-in McAfee antivirus) and the *SpamAssassin* antispam filter. As hinted by their names, `avserver` maintains antivirus plugins, while `spamserver` maintains the *SpamAssassin*.

Both processes are represented by executables located in the directory where *Kerio MailServer* is installed (`\Kerio\MailServer\plugins` on Windows, `/Kerio/mailserver/plugins` on Unix-based systems).

The processes were introduced in *Kerio MailServer's* 6.2 version and they help balance inconsistencies that occurred in connection with the plugins.

Whenever a problem occurs regarding any of the plug-ins (e.g. when connection is closed improperly or if connection "freezes"), automatic restart is initiated by the corresponding process. This implies any error that occurs does not cause failure of the entire mailserver and communication with the corresponding plug-in is even not interrupted for a long time. Initiation of the application's restart also generates and saves a crashdump log that might help discover the problem's cause. Then, when an administrator connects to *Kerio MailServer*, a *Kerio Assist* dialog asks them to decide whether the crashdump log would be sent to *Kerio Technologies* for analysis.

Warning: Any information recorded in the log are used only to solve problems associated with usage of *Kerio Technologies* products. No information including the sender's email address will be misused in any way.

Chapter 5

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.

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.

Note: If *Kerio Administration Console* freezes or fails, a special application called *Kerio Assist* is started which, upon confirmation by the server's administrator, send a special `mailadmin.dmp` file for analysis in *Kerio Technologies*. The file includes only data regarding *Kerio Administration Console* and it cannot be misused.

5.1 Localizations of the Kerio Administration Console

The *Kerio Administration Console* is available in several language versions. Currently, the *Kerio Administration Console* is available in:

- English
- Czech
- Chinese
- Italian
- Japanese
- German
- Portuguese
- Russian
- Slovak
- Spanish
- Dutch
- French

The default version can be set as follows:

1. Run the *Kerio Administration Console*.

2. In the *Tools* → *Options* menu on the *Kerio Administration Console* toolbar, open the *Options* dialog (see figure 5.1).

   The same dialog for Mac OS X operating systems can be found under *Administration for Kerio MailServer* → *Preferences*.

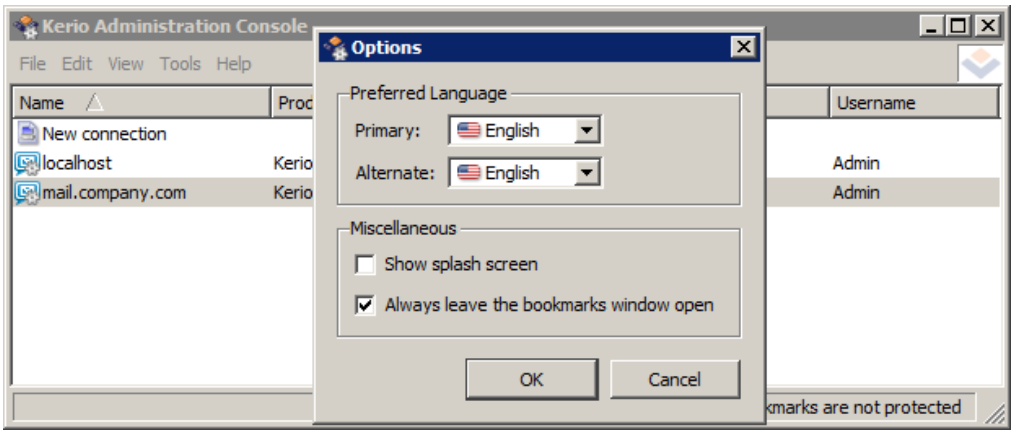

Figure 5.1 Kerio Administration Console — Options

3. In the *Primary* menu, set a language you prefer.

4. Click *OK*. to confirm changes.

5.2 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).

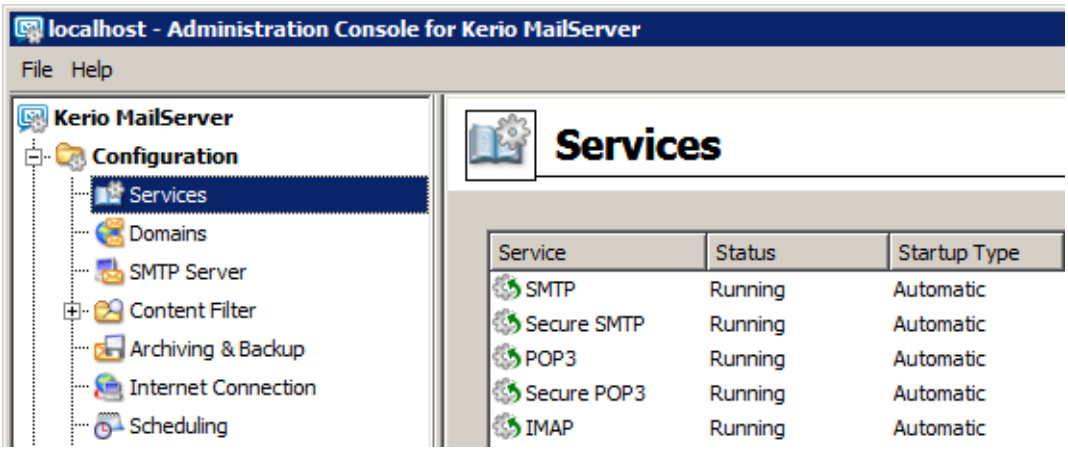

Figure 5.2 Kerio Administration Console

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.

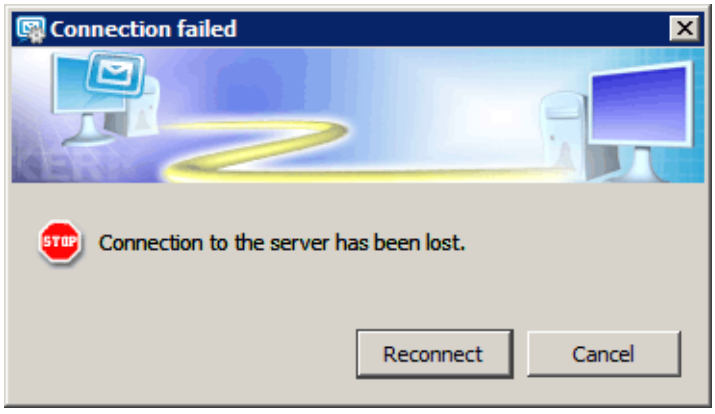

Figure 5.3 Reconnecting

- *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):

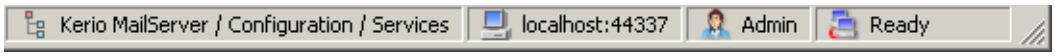

Figure 5.4 Status bar

- 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.

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.

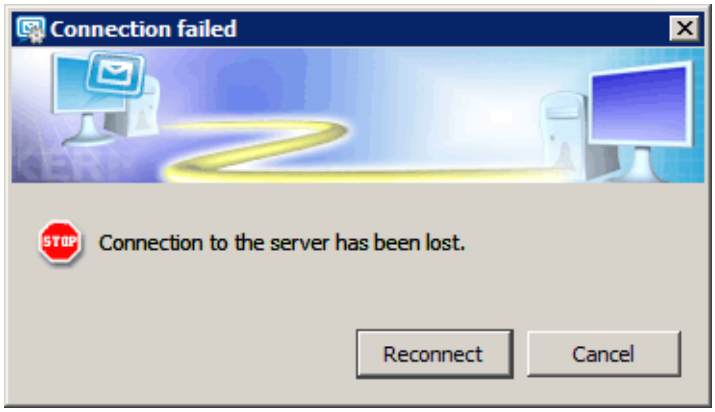

Figure 5.5 Detection of the Kerio MailServer Engine connection failure

5.3 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 pop-up 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.

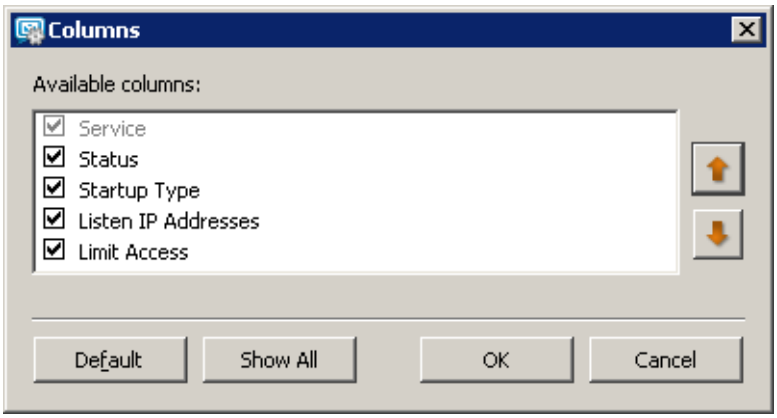

Figure 5.6 Selection of columns

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 also be adjusted in the window view. Left-click on the column name, hold down the mouse button and move the column to the desired location.

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

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*.

Chapter 6

Services

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

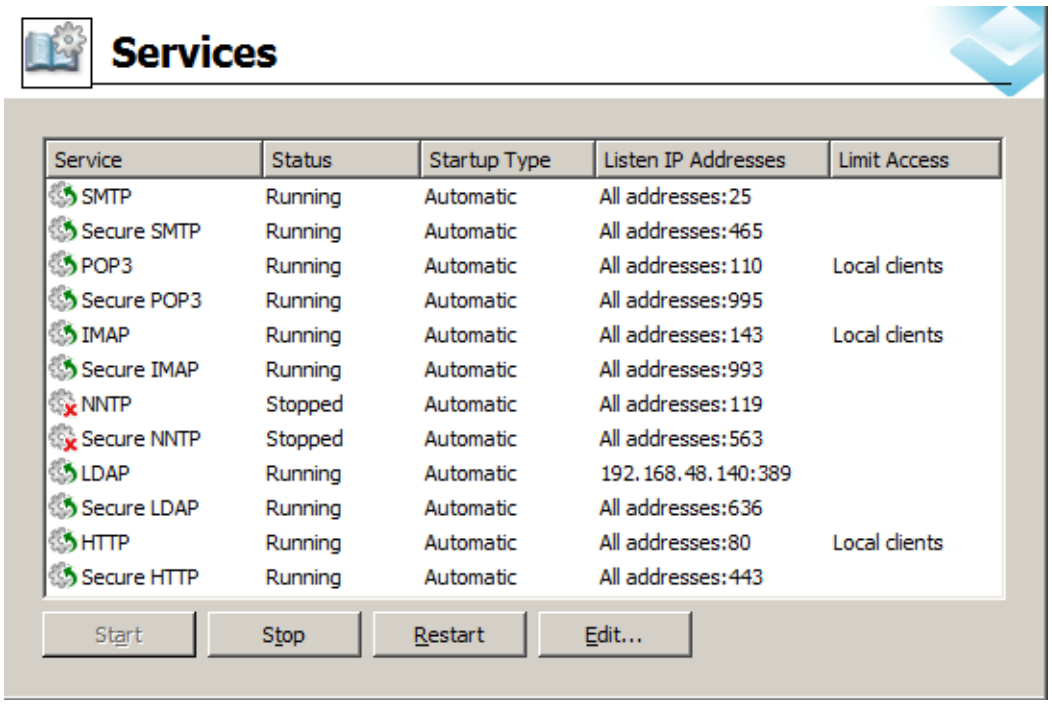

Figure 6.1 Services

SMTP

SMTP protocol server (Simple Mail Transfer Protocol), handling open (non-encrypted) or SSL secured connections. The 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. Port 465 is used as default for the traffic.

Two methods can be used for encryption of SMTP traffic. The traffic can be encrypted either via SMTPS on port 465 or via SMTP on port 25 (STARTTLS, if TLS encryption[1] is supported). The differences between the two methods are as follows:

- SMTP on port 25 with STARTTLS — traffic on port 25 is started as unencrypted. If both sides support TLS, TLS is started via STARTTLS. Otherwise, the traffic is held unencrypted.
- SMTP with SSL/TLS on port 465 — the traffic is encrypted right from the start.

Warning: If traffic between *Kerio MailServer* and mail client is running on port 25, a problem might occur with email sending. Since public WiFi networks often do not support traffic on unencrypted protocols, SMTP on port 25 can be blocked. In such case users cannot send email out of the network. However, SMTPS on port 465 is usually allowed. Therefore, it is recommended to keep SMTPS connection enabled so that notebook and *Apple iPhone* users can use this port to connect to the server. It is also necessary that users' email clients (SMTPS encryption and traffic port) are set correctly.

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. With this protocol, messages 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 newsgroups over the Internet. The service allows users use messages of the news type and use the protocol to view public folders.

Public folders cannot be viewed via NNTP protocol if its name include a blank space or the **.** sign (dot).

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.

If *Kerio MailServer* is installed on a server which is used as a domain controller (in *Active Directory*), it is necessary to run LDAP and LDAPS services on a non-standard

[1] TLS is follower of the SSL protocol, it is actually SSL version 3.1

port or to disable them.

HTTP
The HTTP protocol is used for:

- accessing user mailboxes via *Kerio WebMail*,
- accessing the user administration via the *KMS Web Administration* interface (see chapter 31),
- accessing mail using *Microsoft Entourage* mail client (see chapter 38),
- accessing the *Free/Busy* server,
- automatic upgrades of new versions of the *Kerio Outlook Connector* and the *Kerio Outlook Connector (Offline Edition)*.
- for synchronization via *Kerio Synchronization Plug-in*.
- for synchronization via the *ActiveSync* protocol.
- for *BlackBerry* synchronization via *NotifyLink*.
- for publishing of calendars as iCal

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

Upon the first startup of *Kerio MailServer*, all the services listed above are running on their default (standard) ports.

Note: If you know that services will not be used, it is recommended to disable them (for security reasons).

If any service provided also by *Kerio MailServer* is already running on the server, it is necessary to change traffic port for one of the services. To change a port of a *Kerio MailServer's* service, follow the instructions in section 6.1.

6.1 Service Parameter Settings

The service list (see figure 6.1) includes the following information:

- Service — includes protocol name and an icon informing whether the service is running or stopped.
- Status (running/stopped) — this item shows whether the service is running or stopped.
- Startup (Manual/Automatic) — information whether *Kerio MailServer* is started automatically or it must be run manually upon its restart.
- IP addresses — this item shows all IP addresses and ports used for traffic by the particular *Kerio MailServer's* service.
- Limit Access — *Kerio MailServer* allows narrowing access rights to a certain group of IP addresses which will be allowed to use the particular service (usually, unsecured services are accessible from the local network only).

The parameters of a selected service can be changed. To do this, use the *Edit* button. The button opens the *Service* dialog (see figure 6.2). The dialog consists of the following tabs:

Features

This tab allows setting of startup type and of a TCP port for traffic.

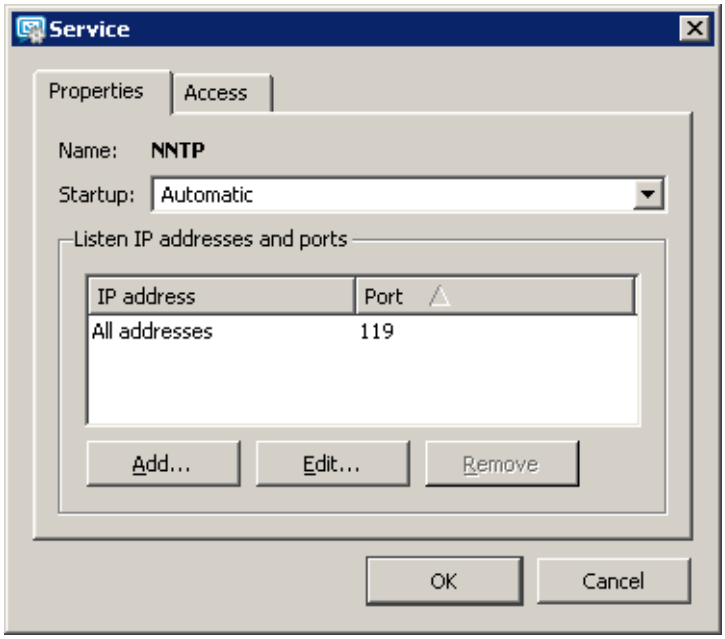

Figure 6.2 Service Parameters

Name

Type of service.

Startup

Kerio MailServer allows two startup modes:

- *Automatically* — the service will be run automatically upon *Kerio MailServer's* startup.
- *Manually* — when the server is started, the service is stopped and it must be run by the administrator if desirable.

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.

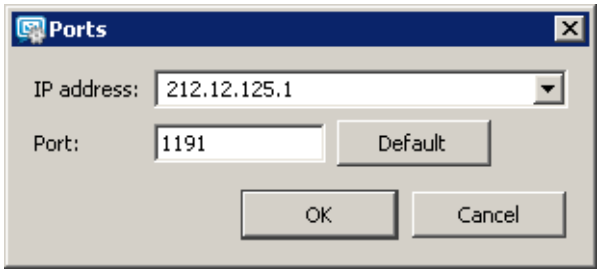

Figure 6.3 Ports

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.

Access

The *Access* tab allows setting limits for access to the particular service. The following parameters can be set:

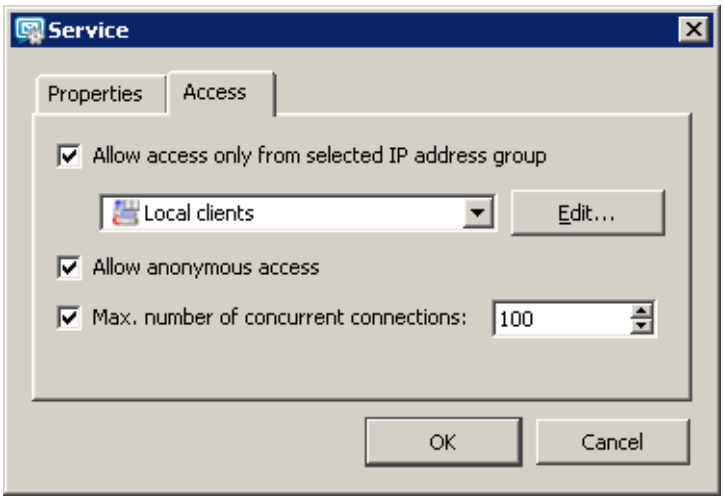

Figure 6.4 Limiting access to service

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.

6.2 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.

6.3 Troubleshooting

When solving problems regarding services, logs of the traffic between the server and clients might be helpful. To log relevant information, enable a corresponding option under *Logs* → *Debug* in the *Kerio Administration Console*:

1. In the *Kerio Administration Console*, go to the *Logs* section and select the *Debug* log.

2. Right-click on the log pane to open a context menu, and select *Messages*.

3. In the *Logged Information* dialog just opened, enable logging for the particular service (see figure 6.5).

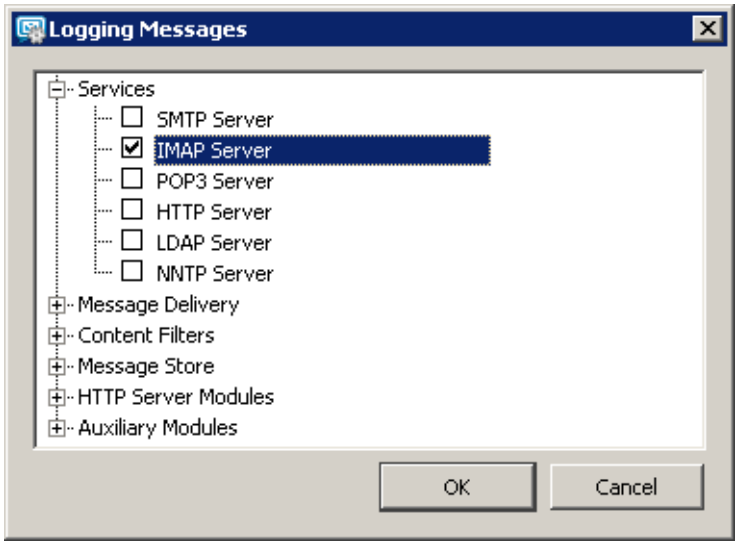

Figure 6.5 The Debug log settings

4. Confirm changes by OK.

The following types of services are associated with the *Debug* log options:

SMTP

If any problems arise in the communication between the SMTP server and a client, it is possible to use the *SMTP Server* and *SMTP Client* options.

POP3

When problems with POP3 server arise, enabling the *POP3 Server* option might be helpful.

IMAP

When problems with IMAP server arise, enabling of the *IMAP Server* logging might be helpful.

NNTP

When problems with NNTP server arise, a log that can be enabled by the *NNTP Server* option might help.

LDAP

When problems with LDAP server arise, a log that can be enabled by the *LDAP Server* option might help.

HTTP

- *HTTP Server* — this option enables logging of HTTP traffic on the server's side.
- *WebDAV Server Request* — this option enables logging of queries sent from the WebDAV server. It can be used in *MS Entourage* or *Apple Mail* where problems with Exchange accounts arise.
- *SyncML Synchronization* — this option enables log that stores information on synchronization of calendars and contacts over the *SyncML Plug-in*. The log may be helpful when solving problems with synchronization over the *Kerio Synchronization Plug-in*.
- *PHP Engine Messages* — the log may be helpful when solving problems with the *Kerio WebMail* web interface.

Once your problems are solved, it is recommended to disable the logging.

To read more on the *Debug* log and its options, see chapter 22.8.

Chapter 7

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 `company.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 `company.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 defines separately in each domain. Therefore, domains must be have been defined before accounts are created.

7.1 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.

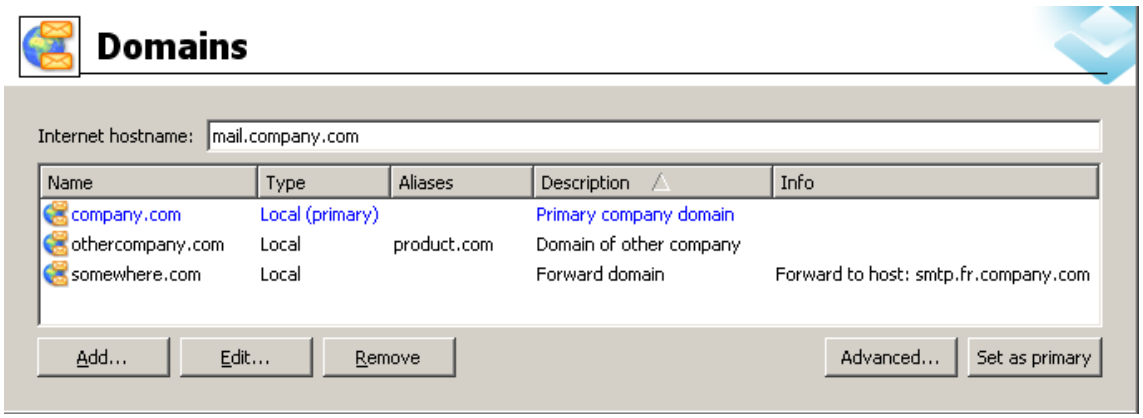

Figure 7.1 Domains

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 13).
- *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 13.5).
- the aliases are defined in it. First, delete all the aliases (for details, see chapter 15.3).
- it is the primary domain. However, you can create another domain and define it as primary. Then, the former domain can be deleted.

7.2 General

Basic domain parameters — the General bookmark:

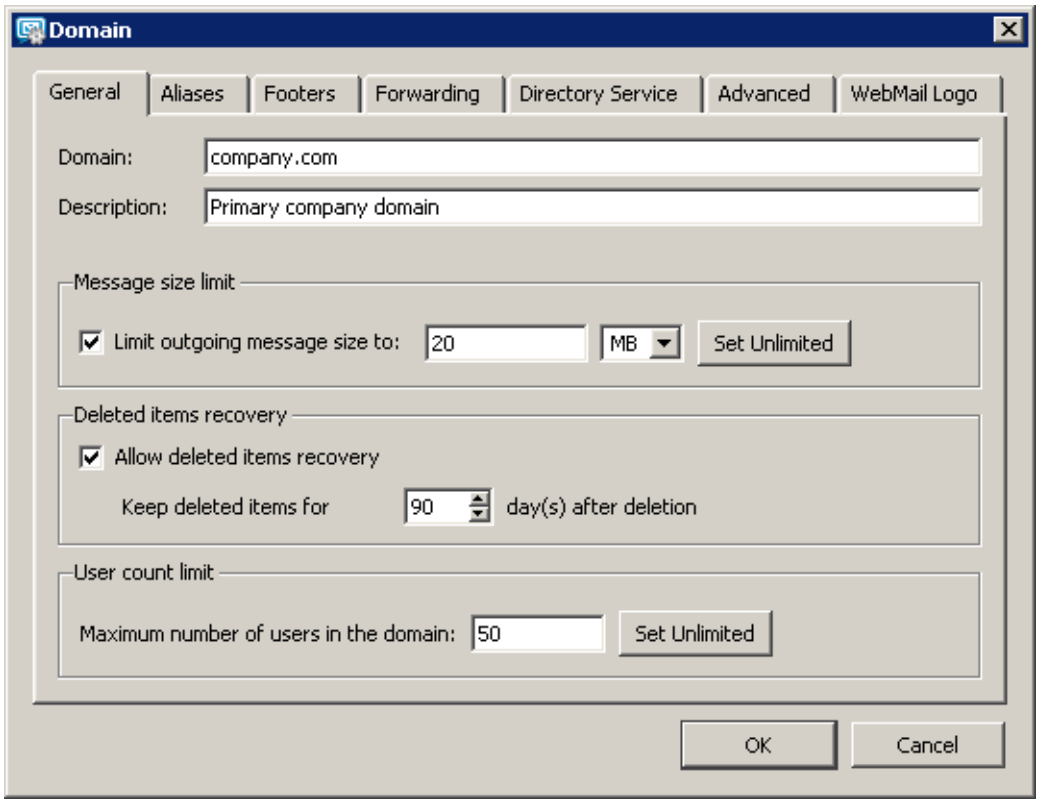

Figure 7.2 Domain settings — basic parameters

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).

Symbols	Restrictions
a-z	these characters are allowed, no restrictions are applied
0-9	these characters are allowed, no restrictions are applied
A-Z	these characters are allowed, no restrictions are applied
.	this symbol is allowed unless at the beginning and/or the end of the string and unless there are two dots next to each other
-	this symbol is allowed, no restrictions are applied

Table 7.1 Symbols allowed in domain name

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`

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 13.2). 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, notes and 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 disk 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 information about restoring items for selected users, see chapter 13.7.

User count limit

This option is useful especially when administration of user accounts via web interface is used (see chapter 31). Users with administration rights cannot break this limit.

7.3 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 was 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 records must be defined in DNS 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.

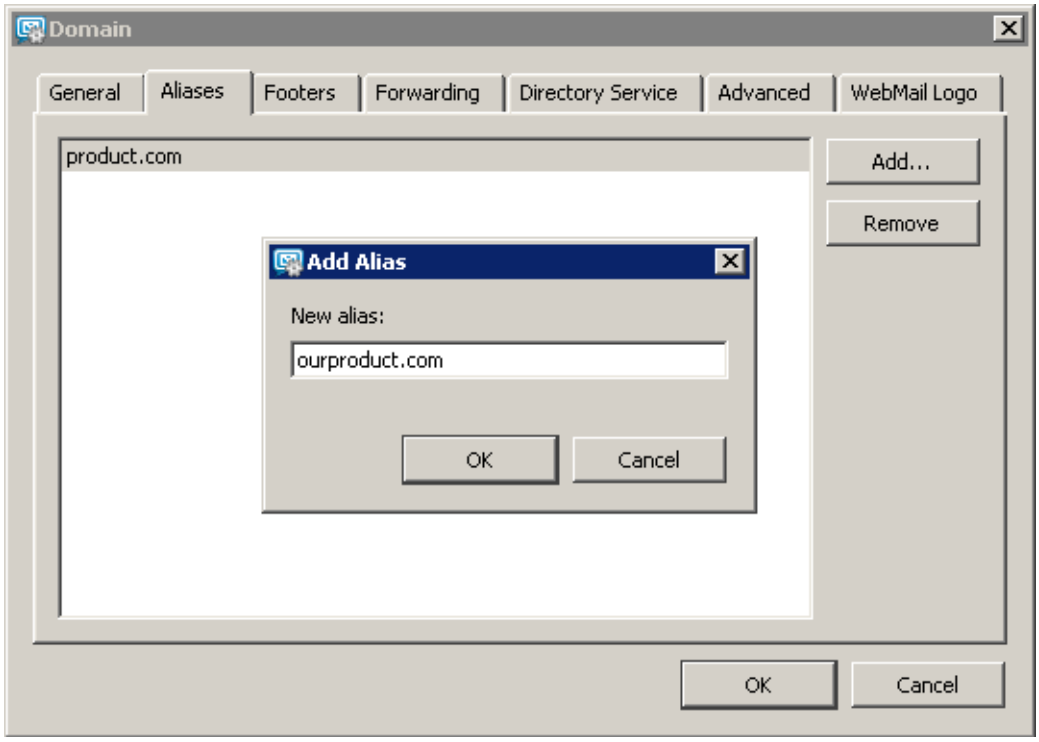

Figure 7.3 Domain settings — equivalent domains (aliases)

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.

7.4 Footers

This tab enables to append the default footer (the footer will be added to each message where sender's address includes the domain) to email messages of this domain.

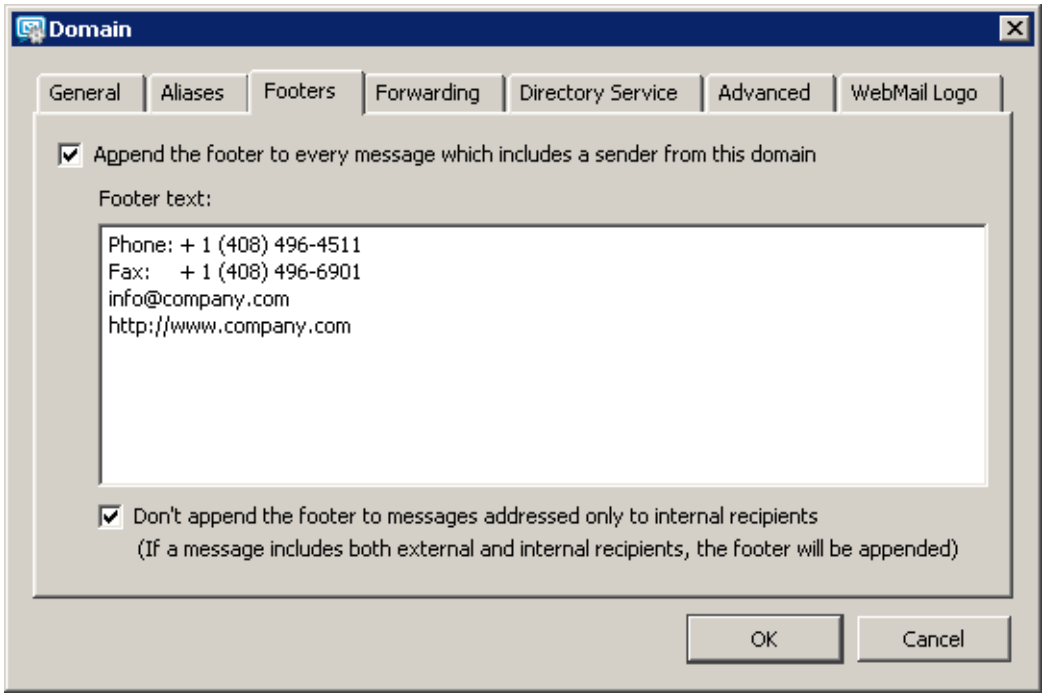

Figure 7.4 Domain settings — footers

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

Since it might be irrelevant to append footers to messages delivered within *Kerio MailServer*, it is possible to allow footers only for messages which are not delivered locally. This can be set by using the *Don't append the footer to messages addressed only to internal recipients* option.

7.5 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 27.4),
- creating a backup mailserver (for more information, see chapter 27.5).

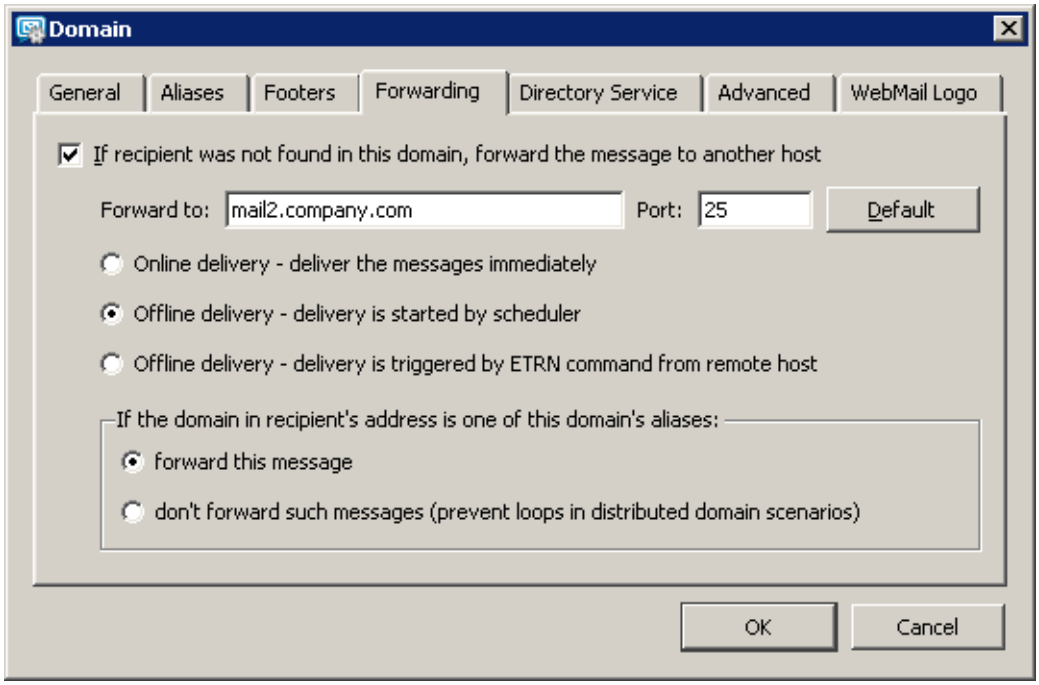

Figure 7.5 Domain settings — forwarding

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*).

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.

Online delivery — deliver the messages immediately

This option is helpful when it is intended to divide a domain to multiple servers while a persistent Internet connection is provided (for details, see chapter 27.4).

Online delivery follows SMTP delivery settings (*Configuration* → *SMTP server* → *Queue options*). For details on this tab, see chapter 15.2.

Offline delivery — delivery is started by scheduler

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 9).

Offline delivery — delivery is triggered by ETRN command from remote host

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 15.1) 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.
Note: If the domain is covered by two servers, set this option on one of them only (for detailed description of a domain covered by two and more servers, see chapter 27.4).

7.6 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 Mac OS X — 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 13.2), install *Kerio Active Directory Extensions* on the *Active Directory* server. For details see the chapter 29.

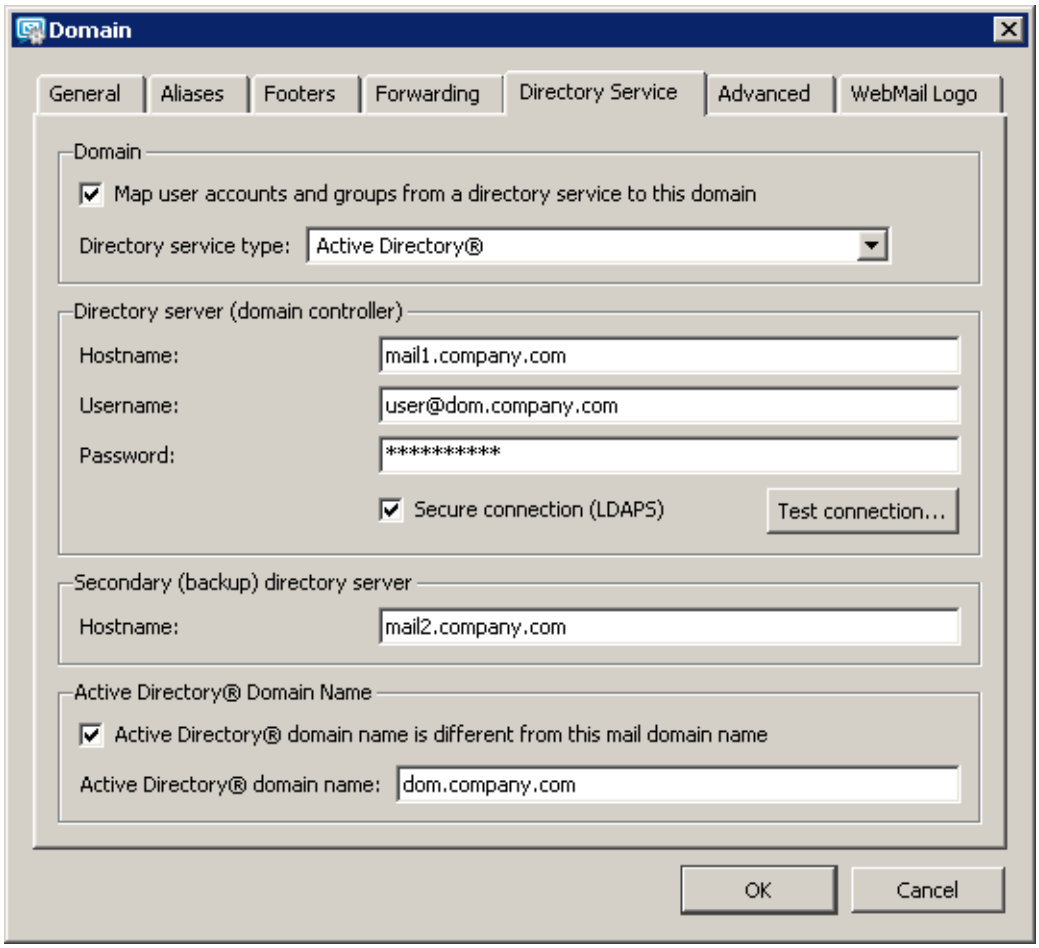

Figure 7.6 Domain settings — Active Directory

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 (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 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 has read rights for the LDAP database in the following form: `xxxxx@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. 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*.
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.

Backup directory server
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 29).

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 19). 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 13.2), install the *Kerio Open Directory Extensions* on the *Open Directory Master* and all replica servers. For details see the chapter 30.

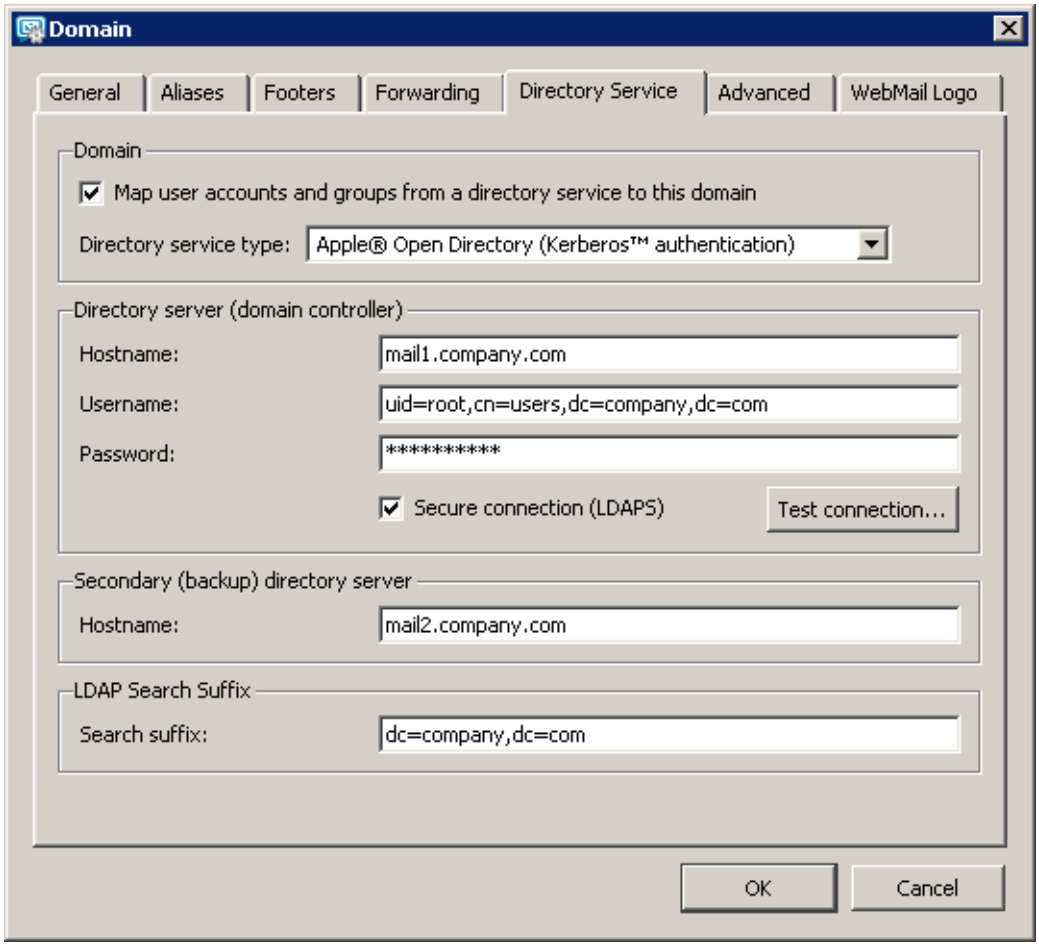

Figure 7.7 Domain settings — Apple Open Directory

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. There are two alternatives of mapping of *Apple Open Directory* accounts that differ in authentication method. Two authentication methods can be used in *Apple Open Directory*: authentication against the password server and Kerberos authentication.

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:

- This authentication method is obsolete and less secure.
- Users are not allowed to change their user passwords on their own (in the *Kerio WebMail* interface).
- The *Apple* company has ended 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 24.

Up to 6.1.3, *Kerio MailServer* used authentication against the password server by default. Since *Kerio MailServer 6.1.4* it is possible to choose an authentication method. It should be also remembered that in the domain settings on the *Advanced* tab under *Configuration* → *Domains* in the *Kerio MailServer's* administration console, name of the Kerberos area must be specified against which the mailserver will be authenticated. It is necessary that the name matches the name of Kerberos area specified in the `/Library/Preferences/edu.mit.Kerberos` file, otherwise the settings will not function properly. For detailed description on authentication against the Kerberos server on Mac OS X operating systems, see chapter 24.3).

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 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=mail1,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 19). However, if the *MailServer* is

installed on an *Apple Open Directory* server the LDAP listening port in the *MailServer's Configuration → Services* must be changed to an alternate port to avoid a port conflict.

7.7 Advanced

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

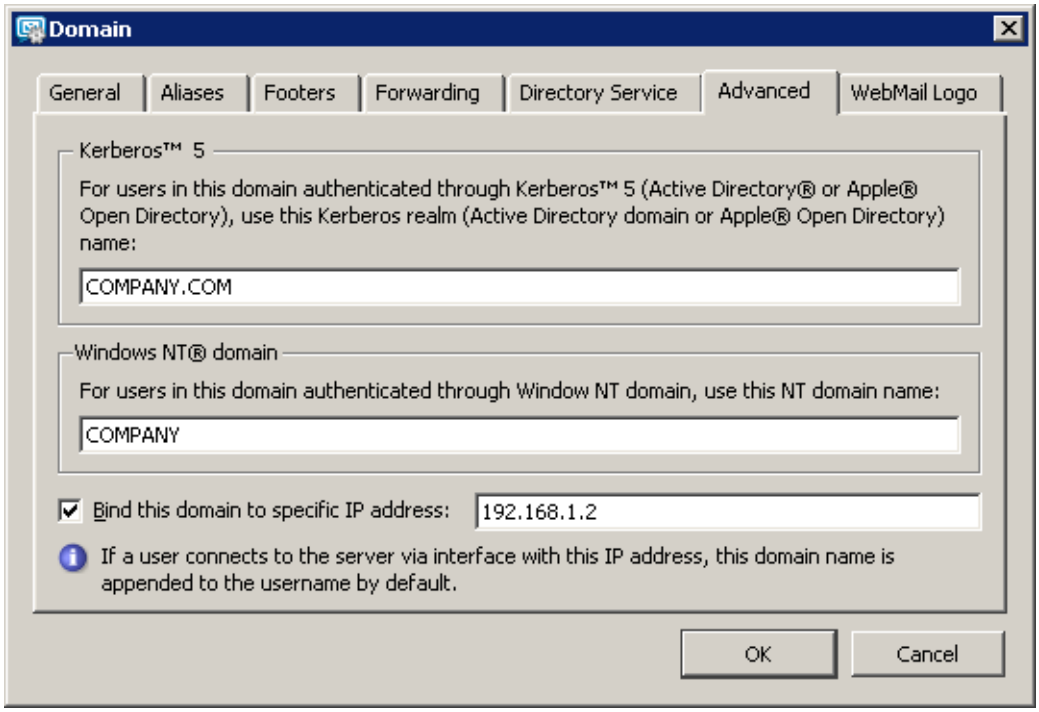

Figure 7.8 Domain settings — parameters for users authentication

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 an authorization and authentication protocol (for details, see information at `http://web.mit.edu/Kerberos/`). *Kerio MailServer* uses this protocol 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. Since *Kerio MailServer 6.0.9*, the name of the Kerberos realm must be in capital letters.

If user account are saved in *Active Directory* or in *Open Directory* (see the *Directory Service* tab), it is required to specify name of the *Active Directory* or the *Open Directory* domain here. If you use the *LDAP database* tab for *Active Directory* definition, this entry will be specified automatically.

Warning: If you use *Open Directory* or a stand-alone Kerberos server, check thoroughly that the Kerberos realm specified on the *Advanced* tab matches the name of Kerberos realm in the `/Library/Preferences/edu.mit.Kerberos` file. In particular, it must match the `default_realm` value in this file. By result, the line may be for example `default_realm = COMPANY.COM`

Authentication settings for the individual platforms are described in chapter 24.

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`.

Note: When creating a user account you can choose how the given user will be authenticated (see chapter 13.2). Different users can be authenticated using different methods in a single email domain.

Bind this domain to specific IP address

Users can use any interface for connection to *Kerio MailServer*. However, each domain can be bound with one IP address. Binding of an IP address with a domain saves users connecting from such an IP address from the necessity of including domain in username (e.g. `jsmith@company.com`) for each login attempt. This implies that such users can use separate user name (e.g. `jsmith`) as if connecting to the primary domain.

Warning: Correct functionality of binding of domains with an IP address requires at most one domain to be bound to each IP address. Otherwise the server would not recognize to which domain the username with no domain defined belongs.

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.

Troubleshooting of external authentication issues

If a problem arises with any of the authentication methods, in *Kerio MailServer*, it is possible to enable logging of external user authentication:

1. In the *Kerio Administration Console*, go to the *Logs* section and select the *Debug* log.
2. Right-click on the log pane to open a context menu, and select *Messages*.
3. In the *Logging messages* dialog box, select *User Authentication*.
4. Confirm changes by OK.

Once your problems are solved, it is recommended to disable the logging.

7.8 WebMail Logo

Each domain in *Kerio MailServer* can have its own *Kerio WebMail* logo (for detailed information about the logo settings, see chapter 11.2).

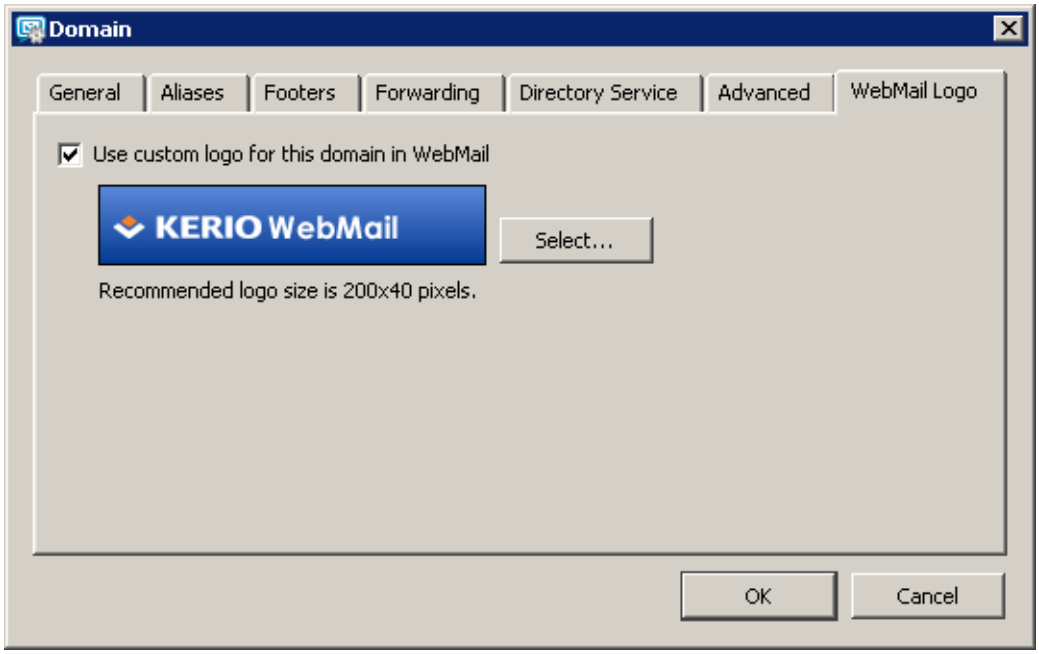

Figure 7.9 Domain settings — Kerio WebMail logo

The recommended parameters of the logo:

- Format: GIF
- Size: 200x40 pixels

Click *Select* to browse to the logo file.

Chapter 8

Internet Connection

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

8.1 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.

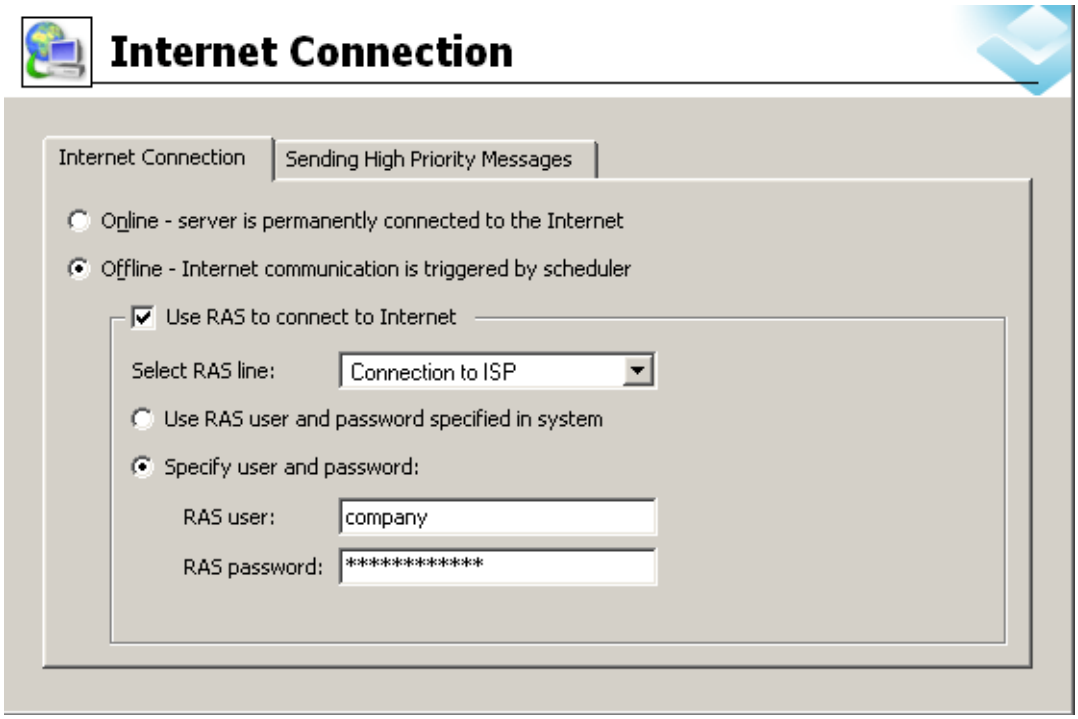

Figure 8.1 Internet Connection tab

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 15.4.

4. Details about setting the scheduler can be found in chapter 9.

8.2 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.

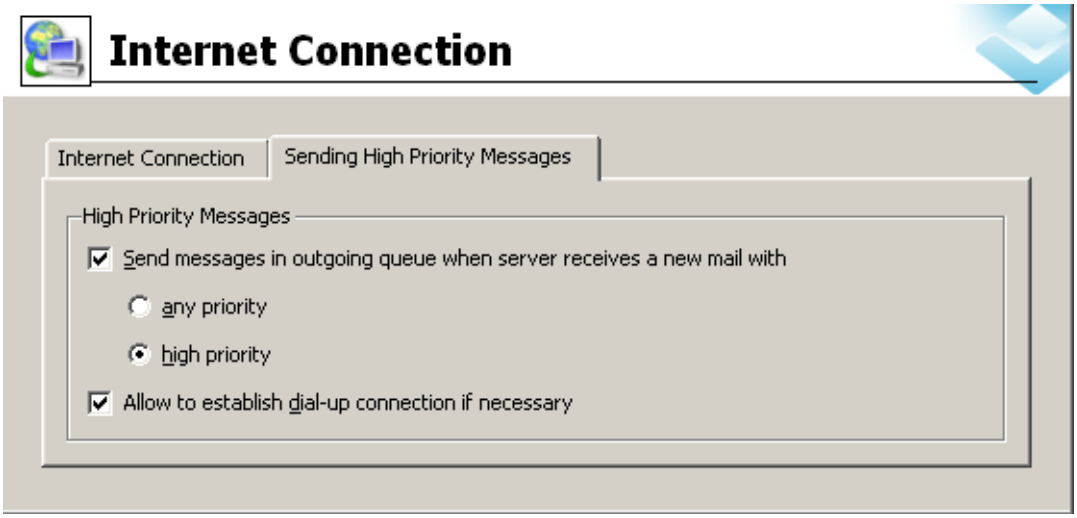

Figure 8.2 Sending High Priority Messages tab

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 9

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 8).

9.1 Setting Up the Scheduler

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

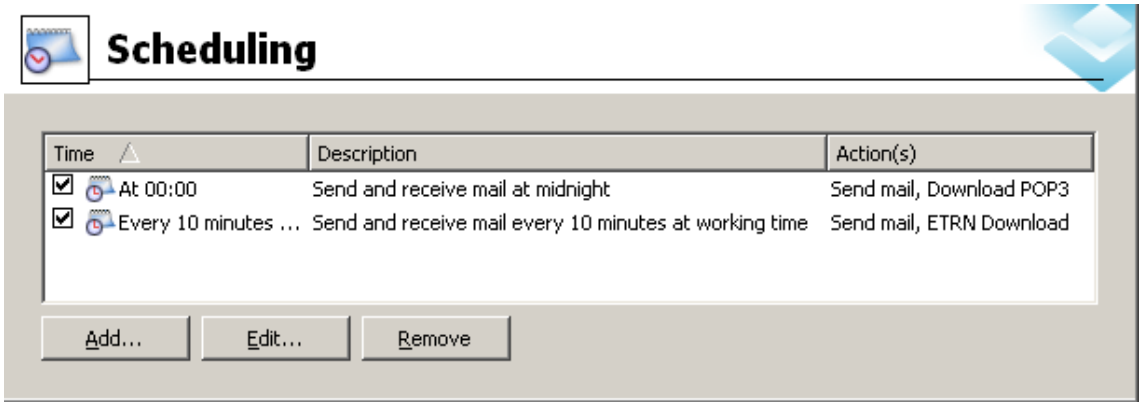

Figure 9.1 Scheduling

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:

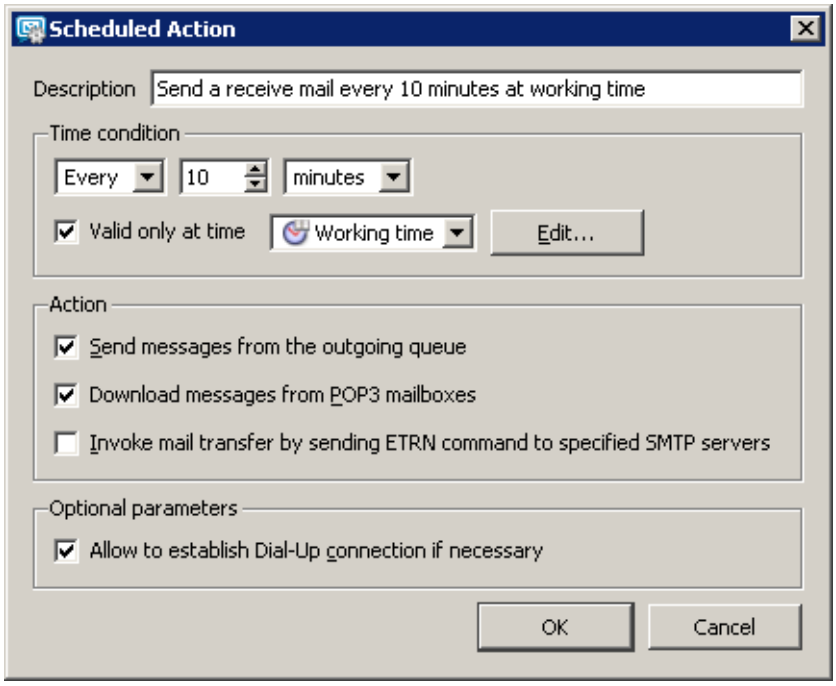

Figure 9.2 Scheduled Action

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.

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 12.2 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.

9.2 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 (*Online*) 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 10

Server's Certificates

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). This method ensures that 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 6) or by setting appropriate security policy (refer to chapter 15.6). Once the server is configured, it is necessary to install a certificate (even a self-signed one) or certificates on clients of all users using *Kerio MailServer's* services.

10.1 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 10.1 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.company.com`), which you must also use in the client (this certificate has been issued for a fictitious name `keriomail`).

Now, there are two options. One is to keep in *Kerio MailServer* the self-signed certificate generated during the mailserver's installation, the other option is to get a certificate authorized by a certification authority. It should be possible to install both types of certificates on client stations. In both cases, it is necessary that the certificate is maintained in the *Kerio MailServer's Configuration* → *SSL certificates* section (see figure 10.2).

In *SSL certificates*, it is possible to create certificates, generate certificate demands for certification authorities as well as export certificates. Here is an overview of all options:

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`.

Figure 10.2 SSL Certificates

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.
- *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.

Figure 10.3 Certificate Creation

View Certificate

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

Figure 10.4 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.

Intermediate certificates

Kerio MailServer allows authentication by so called "intermediate" certificate. To make authentication by these certificates work, it is necessary to add the certificates to *Kerio MailServer* by using any of the following methods:

Locally
Add the "intermediate" certificate file to the `/sslca` directory and copy the server's certificate with the private key to the `/sslcert` directory. Both directories can be found in the directory where *Kerio MailServer* is installed.

Remotely via the Kerio Administration Console
Remote import can be performed as follows:

1. Open the server's certificate and the "intermediate" certificate in any text editor.
2. In the "intermediate" certificate, select the certificate's string and copy it to the server certificate file next to the string of the server certificate. The certificate file should then be as follows:

```
-----BEGIN CERTIFICATE-----
MIIDOjCCAqOgAwIBAgIDPmR/MA0GCSqGSIb3DQEBBAUAMFMxCzAJBgNVBAYTAl
MSUwIwYDVQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMR0wGwYDVQ
     ..... this is a server SSL certificate ...
ukrkDt4cgQxE6JSEprDiP+nShuh9uk4aUCKMg/g3VgEMulkROzFl6zinDg5grz
QspOQTEYoqrc3H4Bwt8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDMzCCApygAwIBAgIEMAAAATANBgkqhkiG9w0BAQUFADCBxDELMAkGA1UEBh
WkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
     ..... this is an intermediate SSL certificate which
           signed the server certificate...
5BjLqgQRk82bFi1uoG9bNm+E6o3tiUEDywrgrVX60CjbW1+y0CdMaq7dlpszRB
t14EmBxKYw==
-----END CERTIFICATE-----
```

3. Save the certificate.
4. Open the *Kerio Administration Console* and go to the section referring to SSL certificates.
5. Import the server's certificate by using the *Import* → *Import new certificate* option.

10.2 Install certificates on client stations

Only in the following cases it is necessary to install certificate on the client station:

- If *MS Outlook* extended by the *Kerio Outlook Connector* is used on the station and secured HTTP traffic is desired between the server and the client (typically when the *Free/Busy* server is used). In such a case, it is necessary to install the certificate, otherwise the communication will not work.
- If *MS Outlook* with the *Kerio Synchronization Plug-in* is used on the station and folders are planned to be synchronized by an SSL-secured protocol. In such a case, it is necessary to install the certificate, otherwise the communication will not work.
- If *MS Entourage* is used and its services are planned to be secured by SSL encryption. In such a case, it is necessary to install the certificate, otherwise the communication will not work.
- For connections to *Kerio WebMail* over HTTPS. If the certificate is not installed, an alert warning of the fact is displayed upon each login (see figure 10.1).

The simplest way to install a certificate is to use a web browser.

Installation in Internet Explorer

Internet Explorer is helpful where the certificate is to be installed to the *MS Outlook* store (*Internet Explorer* and *MS Outlook* share the same certificate store) or where connection to *Kerio WebMail* is to be performed over HTTPS.

To install a certificate, follow these instructions:

1. Run *Internet Explorer* and specify the corresponding URL to login to *Kerio WebMail*. SSL-secured protocol must be used for the connection to the server. This implies that the URL should start with `https://` (example: `https://mail.company.com/`).

2. The *Security Alert* dialog will be opened (see figure 10.1). In this dialog, click on *View certificate*.

3. In the dialog with certificate details displayed, click on the *Install certificate* button.

4. A certificate installation wizard is opened. There is nothing to be set in the wizard. Simply confirm all settings and close the wizard to install the certificate.

Installation in Safari

SSL certificate is required whenever applications are to communicate with *Kerio MailServer* by SSL-secured services. The *Kerio MailServer* certificate can be installed by using the Safari browser (simply connect to the *Kerio WebMail* interface via `https://`):

1. Run *Safari* and specify the corresponding URL to login to *Kerio WebMail*. SSL-secured protocol must be used for the connection to the server. This implies that the URL should start with `https://` (example: `https://mail.company.com/`).

2. Before the *Kerio WebMail's* login page is opened, an alert is displayed informing that the system is not able to authorize the server to which you are connecting since the certificate is authorized by an unknown authority (see figure 10.5).

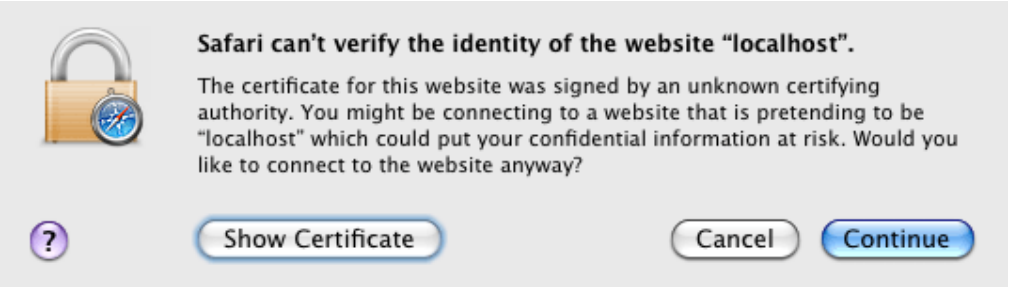

Figure 10.5 Alert on an untrustworthy certificate

3. The alert dialog contains the *Show certificate* button. Click on it to show the certificate (see figure 10.6).

4. Use the mouse pointer to move the certificate's icon to the desktop, as shown at figure 10.7.

Now, all depends on Mac OS version. For Mac OS X 10.3 Panther and Mac OS X 10.4 Tiger, follow these instructions:

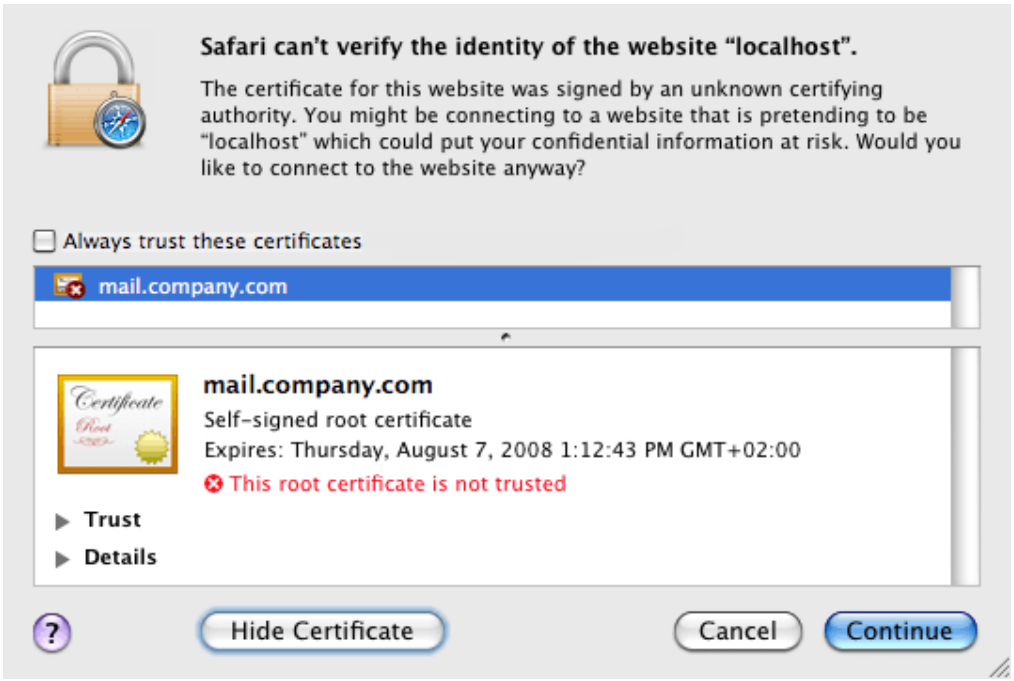

Figure 10.6 Certificate Details

Figure 10.7 Moving the certificate to the desktop

1. On the desktop, click on the certificate. In the *Add Certificates* dialog box (see figure 10.8), 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.[2]

Figure 10.8 The Add Certificates dialog box

2. Administration password is required if you are not logged in as a root user or as an administrator.

3. Along with the *Add Certificates* dialog, the *Keychain Access* store is opened. If not, it can be found in *Applications* → *Utilities* → *Keychain Access*.

4. In the *Keychain Access* application, switch to the *Certificates* tab.

5. Move the certificate from the desktop to the *Keychain Access* application's window. Check that the moved certificate is included in the certificate list (see figure 10.9).

For Mac OS X 10.5 Leopard, follow these instructions:

1. On the desktop, click on the certificate. In the *Add Certificates* window (see figure 10.10), select the *System* option in the *Keychain* menu (all system users will be allowed to use the certificate) or *Login* (only authenticated users will be allowed to use the certificate). Click OK to confirm changes.

[2] 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.

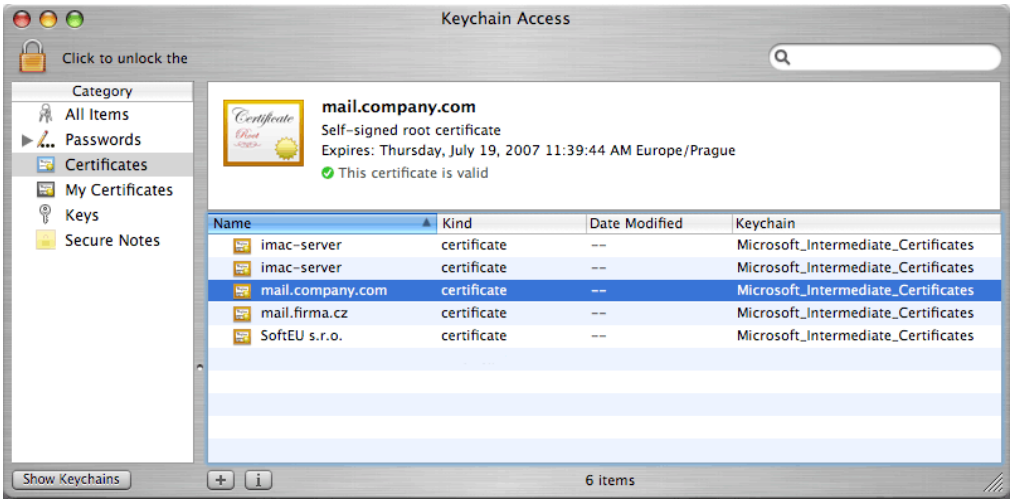

Figure 10.9 Keychain Access — the Certificates tab

Figure 10.10 The Add Certificates dialog box

2. The *Keychain Access* application is started, asking for confirmation that you really want to install the certificate. Confirm the dialog by entering username and password for an account with administration rights.

Installation on mobile devices

To install SSL certificate on mobile devices, use *Internet Explorer*. Import and installation processes vary, depending on a device type. Instructions on installation of SSL-certificates for all supported devices can be found in chapter 36.4.

Chapter 11

Kerio WebMail parameters

Detailed information about *Kerio WebMail* is provided in a standalone document *Kerio MailServer, User's Guide*. This manual is available at *Kerio Technologies* website (`http://www.kerio.com/kms-manual`).

11.1 Skins

Kerio WebMail contains a couple of default skins (skin = *Kerio WebMail* appearance). These skins are stored in the following 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\xyz`

where `xyz` stands for the name of the new skin.

11.2 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. To change the logo globally, use the *Logo* tab in the *Advanced options* (for detailed information, see chapter 15.6). The logos for the individual domains are set in the *Domains* section (see chapter 7.8). 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.

11.3 Language

Currently, *Kerio WebMail* includes the following language versions:

- English
- Czech
- Chinese
- French
- Dutch
- Croatian
- Italian
- Japanese
- Hungarian
- German
- Polish
- Portuguese
- Russian
- Slovak
- Spanish
- Swedish

Custom language version

If *Kerio WebMail* does not include the language localization you need, it is possible to create a custom language version.

All language texts displayed in the *Kerio WebMail* interface are saved in separate localization files. Localization XML files are stored in subdirectory `/translations` (in the directory where *Kerio MailServer* is installed). UTF-8 encoding is used.

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 therefore 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.

Opening of a new localization file requires restart of *Kerio MailServer*.

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 language databases for *Kerio MailServer* are stored. These files can be found in under the `myspell` 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 `myspell` folder. In order for the dictionaries to work properly, they must meet the `myspell` standard. These dictionaries are available on the Internet (e.g. at `http://wiki.services.openoffice.org/wiki/Dictionaries`). Each dictionary includes two files, following the patterns `language_name.aff` (e.g. `fr_FR.aff`) and `language_name.dic` (e.g. `fr_FR.dic`). Copy both files to the `myspell` folder.

To employ the dictionary in the spellchecker, it is necessary to set it as preferred in the *Kerio WebMail* settings:

1. Open the full version of *Kerio Webmail*.

2. Click on the *Settings* button on the toolbar.

3. This opens the dialog divided to several tabs. Switch to the *Mail composing* tab.

4. In the *Spell-checker dictionary* field, select a dictionary (see figure 11.1).

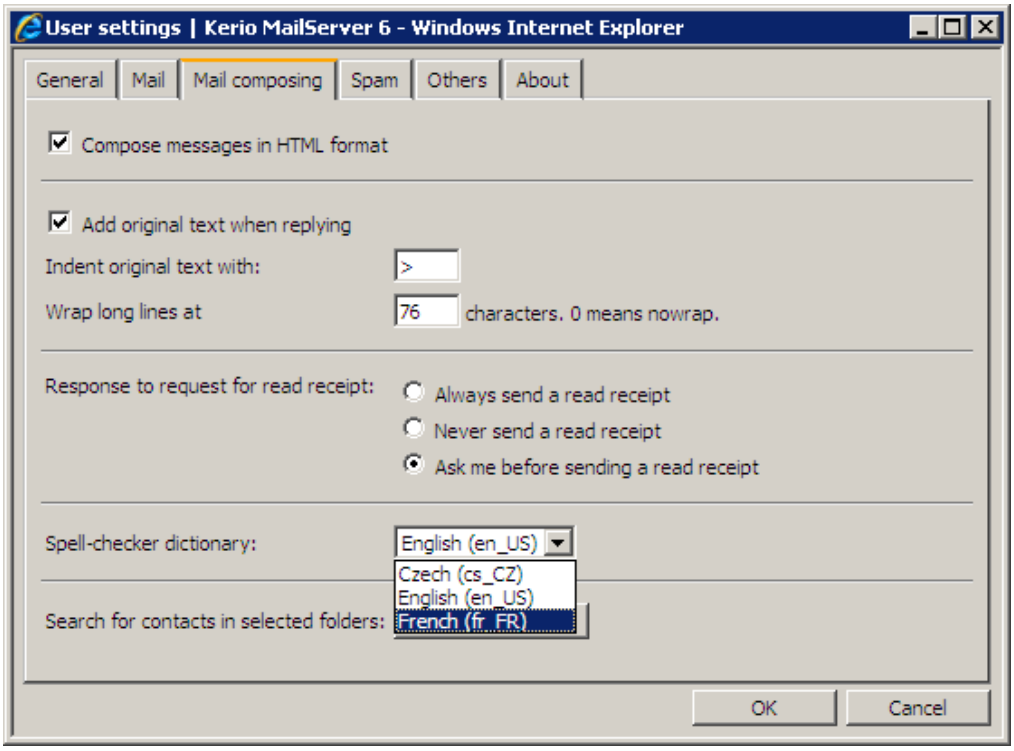

Figure 11.1 Dictionary selection in the Kerio WebMail settings

Chapter 12

Tools

12.1 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.

Group of IP addresses of local ranges is entered automatically. This group can be edited, removed or otherwise manipulated as well as other IP groups.

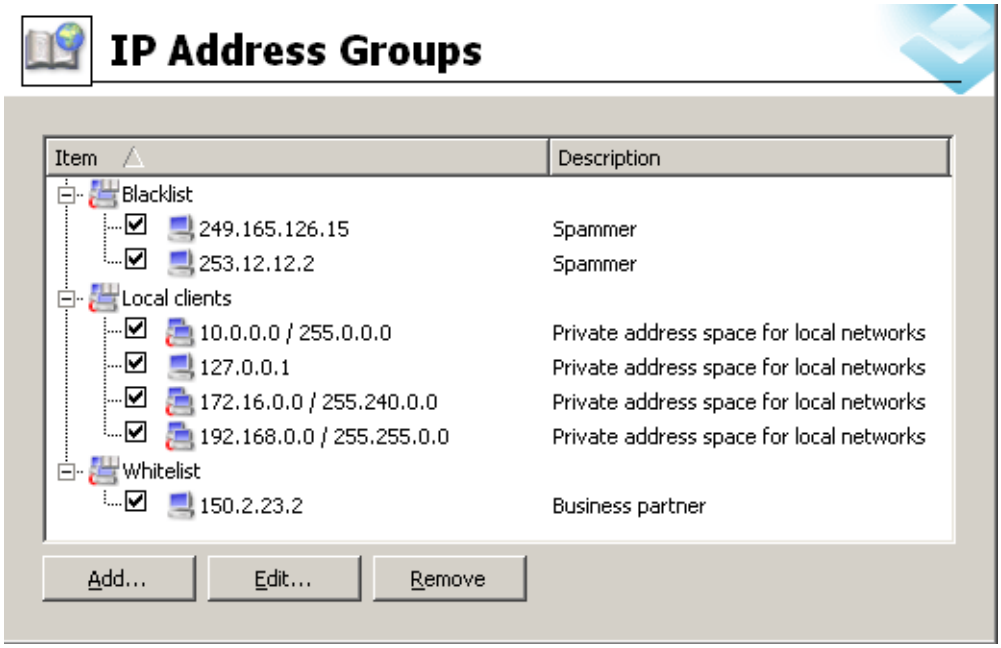

Figure 12.1 IP Address Groups

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:

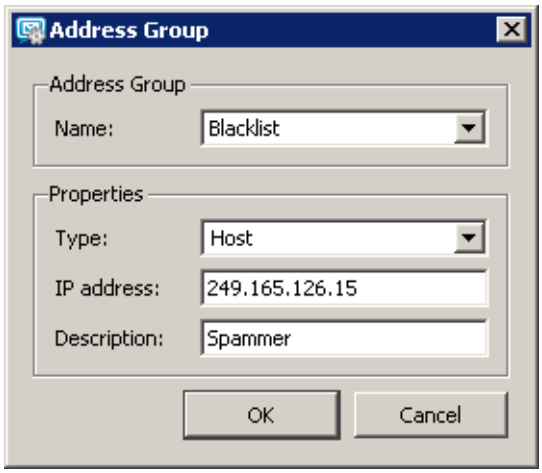

Figure 12.2 IP Address Groups Creation

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

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 cascadable.

IP address, Mask...
: Parameters of new item (dependent on selected type).

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

12.2 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.

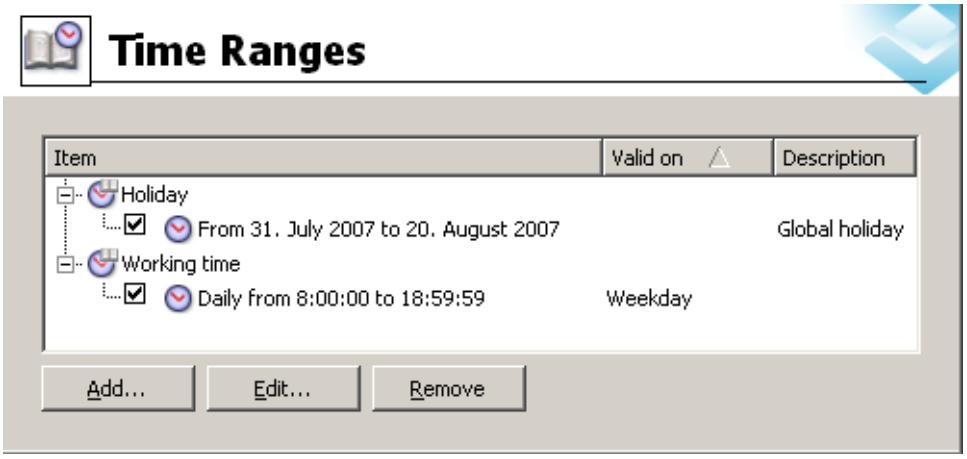

Figure 12.3 Time Intervals

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 | d2 | w1 | w2) & (a1 | 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:

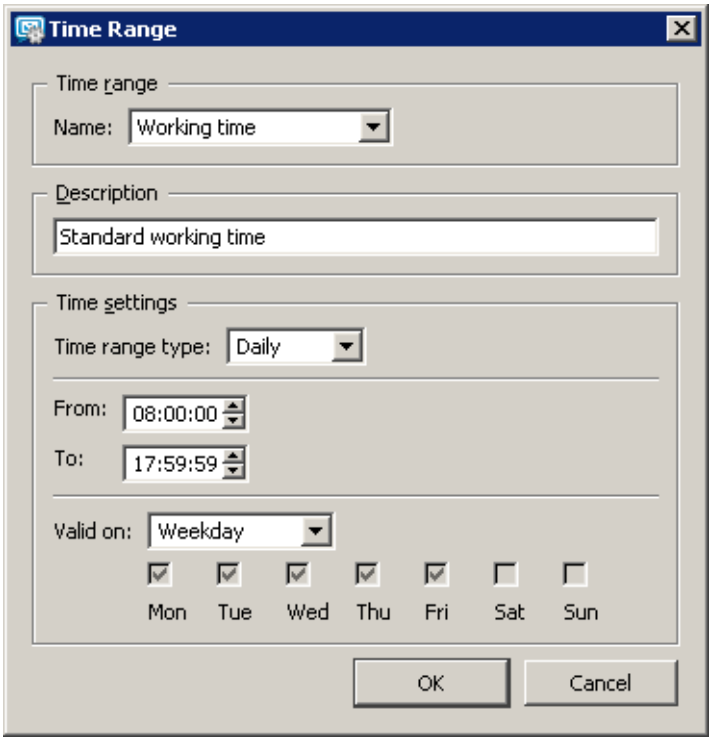

Figure 12.4 Defining Time Interval

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.

12.3 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*:

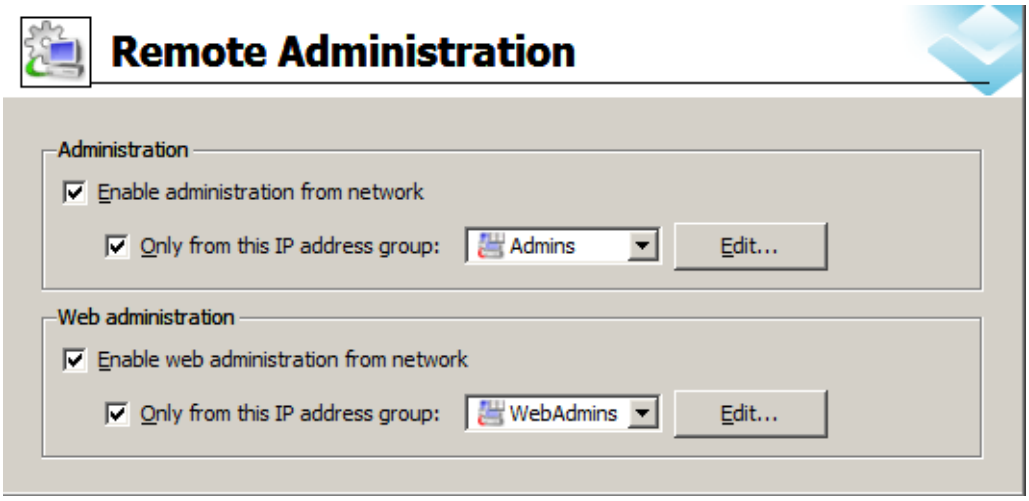

Figure 12.5 Remote Administration

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 12.1).

Web administration of users, groups and aliases

Enable web administration from network

This option enables administration via the Web interface. If this option is disabled, it is not possible to access the interface. For detailed description on administration via the web interface, see chapter 31.

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 12.1).

Chapter 13

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 7).

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 13.2),

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 7.6).

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

- import from the Novell eDirectory (more information in chapter 13.10),
- import from the NT domain (see chapter 13.10),
- import from the Active Directory domain (refer to chapter 13.10),
- imported from a text file.

13.1 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 18.2). Any message which passed through *Kerio MailServer* can be found in the archive.

Administrator can make archive folders shared with other users. 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.

13.2 Creating a user account

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

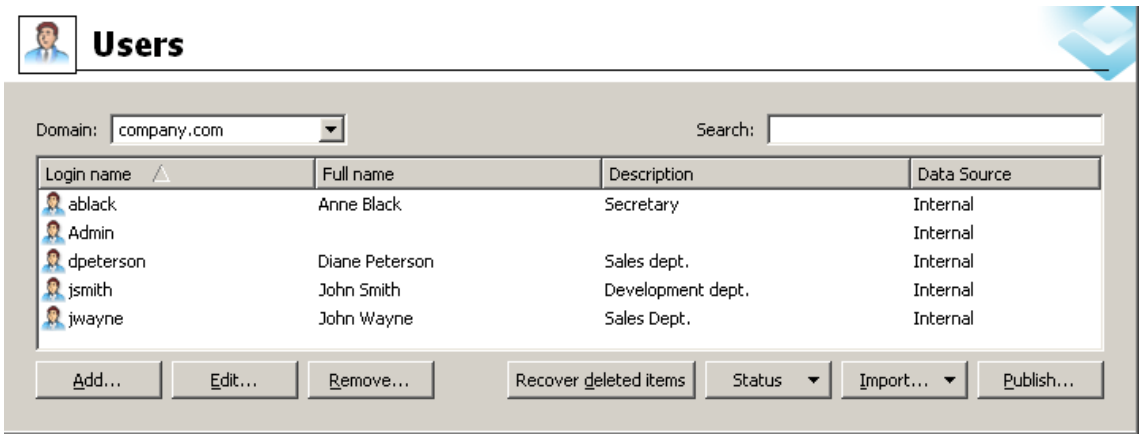

Figure 13.1 User accounts

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). The list of users of the particular domain includes both types of accounts. 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*, *Apple 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 7.6), 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.

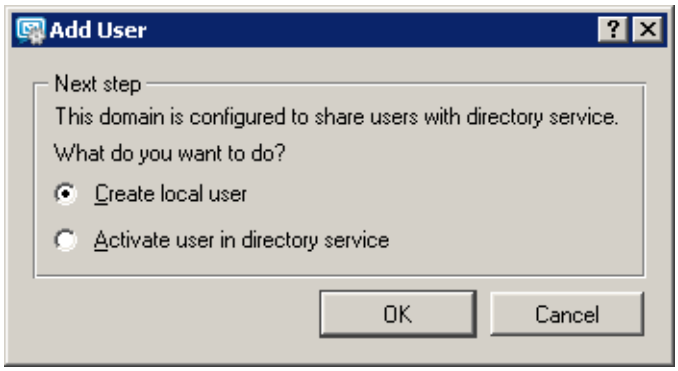

Figure 13.2 Activate user in directory service

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 for creating of new accounts is created. To create new user account templates, 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.

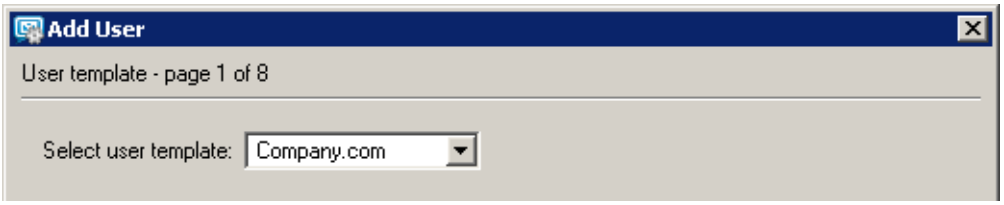

Figure 13.3 New user addition — a template

For information about creation of a new template, refer to chapter 13.12.

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.

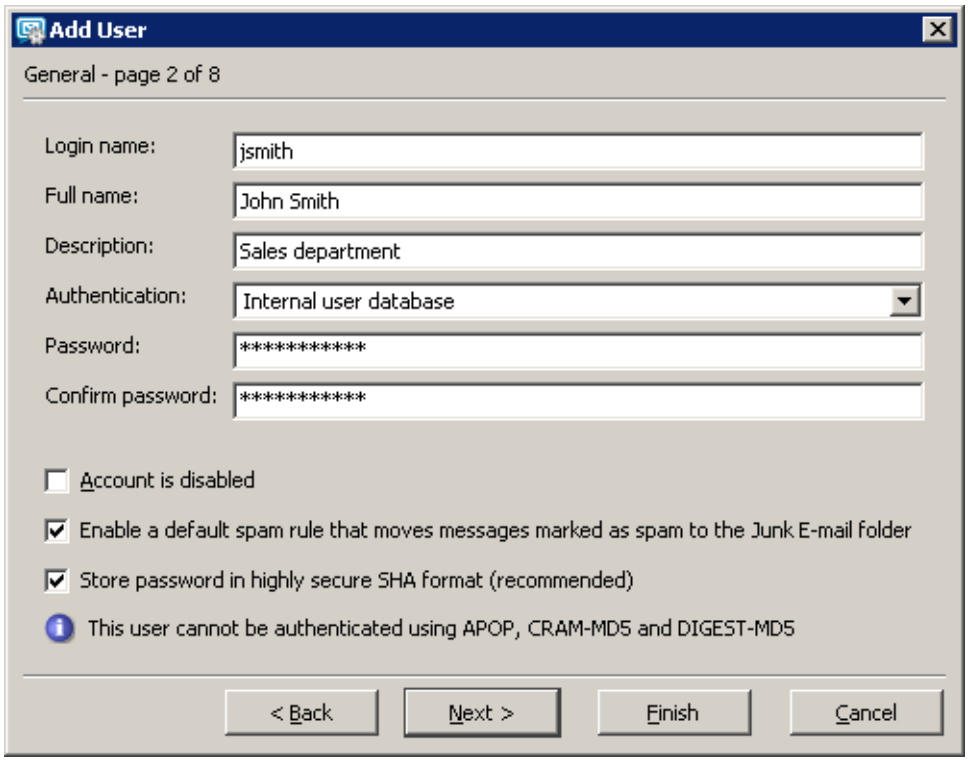

Figure 13.4 New user addition — basic data

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.

Symbols	Conditions
a–z	these characters are allowed, no restrictions are applied
0–9	these characters are allowed, no restrictions are applied
A–Z	these characters are allowed, no restrictions are applied
.	allowed unless at the beginning and/or the end of the string and unless there are two dots next to each other
-	this symbol is allowed, no restrictions are applied
_	this symbol is allowed, no restrictions are applied

Table 13.1 Characters and symbols allowed in user login name

Description

User description (e.g. a position in a company). The *Description* entry is for informative 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 7.7.
- *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.

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. Filtering and rules for incoming email is addressed in *Kerio MailServer, User's Guide*.

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.

Warning: This feature is not identical with account blocking set under *Configuration → Advanced Options*, on the *Security Policy* tab (see section 15.6). If the user enters an invalid password too many times in row and the limit set on the *Security Policy* tab is reached, the account is blocked automatically. To unblock the accounts, use the *Unlock all accounts now* button on the *Security Policy* tab.

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*.

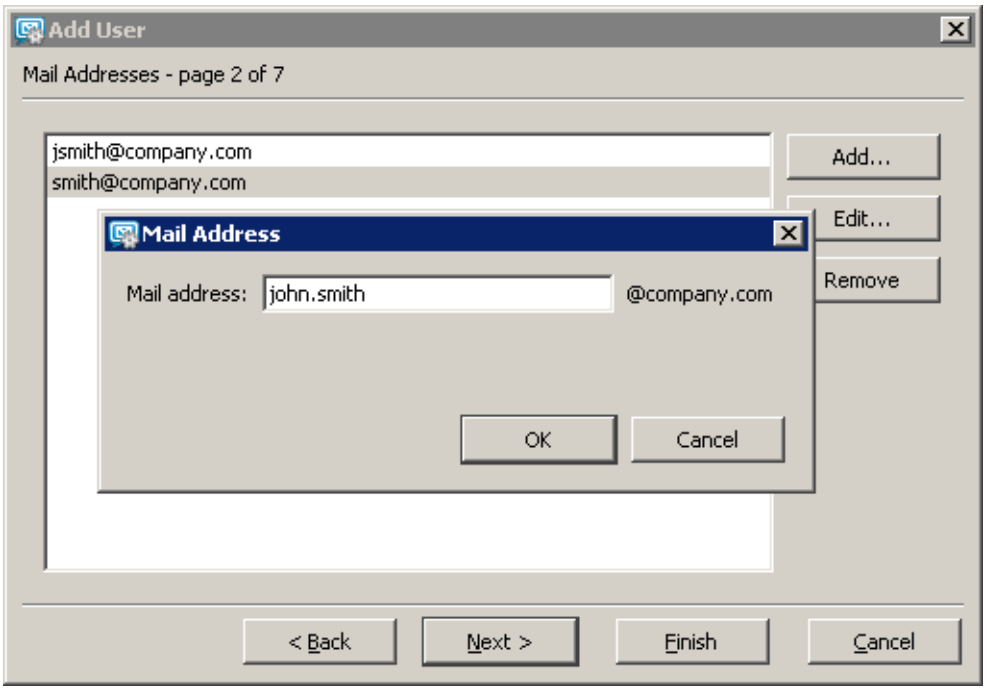

Figure 13.5 New user addition — email addresses

Note: If user accounts are maintained in *Active Directory* (see chapter 7.6), their aliases can be defined in *Active Directory Users and Computers*. Global aliases (in *Domain Settings* → *Aliases*) cannot be defined this way.

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.

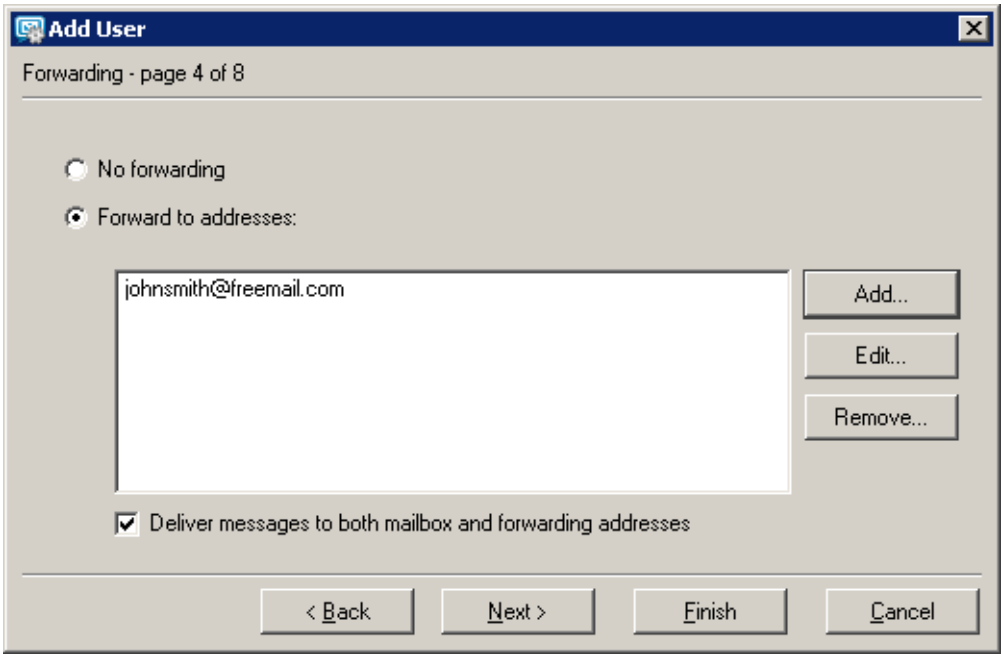

Figure 13.6 New user addition — forwarding messages to other addresses

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.

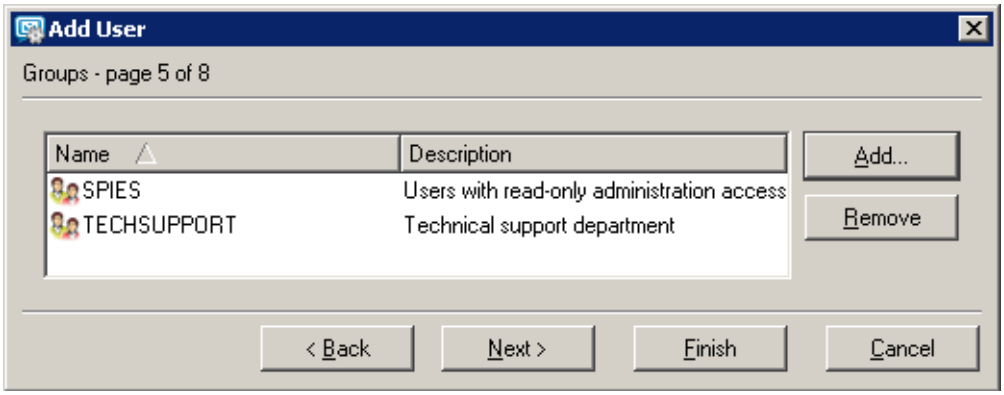

Figure 13.7 New user addition — groups

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.

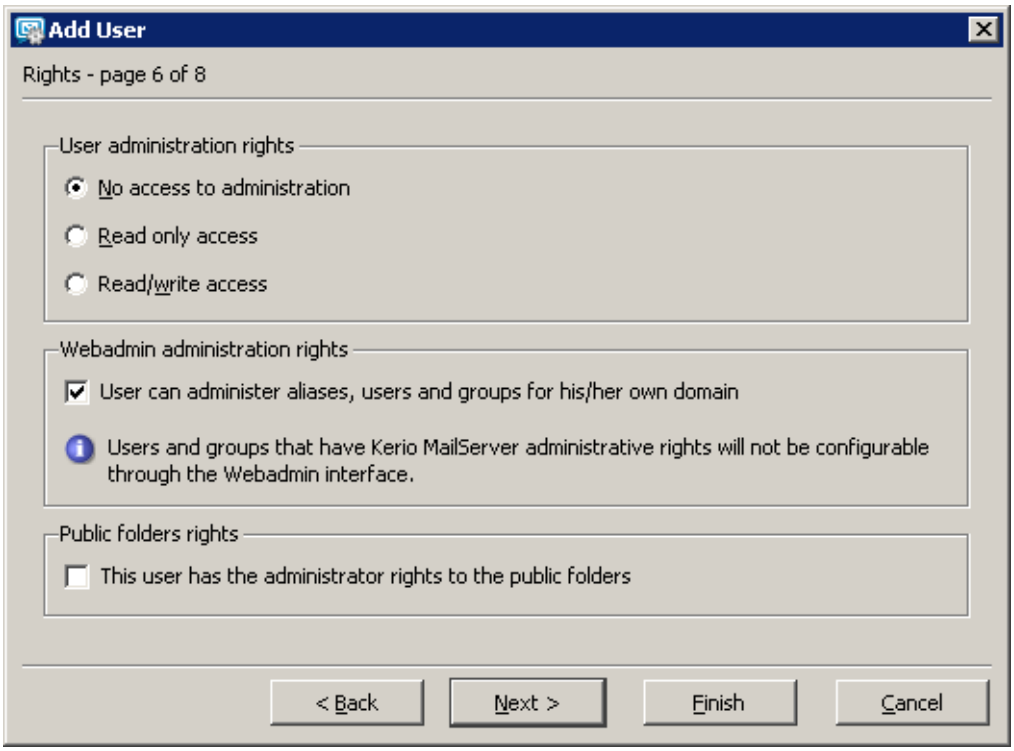

Figure 13.8 Creating a user — user rights

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 for *KMS Web Administration* (for more information, see chapter 31). 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 7.1).

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*.

All types of public services (email, calendars, contacts, tasks, notes) in *Kerio MailServer* can be viewed only in *MS Outlook* extended by the *Kerio Outlook Connector* and in *Kerio WebMail*. Other email clients usually display only email folders (for detailed information about all supported email clients, see *Kerio MailServer, User's Guide*).

Step 7 — Quota

You can set limits for each user's mailbox.

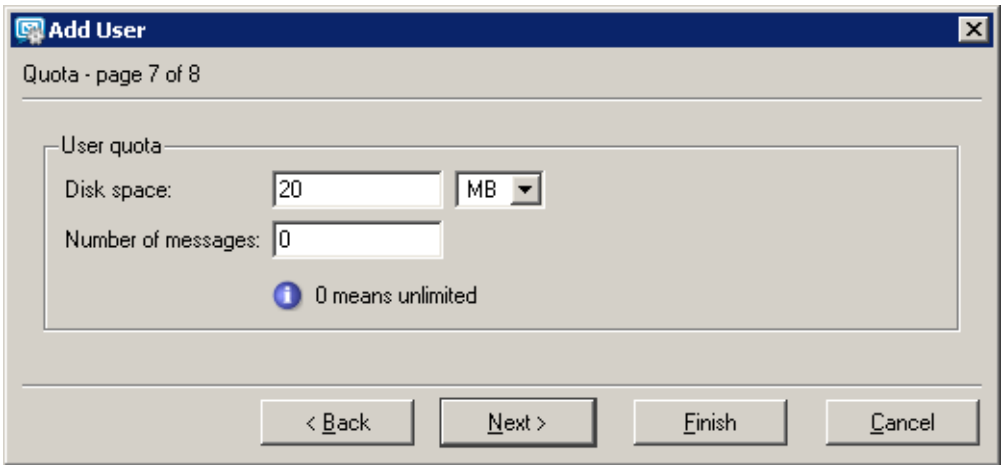

Figure 13.9 New user addition — quota

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 disk 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 treshold 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 disk space reserved). When this treshold is reached, an informative message is send 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

   If the file is being edited on *Mac OS X* or *Linux* operating systems, login to the system as the root user (a special user with full access rights to the system).

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 treshold and then exceeds it again, the next informative message will be sent after 24 hours from the first informatory message.

Note: When solving any problems regarding quota settings arise, information obtained in the *Debug* log might help. The *Debug* log can be found in the *Logs* → *Debug* section

of the administration console. To log information on the quota's behaviour, enable the *Quota and Login Statistics* option (see chapter 22.8 for details).

Step 8 — Advanced settings

This user can send/receive ...

Using this option, the administrator of *Kerio MailServer* can limit communication of the user to traffic on the local domain level. This feature may help solve issues of internal traffic in companies. By checking this domain, a particular user will not be allowed to send and/or receive messages from external domains.

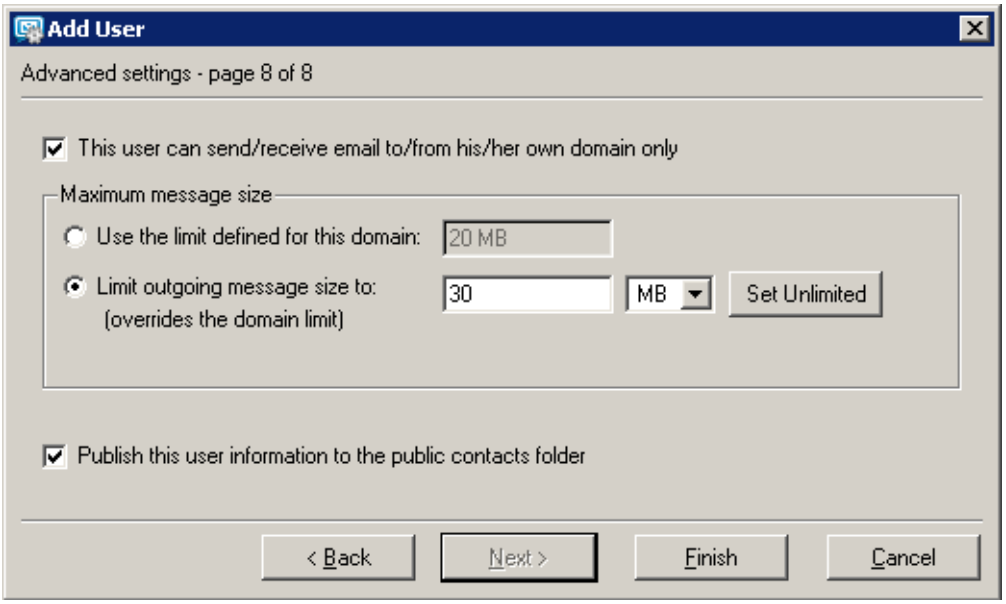

Figure 13.10 New user addition — publish user information to the public contacts folder

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 7.1). 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.

13.3 Editing User Account

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

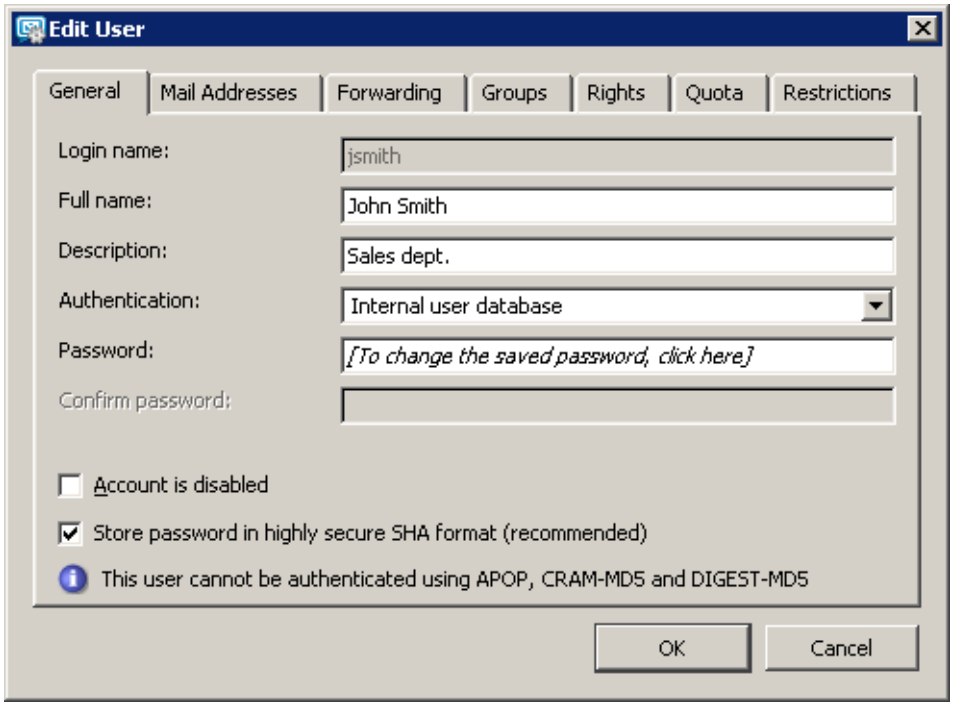

Figure 13.11 Editing User Account

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).

Figure 13.12 Quota is not defined

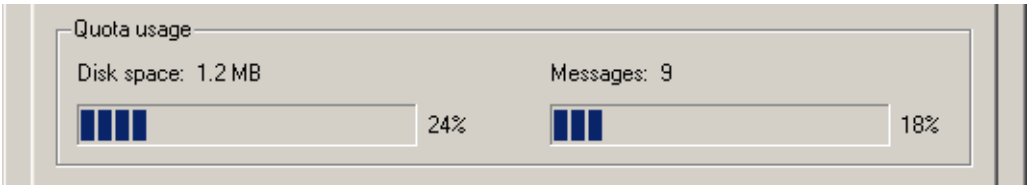

Figure 13.13 Quota is defined

13.4 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.

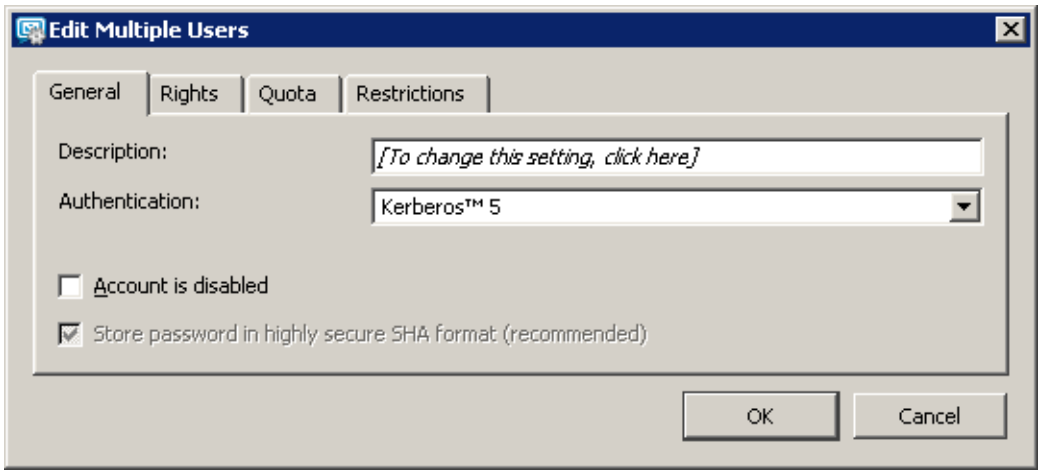

Figure 13.14 Mass change of user accounts

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.

13.5 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.

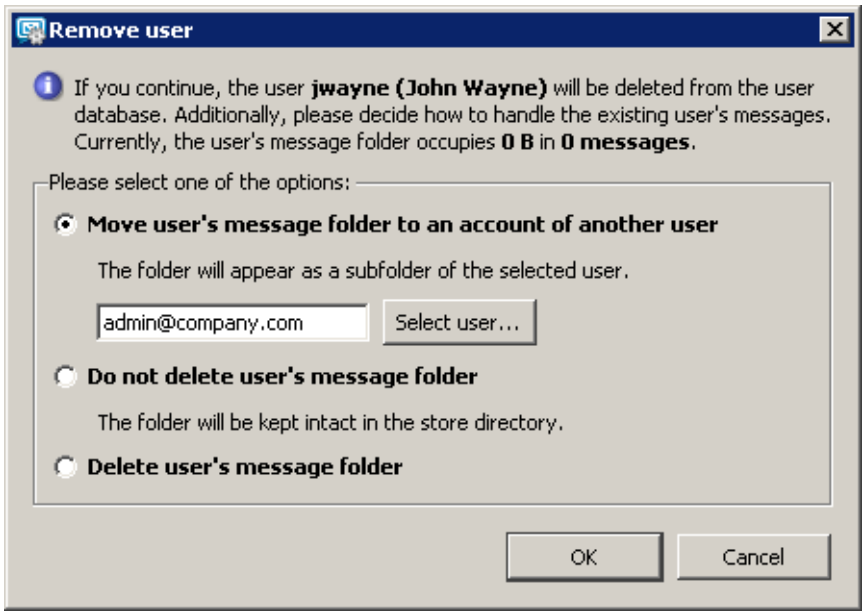

Figure 13.15 Removing a user account

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 22.5).

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.

13.6 Search

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.

13.7 Restoring deleted items

This button is shown only if the correspondent option is enabled in the first tab of the domain settings (see chapter 7.2) 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 18.2), you can use the archiving option; however, it is not designed for this purpose by default.

13.8 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 *Status* → *User 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).

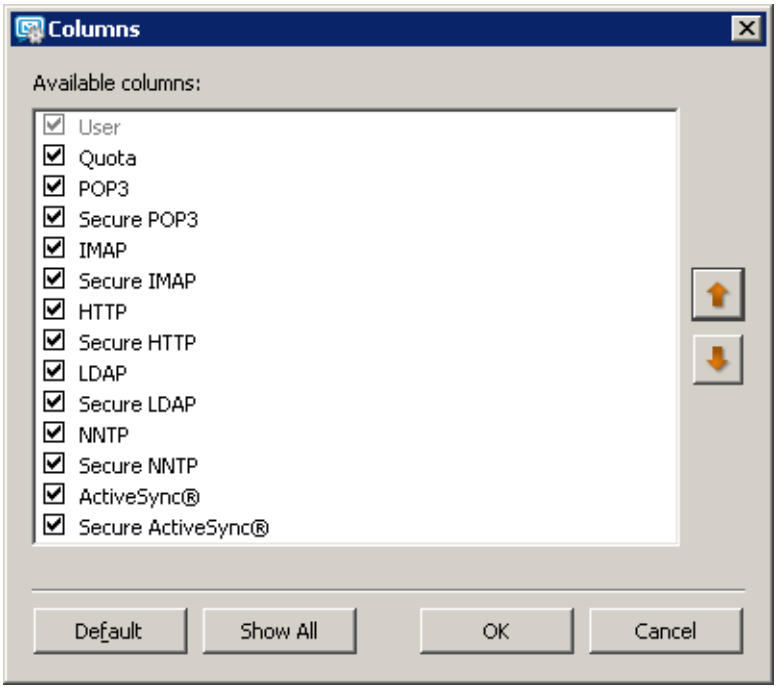

Figure 13.16 Column selection in statistics

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.

Note: If you use *MS Excel* to display and work with statistics, problems with text separator might arise. In CSV formats, commas are usually used as text separators. However, in some localizations *MS Outlook*requires the semi-colon to be used for this purpose (e.g. the Czech localization of *MS Office*). To prevent yourself from collisions which would cause incorrect printing of the statistics in the table, do the following:

1. Select data for the statistics and click on *Export* → *Export to CSV*.
2. In the standard saving dialog box, enter a name for the file and select a directory to save it in.
3. Open *MS Excel*.
4. In the *Data* menu, click on *Import external data* → *Import data*.
5. The *Select data source* dialog box is opened where you can look up the statistics file.

6. This opens the *Text import wizard*. Switch to the *Delimited* mode (otherwise, individual items of the statistics will not be displayed in columns).

7. Click on *Next*.

8. In the next dialog, select comma as a delimiter.

9. Click on *Finish*.

13.9 Administration of mobile devices

Users can connect to *Kerio MailServer* from various mobile devices (PDAs or so called "smart" phones). Connections between mobile devices and *Kerio MailServer* are allowed by support of the *ActiveSync* protocol (for detailed information on this protocol and its usage, refer to chapter 36).

The administration console includes tools for administration of mobile devices that can be used by the *Kerio MailServer* administrator to overview devices currently used by individual users.

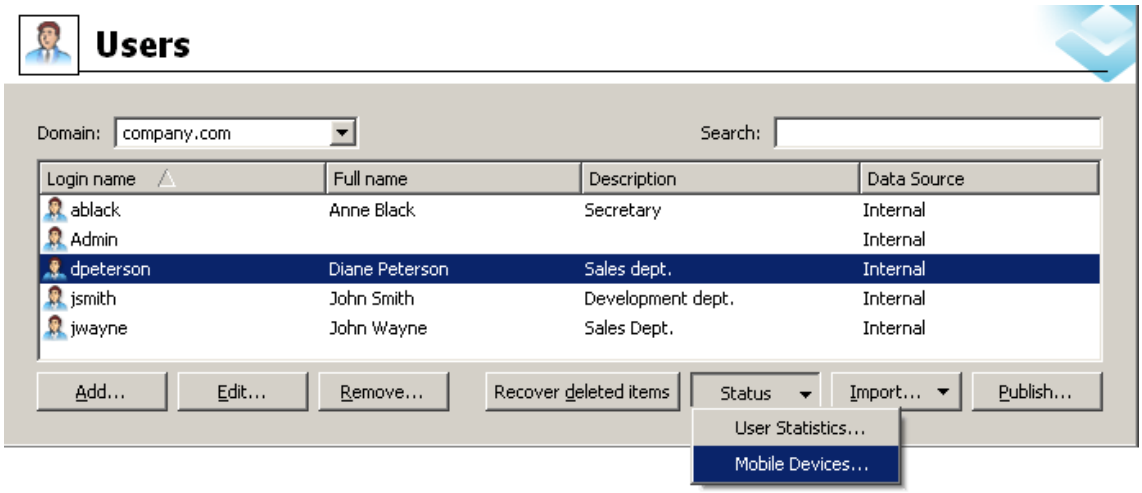

Figure 13.17 User's pop-up menu — Mobile Devices

The mobile device administration tools can be found in *Domain Settings* → *User Accounts*. In this section, simply select a user who uses a mobile device to connect to the server. Click on *Status* and select the *Mobile Devices* option in the menu (see figure 13.17). The *Mobile Devices* window just opened overviews all devices used by the particular user for connection to the server (see figure 13.18). Several buttons are available below the device list:

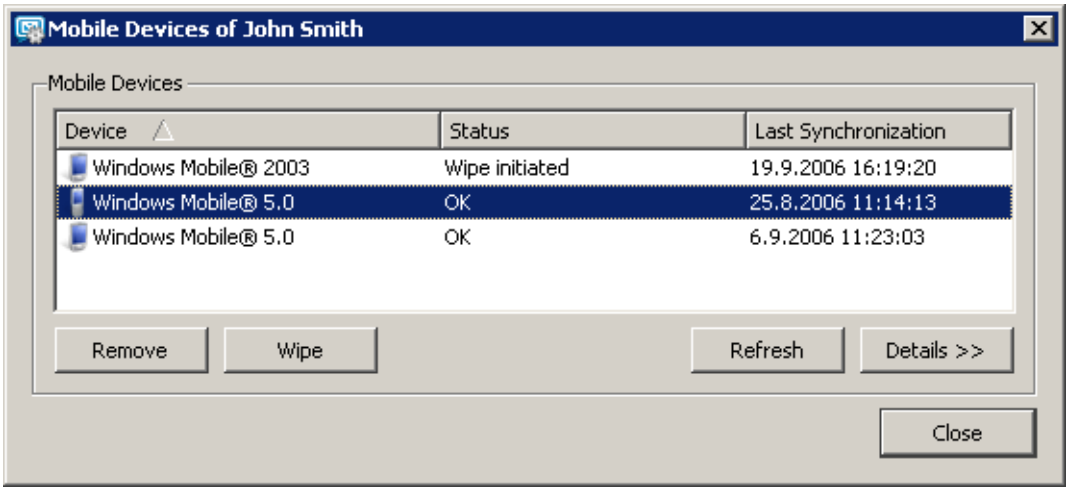

Figure 13.18 Mobile devices

- *Remove* — removes selected devices from the list. This option is helpful especially when a device is not used (for details on this option, see chapter 36.6).
- *Wipe* — this option allows remote removal of user data from the selected device (see chapter 36.5).
- *Refresh* — the button refreshes information on status of connected devices.
- *Details* — use this button to view details on a selected device. Click the button to display another section including details on the device connected as well as on synchronization. The section consists of two parts (see figure 13.19). The first part, providing information about the device connected and about the synchronization, is called *Details*:

  Operating system and OS type
  The first line includes an icon of the device reflecting its real appearance. Type of the operating system installed on the device is provided next to the icon, as well as information about the device type (PDA or Smartphone).

  Protocol version
  ActiveSync version.

  Device ID
  Serial number of the device.

  Device Registered
  The date when the user specified server info in *ActiveSync* and established the first connection.

  Last Synchronization
  Date and time of the last synchronization.

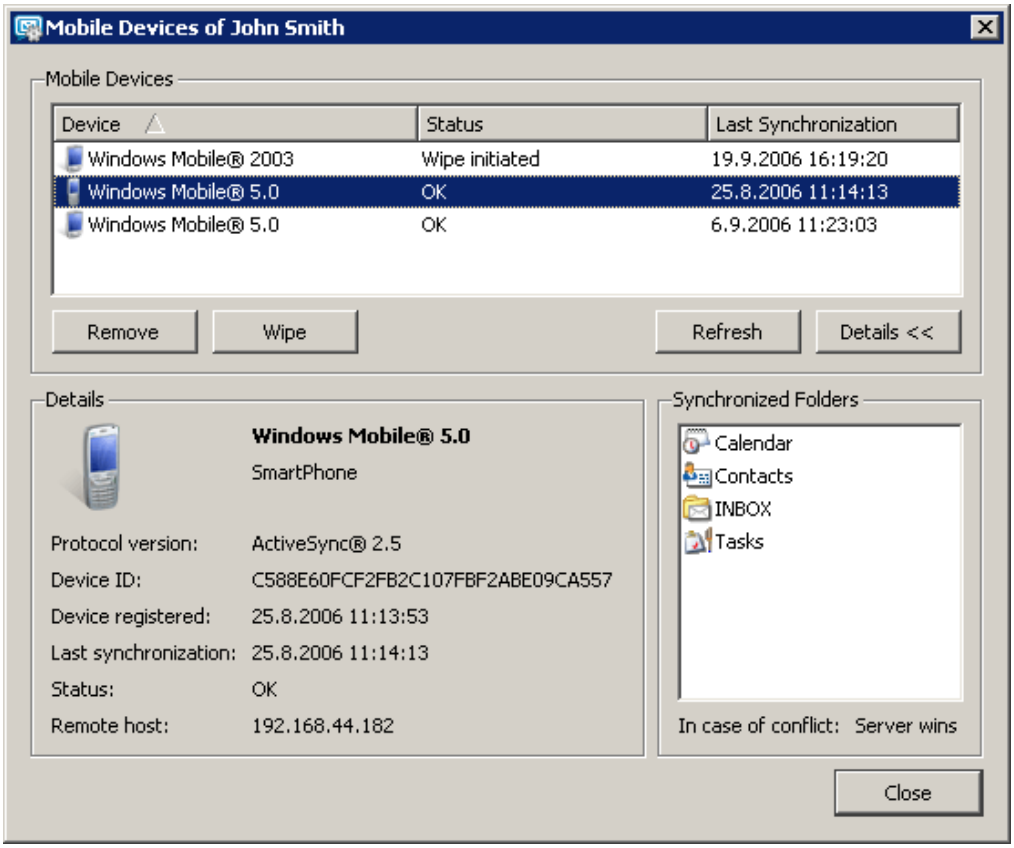

Figure 13.19 A mobile device — details

Status

Synchronization status. This item provides synchronization status information, i.e. whether the process was completed successfully, if any problems arose, etc.

Remote Host

IP address assigned to the device's network adapter.

The *Synchronized Folders* section lists all synchronized folders. Older device types usually support only synchronization of email, calendars and contacts, whereas newer devices support also synchronization of tasks.

Below the pane where folders are overviewed, an information addressing solution of synchronization collisions is provided. A collision is detected if the same data items are changed both on the server and on the device.

- *Server wins* — if there is a collision, data saved on the server overwrite the data stored in the device.
- *Client wins* — if there is a collision, data saved on the device overwrite the data stored on the server.

13.10 Import Users

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

- from CSV files
- NT domains
- Active Directory
- Novell eDirectory

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 7.6). 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).
- It is recommended to enable the *Directory Service Lookup* option in the *Debug* log (for more information, see chapter 22.8) before starting the import process. Logged information about the import process might help you where troubleshooting is necessary.

The *Import* button located below the user list is also a menu. This menu includes options of import from a directory service (NT domain, Active Directory, Novell eDirectory) or import from a CSV file. Select an option to open the user import dialog:

Import from a file

There is an option to import user accounts from CSV files. Data in the file must follow certain rules. Headlines of individual columns must correspond with *Kerio MailServer's* items. The following items are supported:

- Name — username (e.g. `jwayne`). Required.
- Password — user password. Optional.
- FullName — user's full name (e.g. `John Wayne`). Optional.
- MailAddress — user's email address. Only the part preceding the at-sign should be inserted. Any number of email addresses is accepted (e.g. `jwayne`, `wayne`, `john`, `john.wayne`). Optional.
- Groups — groups where the user is subscribed. Multiple groups are allowed. Optional.
- Description — user's description. Optional.

Columns can be ordered as wish, there are no rules to be followed. It is also possible to leave some of them out (except the Name item).

When creating a file to be imported, bear in mind it is important that individual data items are separated by commas (`,`) or semicolons (`;`). If semicolons are used, the process is simpler. Create a table where standard item names (see above) are in caption and add corresponding data. Multiple items can be included in `MailAddress` and `Groups`. Individual email addresses and/or groups must be separated by commas (see table 13.2).

Name	Password	FullName	Description	MailAddress	Groups
jwayne	VbD66op1	John Wayne	Developer	jwayne	read-only,all
jsmith	Ahdpppu4	Joseph Smith	Sales	jsmith,smith	sales, all
amonroe	SpoiuS158	Ada Monroe	GM's Assistant	amonroe,ada.monroe	all
psycho	pfgzInI1	Peter Sycho	General Manager	psycho,sycho	all,sales

Table 13.2 Imported data — items separated by semicolons

If commas are used as separators, additional separators must be used for `MailAddress` and `Groups` items since commas used there as separators might collide with the other comma separators. Quotes (`"..."`) or apostrophes (`'...'`) can be used as separators. In table 13.3, quotes are used.

Name	Password	FullName	Description	MailAddress	Groups
jwayne	VbD66op1	John Wayne	Developer	jwayne	"read, all"
jsmith	Ahdpppu4	Joseph Smith	Sales	"jsmith,smith"	"sales, all"
amonroe	SpoiuS158	Ada Monroe	GM's Assistant	"amonroe,ada.monroe"	"all"
psycho	pfgzInI1	Peter Sycho	General Manager	"psycho,sycho"	"all,sales"

Table 13.3 Imported data — items separated by commas

Once a CSV file is created, follow these instructions:

1. Run the *Kerio Administration Console*.

2. In *Domain Settings* → *User Accounts*, click on *Import* and select the *Import from CSV file* option.

3. This opens a dialog (see figure 13.20) where file path and encoding type which will be used for saving (generally, the default *Local (System)* option can be kept) can be set.

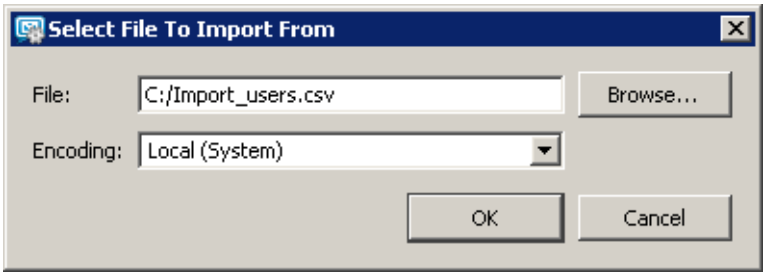

Figure 13.20 Import from a file — file selection

4. Click on *OK* and wait until the file is uploaded. The *User import* dialog is opened providing a list of all users defined in the CSV file (see figure 13.21).

   If problems occur regarding the upload, it might be caused by the following reasons:

   - The file is not saved in the CSV format.
   - Columns in the file are not labeled correctly. CSV file needs to include a line with captions including column names, otherwise *Kerio MailServer* cannot read the data.
     Correct version:
     ```
     Name;Password;FullName;MailAddress
     silly;VbD66op1;Stephen Illy;silly
     ewood;Ahdpppu4; Edward Wood;ewood,wood
     ```
     Wrong version:
     ```
     silly;VbD66op1;Stephen Illy;silly
     ewood;Ahdpppu4; Edward Wood;ewood,wood
     ```
   - Separators are not used properly. Proper way of how to use separators is described above.

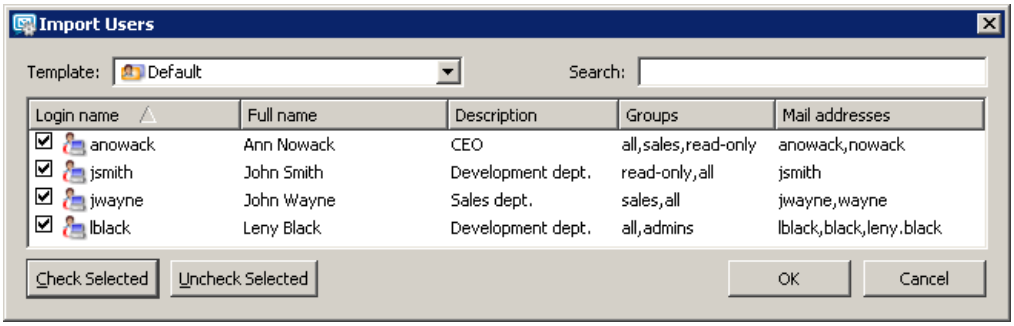

Figure 13.21 Import from a file — imported users

5. Check all users to be imported. Where many users are imported, the *Check selected* and *Uncheck selected* buttons might be helpful.
   - *Check selected* — all users marked by the mouse pointer (using the `Shift` and `Ctrl` keys) will be checked.
   - *Uncheck selected* — clears selection.
6. Templates for email accounts can be selected and set in the *Template* menu. If there is no template to be set, keep the default settings.

   For detailed information on templates and their application, see section 13.12.
7. Confirm selection by clicking on *OK*.

NT Domain

Use the *Import users from* option to select a source from which users will be imported. *Windows NT domain (Windows NT 4.0)* is used in this case.

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.

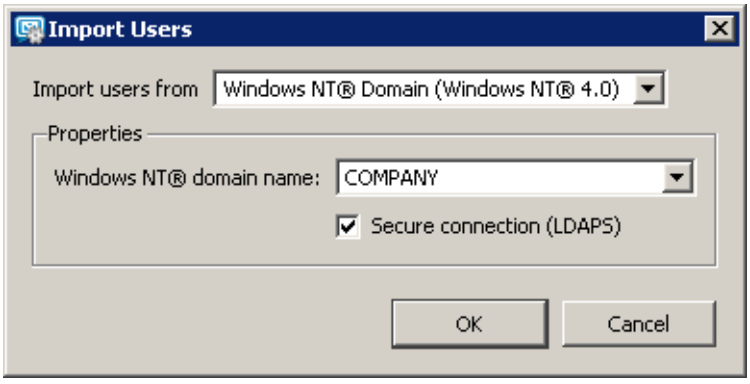

Figure 13.22 Import users from NT Domain

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

Use the *Import users from* option to select a source from which users will be imported. *Active Directory (Windows 2000/2003)* is used in this case.

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* — this item is available upon clicking on *Advanced*. This option allows to modify the request for LDAP server users will be imported from. 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.

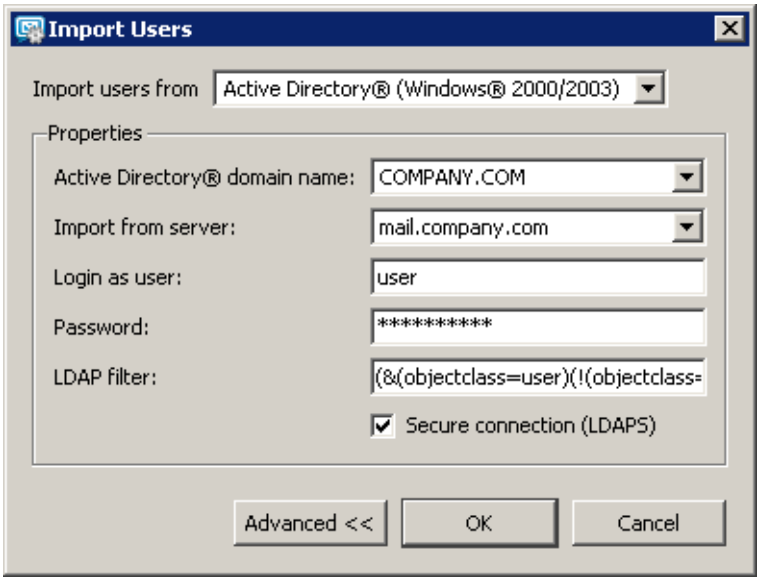

Figure 13.23 Import users from Active Directory

Novell eDirectory

Use the *Import users from* option to select a source from which users will be imported. *Novell eDirectory*is used in this case.

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

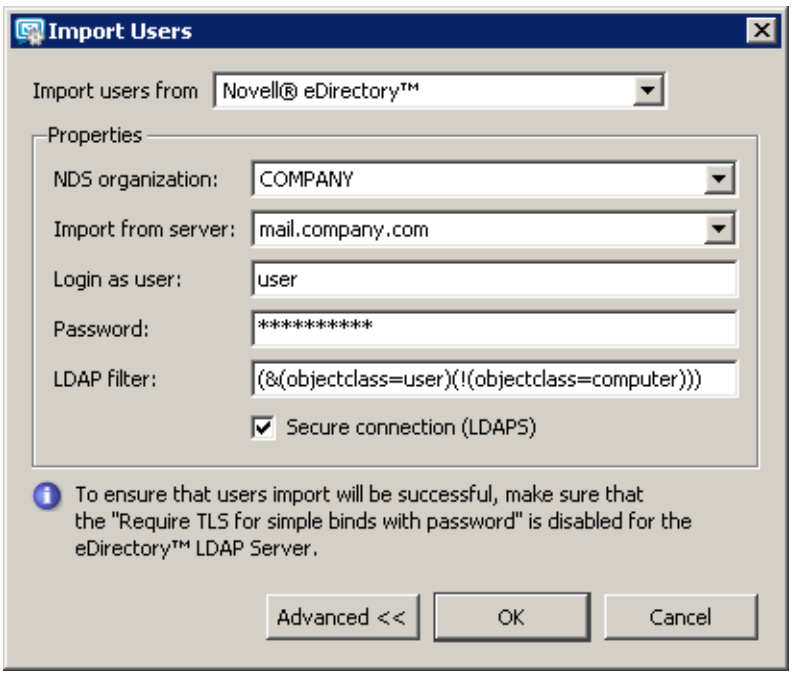

Figure 13.24 Import users from Novell eDirectory

- *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.
- *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* — this item is available upon clicking on *Advanced*. This option allows to modify the request for LDAP server users will be imported from. 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

Once all conditions are met (valid login data has been entered, the server is available, etc.), click *OK* to view user list (see figure 13.25):

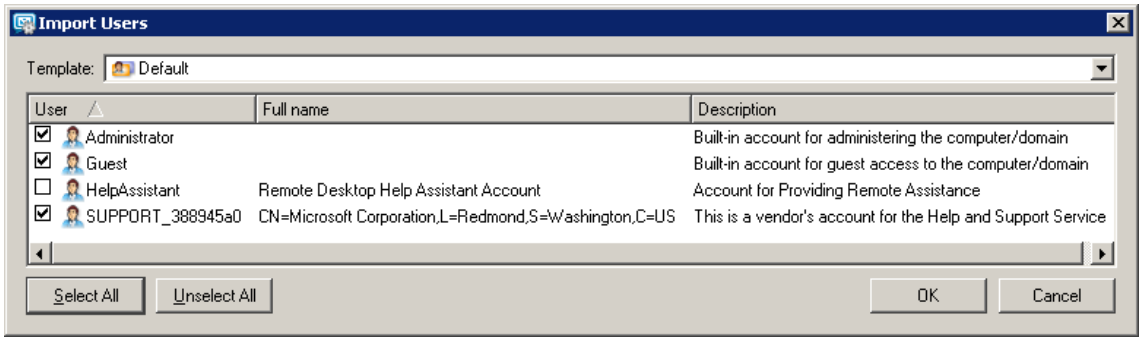

Figure 13.25 Users selection for import

1. Check users to be imported into *Kerio MailServer*.

2. Templates for email accounts can be selected and set in the *Template* menu. If there is no template to be set, keep the default settings.

   For detailed information on templates and their application, see section 13.12.

3. Click on *OK*.

Notes:

- If the users are imported from *Active Directory*, the platform on which *Kerio MailServer* is running is not important.
- Authentication type will be set for the users in accordance with where they were imported from: *Windows NT Domain* for the NT Domain users and *Kerberos 5* for the *Active Directory* users.

13.11 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.

In the dialog opened, select a folder where user information will be published. The dialog provides a list of users selected fr the export (see figure 13.26).

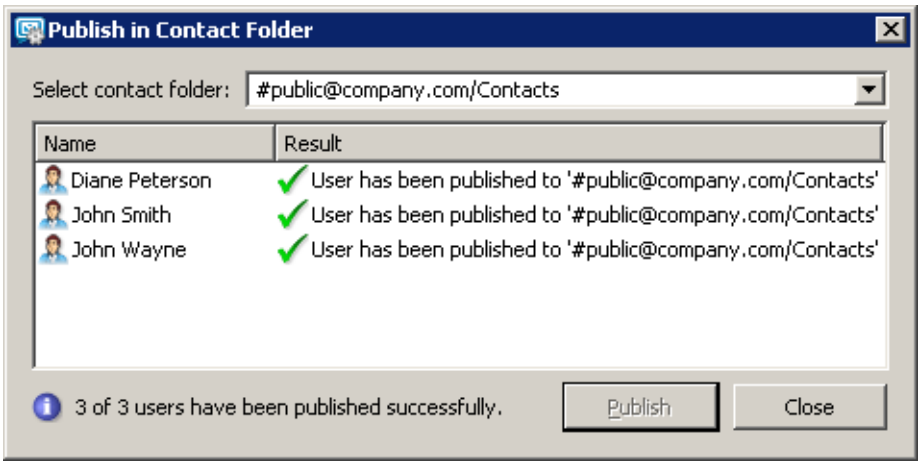

Figure 13.26 Export to Address Book

If there is no public address book defined, the `#public@domena/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 13.11). Rights for public folders are not required.

When the publishing process is completed, its results are provided (see figure 13.26).

13.12 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.

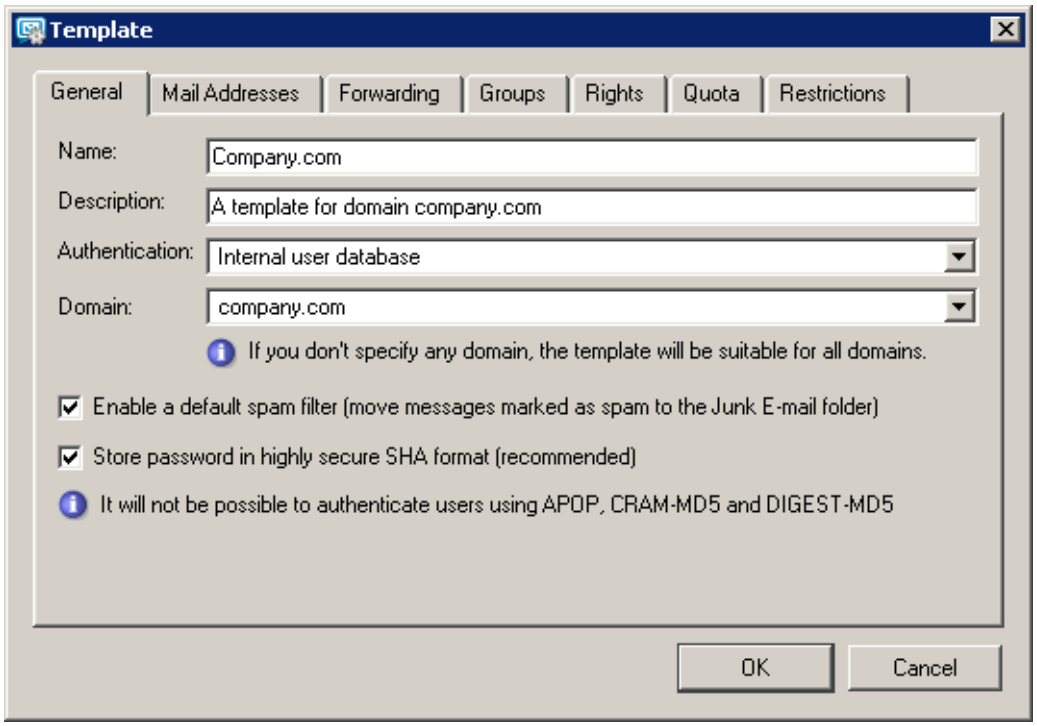

Figure 13.27 Defining a template

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 13).

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 13.2.

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 13.2.

Chapter 14

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 15.3) — 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.

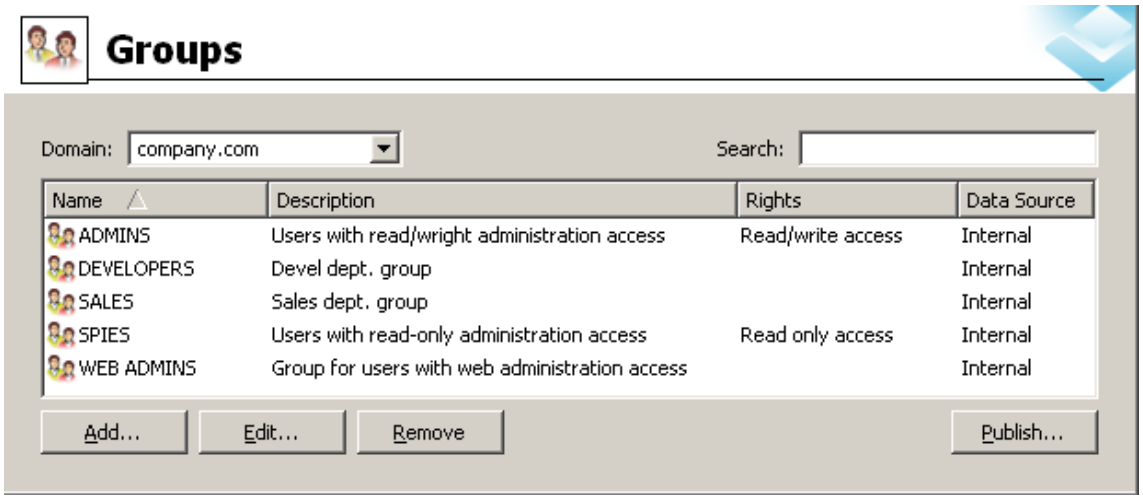

Figure 14.1 User groups

The *Search* field and the *Publish* button have the same function as described in section *Users*. For detailed description of these items, see chapter 13.

14.1 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.

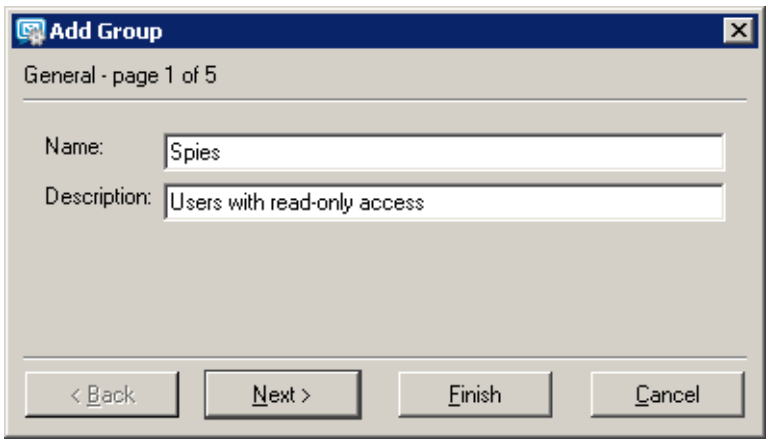

Figure 14.2 Creating a group — basic data

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 7.6), their aliases can be defined in *Active Directory Users and Computers*. Global aliases (in *Domain Settings* → *Aliases*) cannot be defined this way.

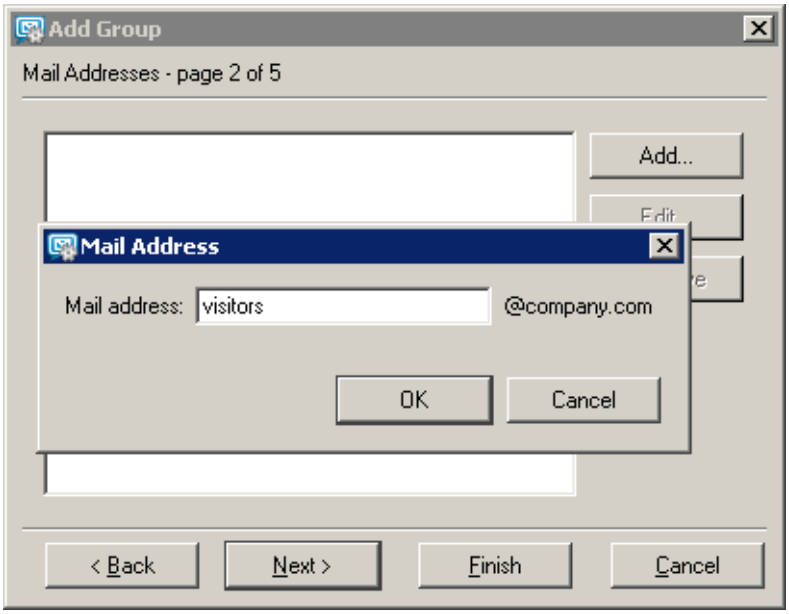

Figure 14.3 Creating a group — e-mail address

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 13.2).

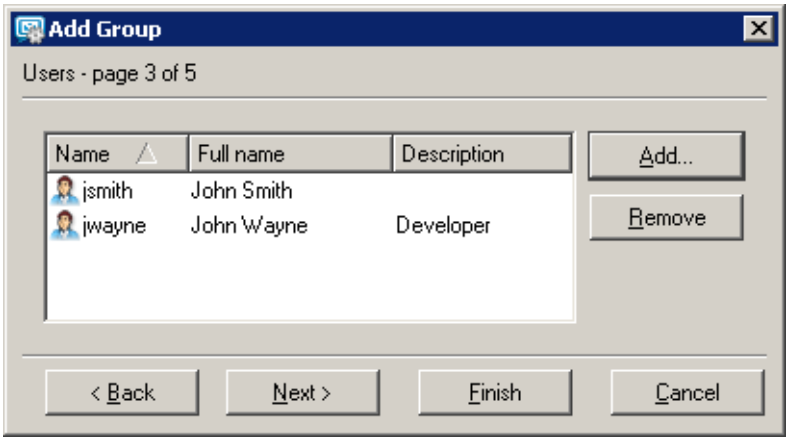

Figure 14.4 Creating a group — users addition

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.

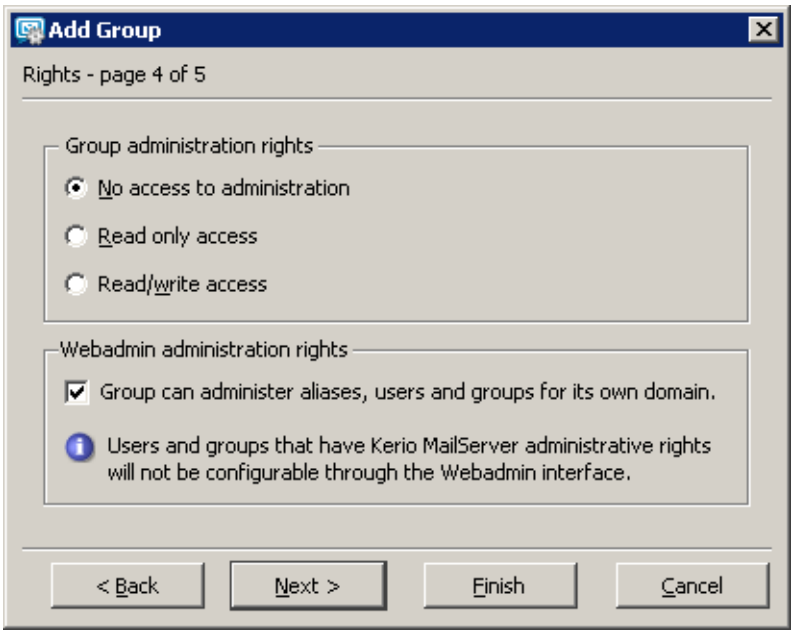

Figure 14.5 Creating a group — user rights

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 user accounts, ...
: A special access right for *Kerio Web Administration* (for more information, see chapter 31). 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 ...

This option allows the *Kerio MailServer* administrator to narrow traffic of this group's members to the local domain level. This feature may help solve issues of internal traffic in companies. If this option is enabled, no user of the particular group will be allowed to send or receive messages from external domains.

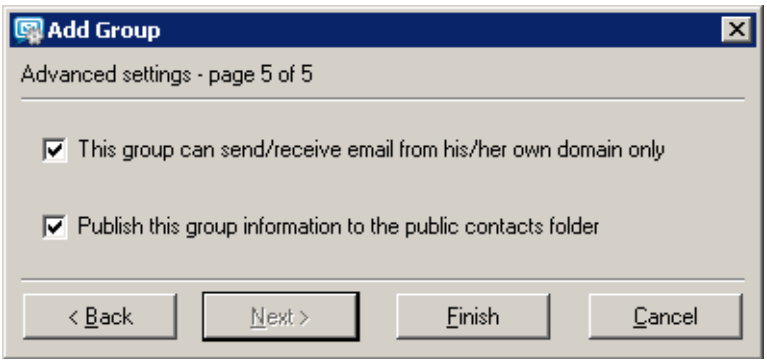

Figure 14.6 Creating a group — publish information to the public contacts folder

Publish this group information to the ...

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

Chapter 15

Sending and Receiving Mail

15.1 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. J

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:

```
company.com              MX      10      mail.company.com
                         MX      20      smtp.provider.com
mail.company.com         A               215.75.128.33
smtp.provider.com        A               215.75.128.1
```

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. 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 27.5).

   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 15.4), 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.

Access of email clients to user accounts

User can use various methods to access their email accounts:

POP3

POP3 (Post Office Protocol version 3) is an Internet protocol used for downloading of email from a server to another server (see the *Domain Mailbox* section) or to an email client. POP3 protocol is defined in RFC 1939.

POP3 protocol works on client-to-server basis. Connection is always established by the client, then requests and responses of the client and of the server take regular turns until the connection is closed. As soon as the client initializes the connection and is successfully authenticated by name and password, it is possible to work with the email (download it to the client, delete it, etc.).

Under usual circumstances, *Kerio MailServer* works as a server. If, however, it downloads email from remote POP3 accounts, it can also work as a client.

POP3 protocol is quite obsolete. The protocol can download email to a client application and can work with merely one folder (INBOX). This means that any message moved to another folder would disappear since moved out of the only folder available. And the other way round. If a user can access multiple folders and moves a message from Inbox to another one, the message cannot be uploaded to the client application. Therefore, it is generally recommended to use IMAP, a more modern protocol. Advantages of the IMAP protocol can be seen in the comparative table 15.1.

The only advantage of this protocol might be low demands on server's disk space. Users download their email to their local disks and there it is possible to sort messages in folders, remove items, etc. Therefore, POP3 accounts are used especially for freemail services where users have mailboxes with capacity of a few megabytes and download their email to their local disks regularly. Another advantage is the good availability of offline transactions which can be used if connection to the Internet is time-limited. Nowadays, however, most of email clients work well in their offline modes both with POP3 and with IMAP accounts.

IMAP

IMAP (Internet Mail Access Protocol) is an Internet protocol used for connections to email servers, as well as for reading of messages and for other email transactions. IMAP protocol is defined in RFC 3501.

In addition to downloading email to users' local hosts, IMAP protocol enables administration of email account on the server. It is, therefore, possible to access email accounts from various client stations. Unlike POP3, IMAP protocol allows keeping email on the server and handling it there (reading, removing, sorting to folders). It is also possible to keep the email stored in the email client. This solution is helpful especially if users have a time-limited Internet connection or can be connected to the server only temporarily or irregularly and need to work with their email offline. Once reconnected to the network, folders on the server and on the client are synchronized.

Another difference is that in case of IMAP protocol, email can be handled while items are downloaded to the local store. In case of IMAP protocol, email headers are downloaded first and user can select any of them to be opened as the first. When the message is selected, it will be considered as a high-priority item and it can be read, moved to another folder or otherwise manipulated while the other email is being downloaded.

POP3	IMAP
both secured and unencrypted (POP3S)	both secured and unencrypted (IMAPS)
enables authorization	enables authorization
works with a single folder only	allows manipulations with folders (e.g. moving messages between folders), all folders are created and stored on the server
downloads entire messages (messages are displayed one by one as downloaded from the server)	downloads email headers first, message bodies later
synchronous (it is not possible to handle email while it is being downloaded, one must wait until the email is available on the local disk)	asynchronous (individual messages can be handled while email is being downloaded)
only one client can be connected to the account	multiple clients can be connected to the account

Table 15.1 POP3 and IMAP comparison

Access via the MAPI interface (MS Outlook)

Kerio MailServer enables access to email via the MAPI interface. MAPI (Messaging Application Programming Interface) is a versatile interface for email transmission, developed by Microsoft. It is a software interface that enables any MAPI client to communicate with any mailserver (*MS Outlook* and *Kerio MailServer* in this case).

To enable traffic via the MAPI interface, *Kerio Technologies* developed *Kerio Outlook Connector*, a special application which is installed on a client and work as an *MS Outlook* extension. *MS Outlook* extended by *Kerio Outlook Connector* handles email in the same manner as the IMAP protocol, and it even allows additional options.

Thanks to this modification, *MS Outlook* is able to work with groupware data (contacts, calendar, tasks, notices) 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), *MS Outlook* with the *Kerio Outlook Connector*.

MS Outlook with the *Kerio Outlook Connector* also enables better scheduling of meetings and tasks (the *Free/Busy* calendar) as well as sharing of various types of data (shared and public folders).

For more information on *Kerio Outlook Connector*, see chapter 32.2.

Access via the WebDAV interface (MS Entourage)

Kerio MailServer supports the WebDAV interface (Web Distribution Authoring and Versioning) which can also be used for accessing email accounts. Using WebDAV, users can group-edit and organize files located on servers.

Support for the WebDAV interface in *Kerio MailServer* enables connection of *MS Entourage*. *MS Entourage* is an *MS Office 2004 for Mac* email client which can use POP3, IMAP protocols and the WebDAV interface to connect to email servers.

Users who want to use *MS Entourage* to connect to *Kerio MailServer* can use a special interface originally developed for communication with *MS Exchange*. In *MS Entourage*, the interface is represented as an *Exchange* account and it is based on WebDAV traffic.

The WebDAV interface in *MS Entourage* provides similar options as the *Kerio Outlook Connector*. This implies that, in addition to email manipulation, it enables working also with groupware data (email, calendars, contacts, public folders), it supports *Free/Busy* server, etc.

In older versions, IMAP protocol was used to access email and the WebDAV interface was used for other folder types. *MS Entourage 2004*, however, uses WebDAV also to access to email folders.

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.

To learn more on *MS Entourage* and its correct settings, see chapter 38.

15.2 SMTP server

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

Protection of the SMTP server 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 16.5). Trusted servers will not be even checked by *SpamAssassin*. However, this filter can be enabled by a special option in the *Spam Filter* section on the *Spam Rating* tab if necessary (for more information, refer to chapter 16.1).

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

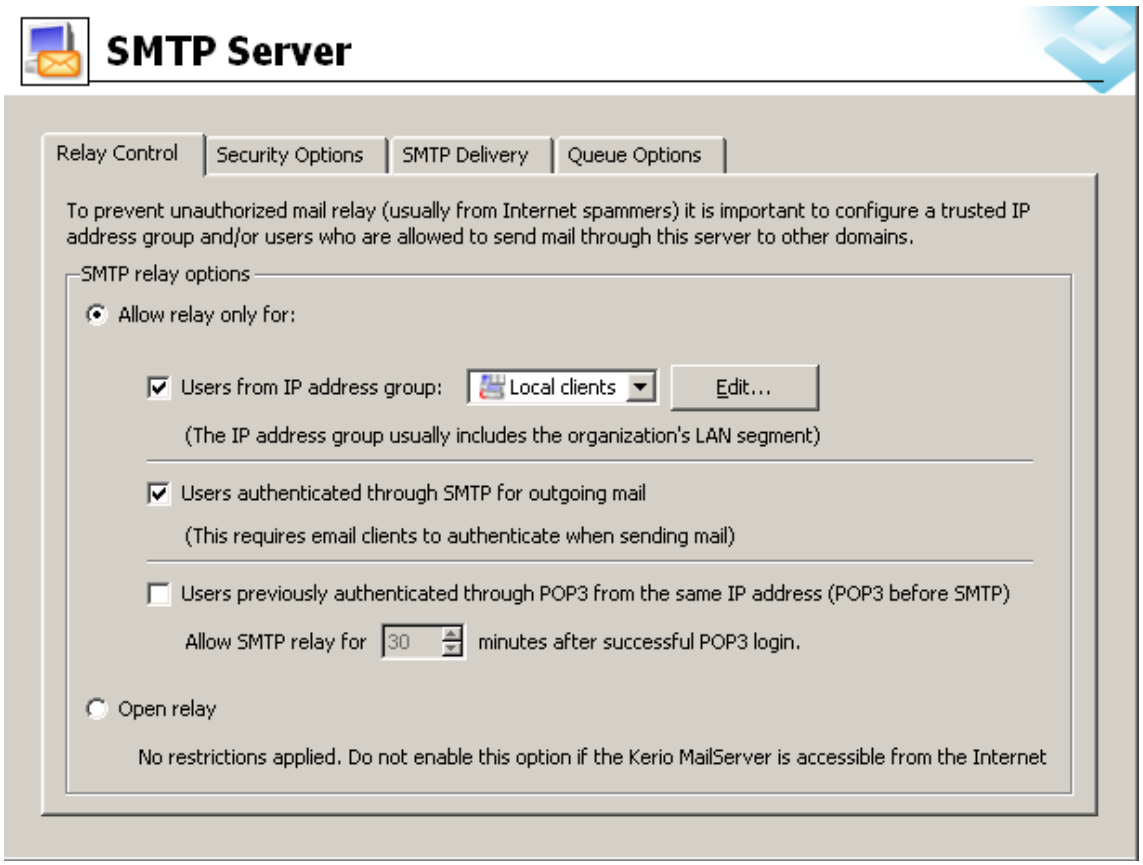

Figure 15.1 Relay Control tab

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 12.1).

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.

Figure 15.2 Security Options — IP address based limits

Max. number of messages per hour...

Maximum count of messages that can be sent from one IP address per hour. This protects the disk 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 our is discarded.

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.

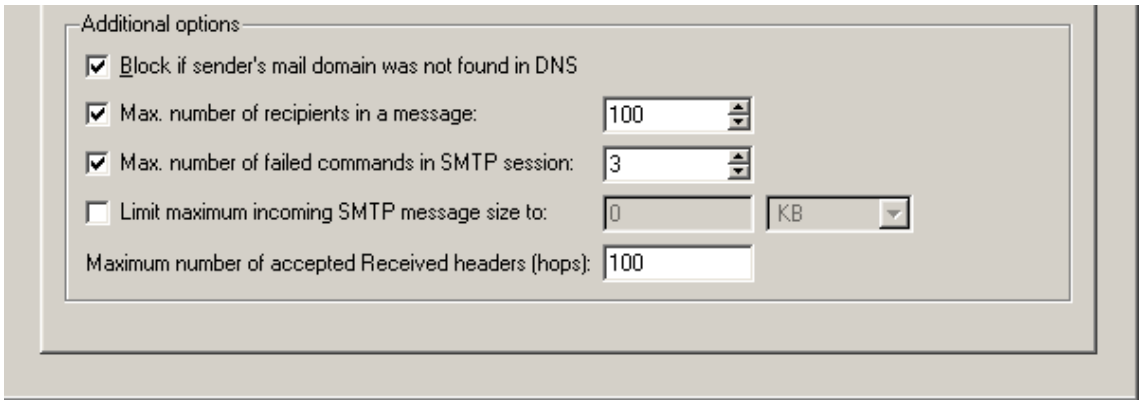

Figure 15.3 Security Options — Advanced options

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).

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:

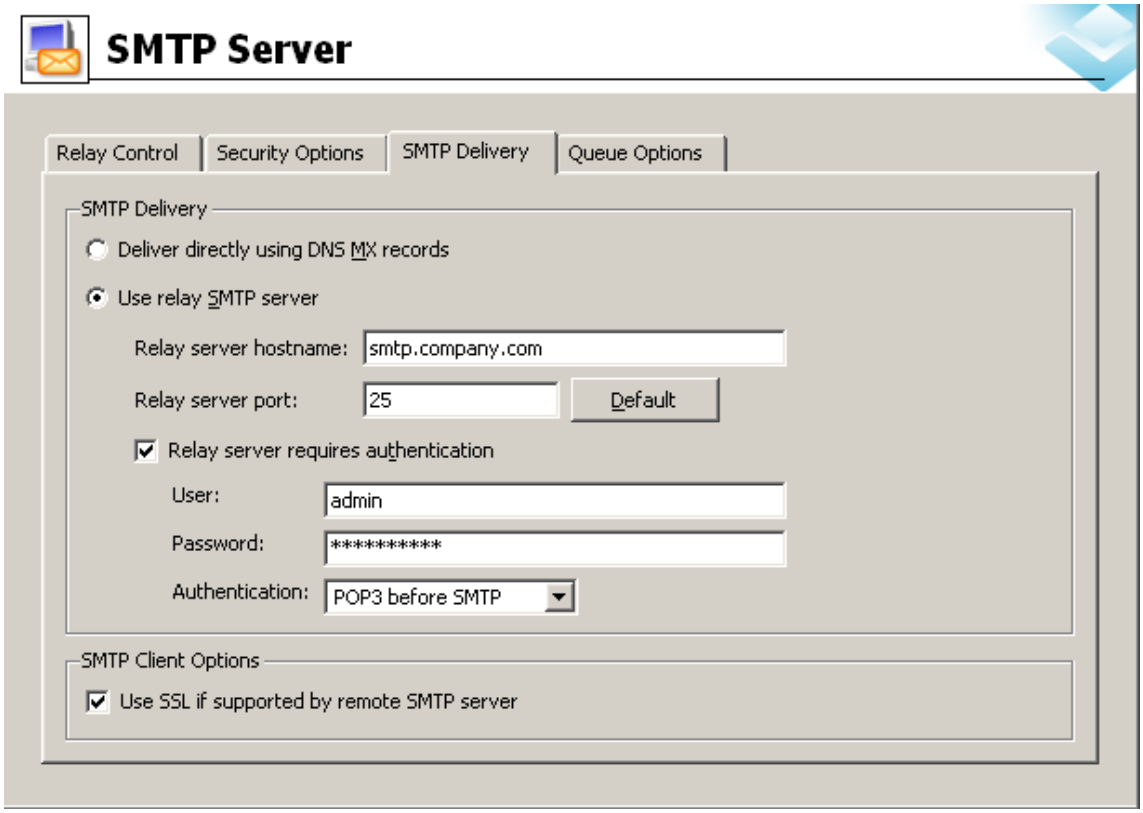

Figure 15.4 SMTP Delivery tab

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

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

SMTP server
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 messages 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*.

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.

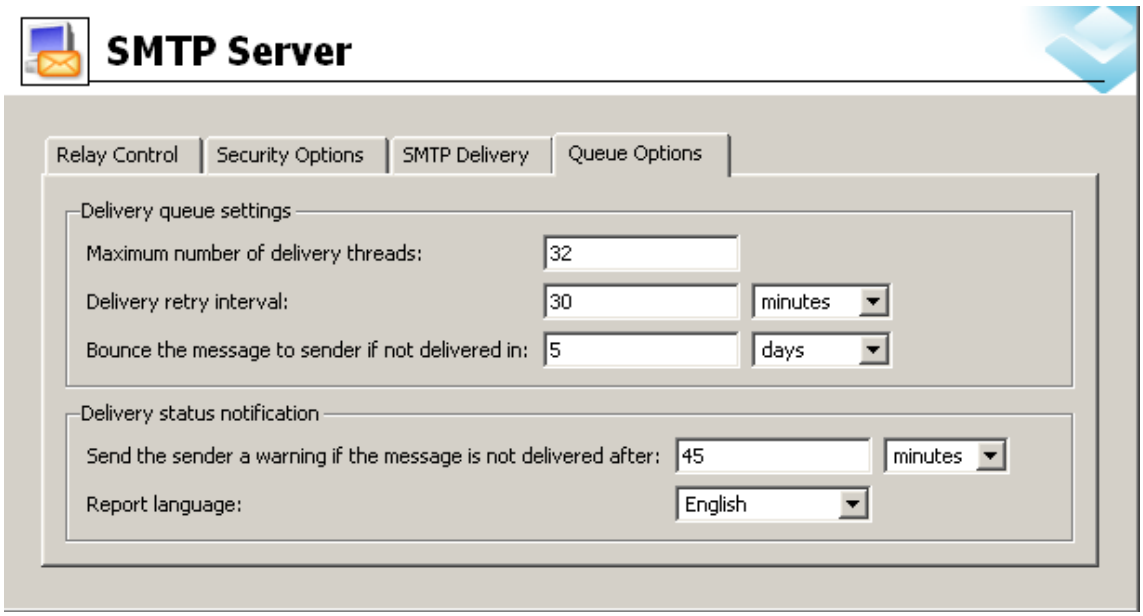

Figure 15.5 Queue Options

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.

15.3 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@company.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 `time`, `dime`, 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 13), 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 13.2), or group definition (see chapter 14.1).

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:

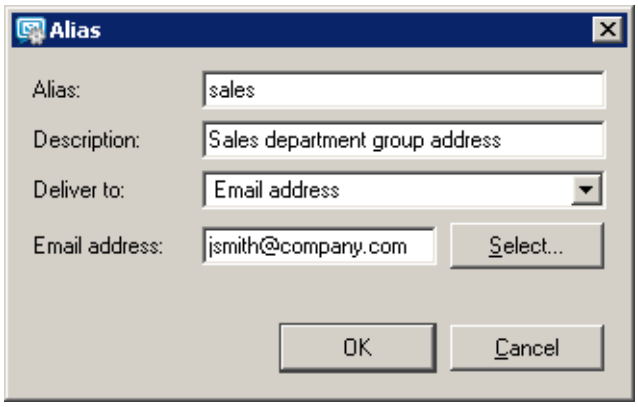

Figure 15.6 Defining Alias

Alias

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

Character type	Description
`a-z`	all lower-case letters except special characters (diacritics)
`A-Z`	all upper-case letters except special characters (diacritics)
`0-9`	all numbers
`.`	dot
`-`	dash
`_`	underscore
`?`	question mark
`*`	asterisk

Table 15.2 Symbols allowed in alias name

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).

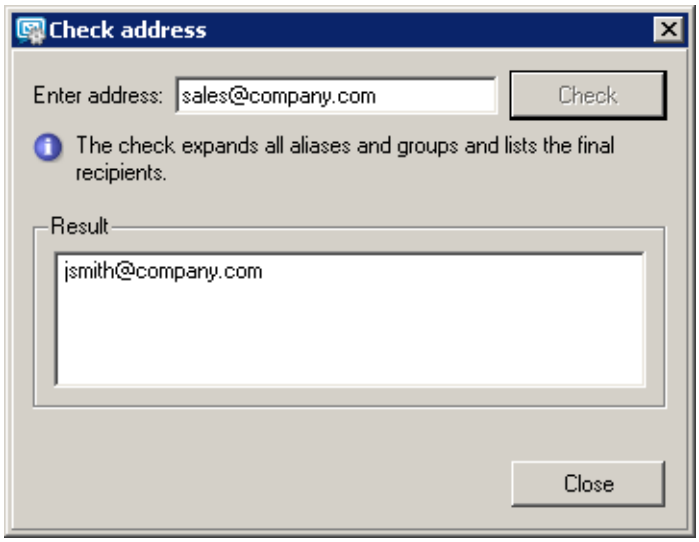

Figure 15.7 Check Address

15.4 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.

Retrieving POP3 mailboxes is controlled only by a scheduler (see chapter 9). 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.

Downloading of POP3 accounts disables antispam features which depend on reception of email by SMTP (typically DNS blacklists and check of Caller ID and SPF sender servers. Configuration and features of antispam filters are focused in chapter 16.

Defining Remote Mailboxes

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

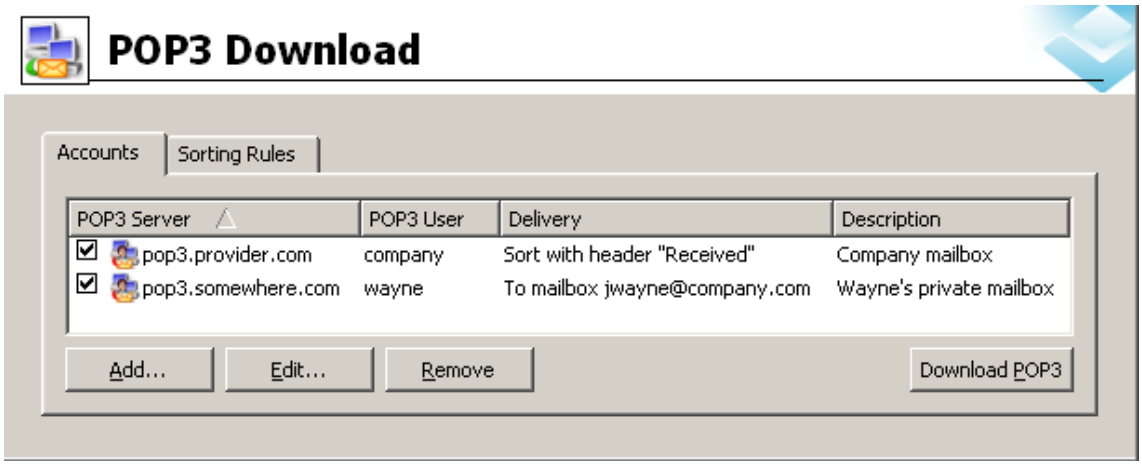

Figure 15.8 Remote POP3 download

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

Username and Password
: The username and password for the mailbox

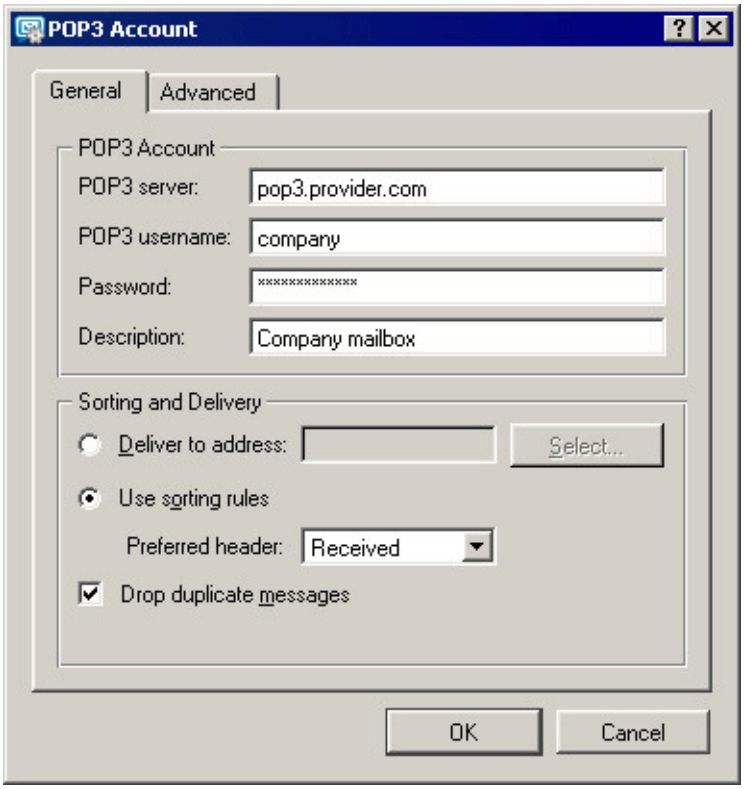

Figure 15.9 Defining Remote Mailboxes

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.

This dialog (see picture 15.10) 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

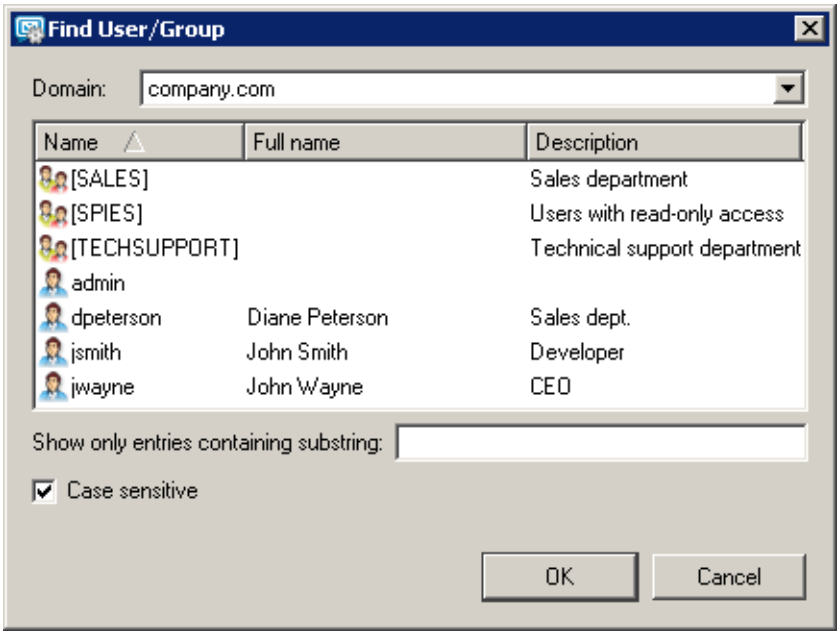

Figure 15.10 Find User/Group dialog

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:

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

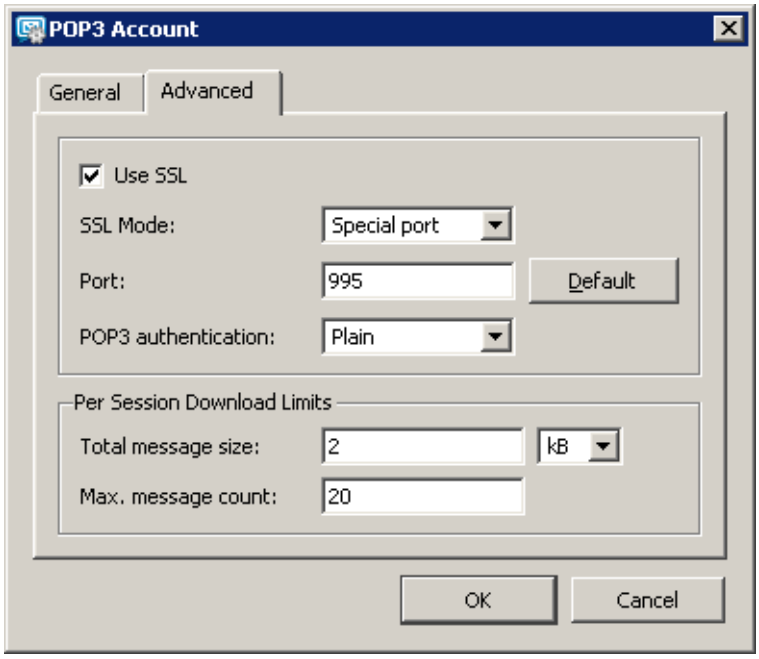

Figure 15.11 More detailed settings for downloading POP3 mailboxes

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.

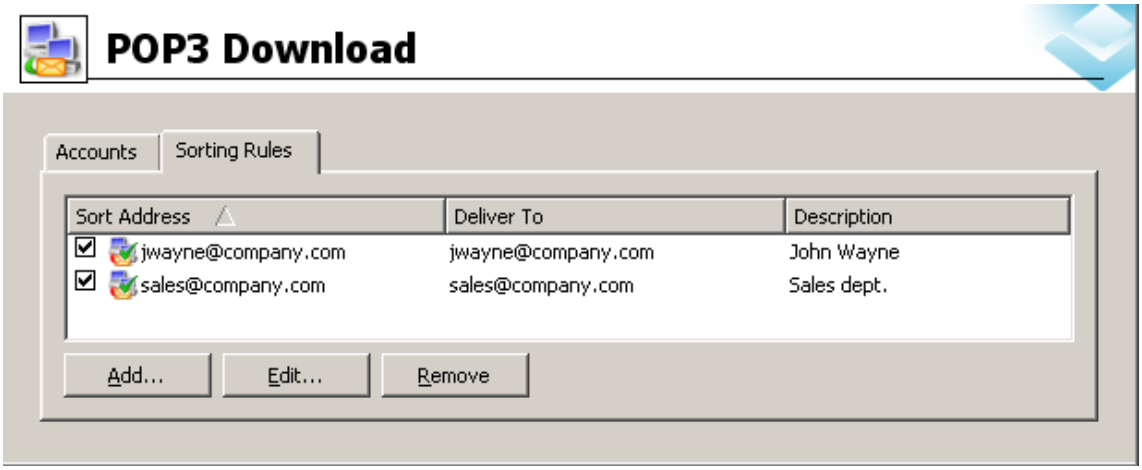

Figure 15.12 Sorting Rules

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.

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

- 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 other email address.

Note: To deliver messages to groups, you must assign addresses to these groups (or you can create an alias). For details refer to chapter 14.

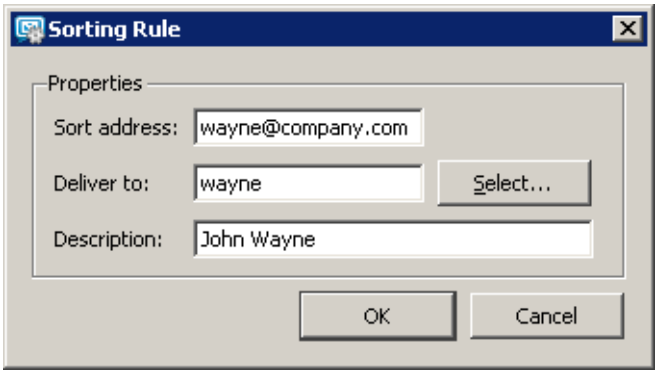

Figure 15.13 Sorting Rule dialog

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.

Example of wildcard usage

In this section you will find examples of how wildcard can be used for the simplest settings of sorting rules. The configuration consists of the following rules:

- The first rule sorts messages by alias settings and by addresses of user accounts.

  `*@company.com` → `*@company.com`

- The second rule sorts messages which, by any reason, cannot be sorted to any particular user account.

  `*` → `admin@company.com`

Note: If any other rule is placed above these rules, it will be processed before them. Rules are always processed in the following order:

1. `address@domain`
2. `*@domain`
3. `*`

15.5 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).

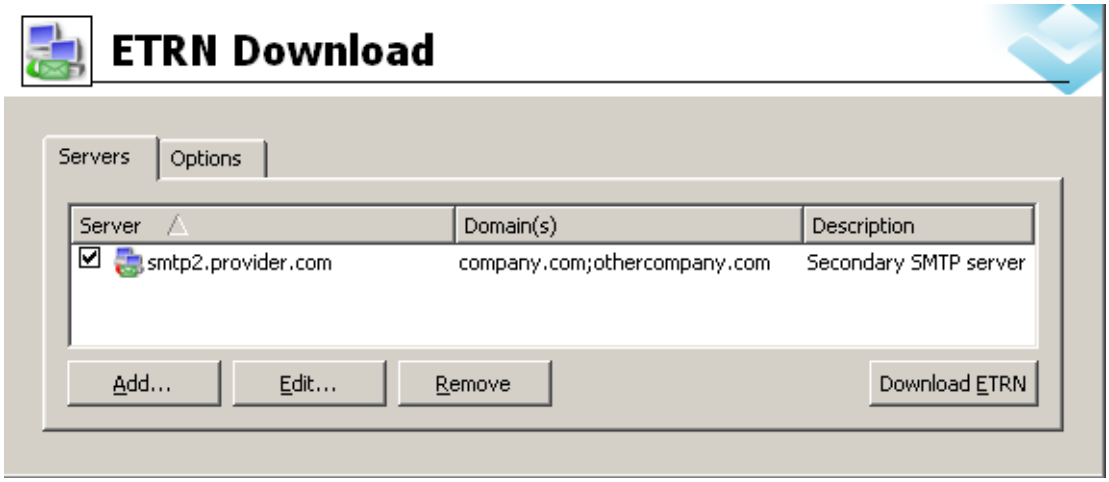

Figure 15.14 ETRN Download

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 (;).

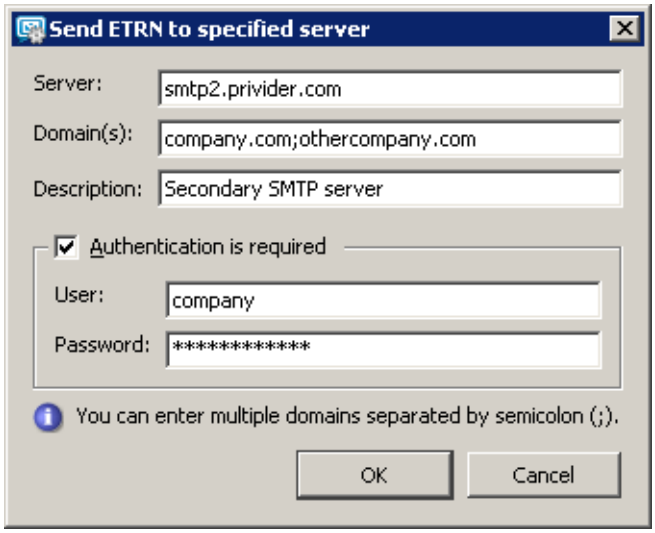

Figure 15.15 Setting parameters for accessing the server

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.

15.6 Advanced Options

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

Miscellaneous tab

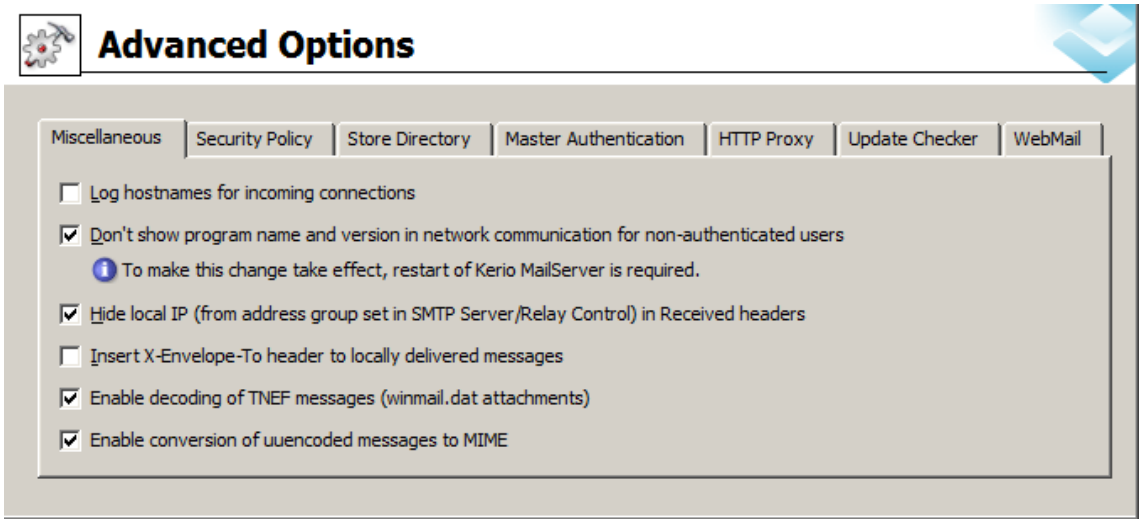

Figure 15.16 Miscellaneous tab

Log hostnames for incoming connections
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.

Warning: To activate or disable the option, restart of *Kerio MailServer* is required.

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 15.2).

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*.

Note: If any problems regarding message decoding occur, the *Debug* log may help

where it is necessary to enable the *Message decoding* option. See chapter 22.8 for more information.

Enable conversion of uuencoded messages to MIME

Uuencode (Unix-to-Unix Encoding) is an encoding method used for sending of files by email. It encodes binary data to a text format so that the data can be inserted directly to message bodies. The main problem is that some email clients may miss a special decoder which decodes the encoded files and transforms them to their original format. Therefore, *Kerio MailServer* includes a built-in Uudecode decoder (Unix-to-Unix decoding). Email messages are decoded to the standard MIME format on the server's side so that users do not have to worry about this topic.

It is recommended to enable the *Enable conversion of uuencoded messages to MIME* option especially if users use *Kerio WebMail* and *MS Outlook* with *Kerio Outlook Connector* to access their mailboxes.

Note: If any problems regarding message decoding occur, the *Debug* log may help where it is necessary to enable the *Message decoding* option. See chapter 22.8 for more information.

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 15.17).

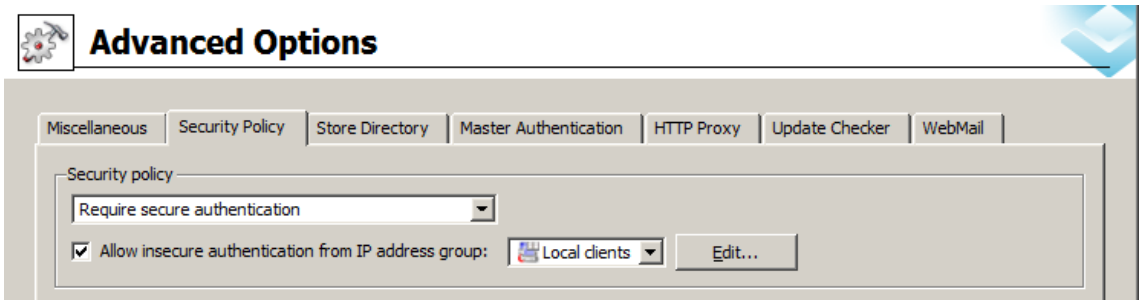

Figure 15.17 Security Policy tab

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 12.1.
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 12.1.
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 10).

Supported authentication methods

Kerio MailServer supports the following methods of user authentication:

Figure 15.18 Authentication methods

- 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).
- 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*. Configuration of NTLM authentication is addressed in chapter 25.
- 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.

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.

To see what is necessary to be set in *Kerio MailServer* to make NTLM authentication work smoothly, refer to chapter 25.

In the *Account lockout* section the following parameters can be defined (see figure 15.19):

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
MS Windows	NTLM LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN
LINUX	LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN
Mac OS X	LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN

Table 15.3 Authentication methods

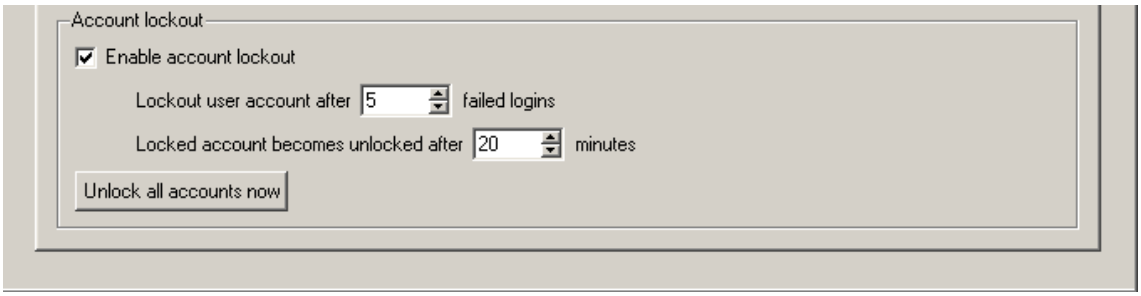

Figure 15.19 Account lockout

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.

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.

Warning: Blocking of accounts upon unsuccessful login attempts is not identical with blocking in user account settings (see section 13.2).

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). By technical reasons, it is necessary to locate the store directory locally (i.e. on the server where *Kerio MailServer* is running).
If the data directory path needs to be changed, follow these instructions:

1. Create a new directory for the store.
2. In *Kerio Administration Console* (*Configuration* → *Advanced Options* → *Data store*), specify the new path.
3. Stop *Kerio MailServer*.
4. Move all files included in the data store to the new directory.
5. Run *Kerio MailServer*.

Warning: It is not allowed to specify the *Path to the store directory* entry by a UNC path.

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 22.6).

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 22.6).

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.

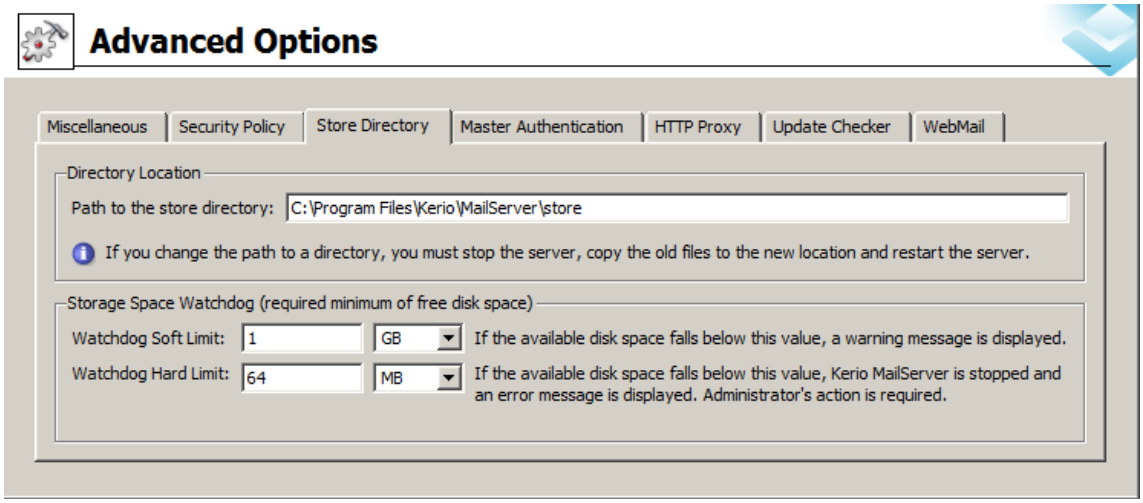

Figure 15.20 Store Directory tab

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.

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*.

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*).

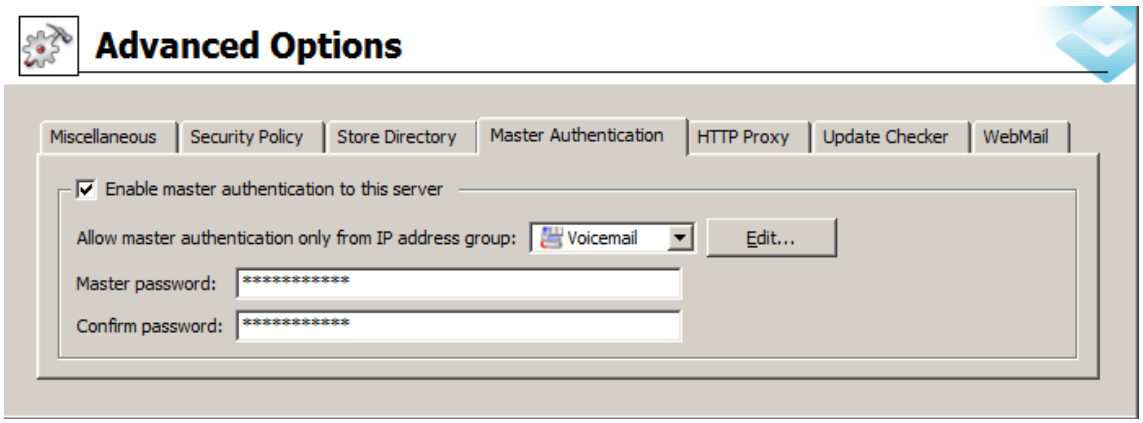

Figure 15.21 Master Authentication tab

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 12.1). 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.

Proxy server requires authentication

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

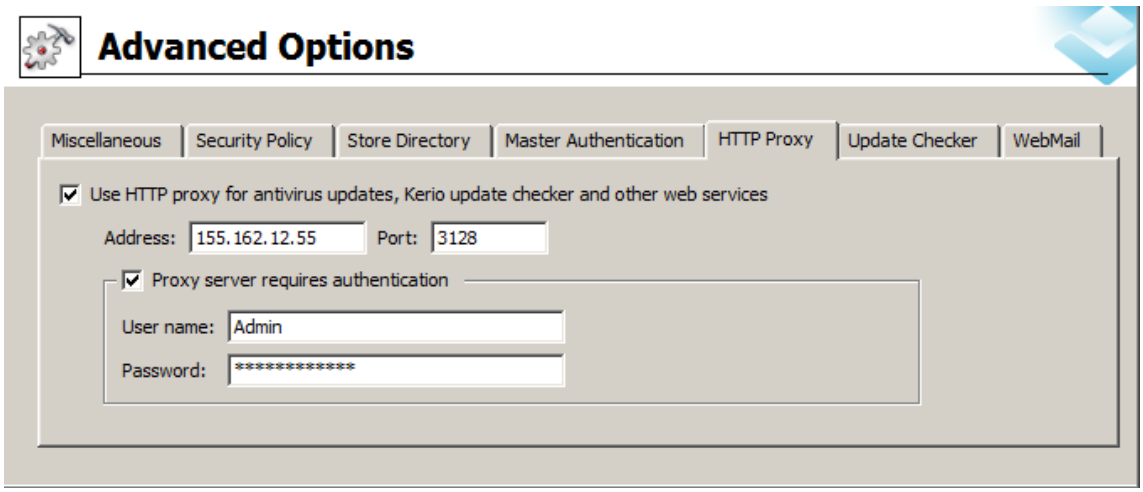

Figure 15.22 HTTP Proxy tab

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

Password
Insert your password to connect to the proxy server.

Update Checker tab

The tab defines updates of new versions of *Kerio MailServer* and automatic updates of the *Kerio Outlook Connector* and the *Kerio Synchronization Plug-in*:

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.

Check for new versions of Kerio MailServer
This option enables the feature of automatic checking whether there is a new version of *Kerio MailServer* available at the *Kerio Technologies* website.
If a new version was released by *Kerio Technologies*, the *Update* tab will contain link to the download web page.

Check also for beta versions
This option enables informing users that a new betaversion of *Kerio MailServer* is available.
Warning: 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.

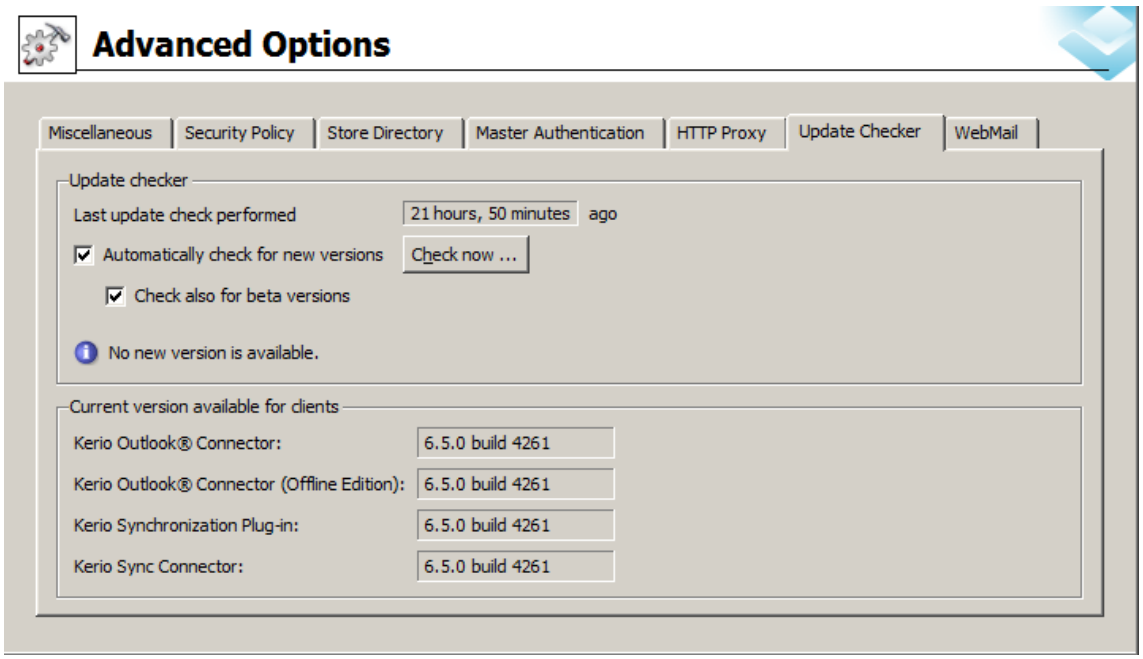

Figure 15.23 Update Checker tab

The installation package includes also automatic installations of the *Kerio Outlook Connector*, the *Kerio Outlook Connector (Offline Edition)*, the *Kerio Synchronization Plug-in* and the *Kerio Sync Connector for Mac*.

The *Current version available for clients* field displays the information about the module versions currently used (including build numbers).

- *Kerio Outlook Connector* — the package is updated for all users immediately upon update of the server.
- *Kerio Outlook Connector (Offline Edition)* — the package is updated for all users immediately upon update of the server.
- *Kerio Synchronization Plug-in* — the package is updated for all users immediately upon update of the server.
- *Kerio Sync Connector for Mac* — users on client stations will be informed about available updates for the *Kerio Sync Connector*. If they conform the dialog, the program gets updated.

Kerio MailServer performs automatic update checks for the *Kerio Outlook Connector*, the *Kerio Outlook Connector (Offline Edition)* and the *Kerio Synchronization Plug-in*. The update checks help avoid problems caused by incompatibility of older server and newer plug-in versions or, vice versa, of newer server and older plug-in versions. In case that there is a collision detected, users are informed that the plug-in should be upgraded/downgraded. The correct version is installed upon confirmation. If a user rejects

to install a new version, it depends whether the server version differs in the version number or in the build number only:

1. Build numbers are different — plug-in is started along with the *MS Outlook*. Before each startup of the *MS Outlook*, alert is displayed informing that the plug-in should be updated.

2. Version numbers are different — the plug-in refuses to connect to the server until it is updated.

New versions of the *Kerio Outlook Connector*, the *Kerio Outlook Connector (Offline Edition)*, the *Kerio Synchronization Plug-in* and the *Kerio Sync Connector* are saved in

`Kerio\MailServer\webmail\download`

Warning: Update of plug-ins requires the HTTP or the HTTPS service to be running. Only for *Kerio Synchronization Plug-in* — 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 client stations (a self-signed certificate can be used). Otherwise, new versions will not be updated automatically.

A server certificate can also be created in the *Kerio MailServer's* administration console. For detailed instructions, see chapter 10.

Note: If any problems regarding the update occur, enable the *Update Checker Activity* option (detailed information can be found in chapter 22.8) in the *Debug* log settings. Logged information might help you where any problems to be solved occur.

WebMail

In *Kerio Administration Console*, several parameters for *Kerio WebMail* can be set (see figure 15.24):

Message size limit

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

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

Warning: Maximal value of the limit is 128 MB. It is not possible to enter a greater value in the *Kerio Administration Console*.

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.

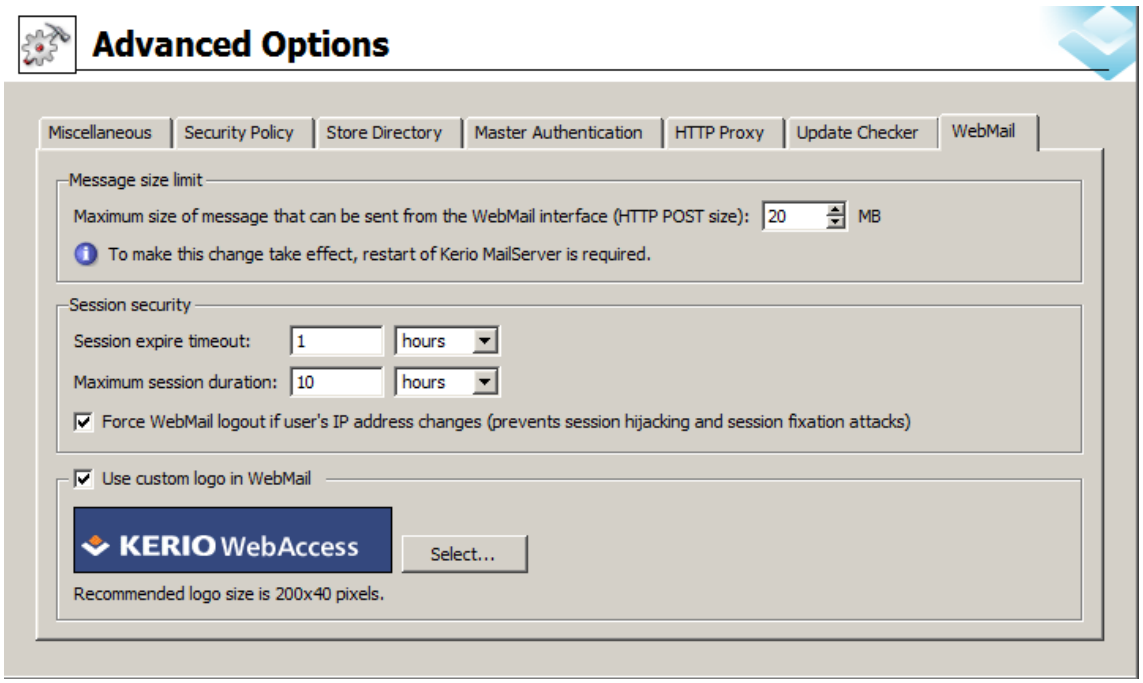

Figure 15.24 WebMail

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

The minimum 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 minimum 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.

Maximum time can also be set for sessions in addition to the session's expiration time. The maximum session time means the time since user's connection. If users use the *Kerio WebMail* interface as the main connection to their mailboxes, set the time to a value between 8 and 10 hours. Too short interval might cause inappropriate closure of a session (while a user is editing a message, for example). This is not desirable.

Note: If the user has started composing a message and has not finished it yet and the session expires, user authentication will be required for reconnection. After successful re-authentication, the message can be finished and sent.

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 11.2). The image parameters are as follows:

- Format: GIF
- Size: 200x40 pixels

Click *Select* to browse to the logo file.

Chapter 16

Antispam control of the SMTP server

Antispam control of SMTP server protects users from spam. Spam is an 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).

Kerio MailServer includes many options and features to dispose of spam. These features include various filters, testing and monitoring technologies which help distinguish quite precisely spam messages from desirable email.

To detect and eliminate spam, *Kerio MailServer* uses the following methods and tests:

- SpamAssassin (detailed information on its features and settings, see section 16.4).
- Black/White lists (detailed information on their features and settings, see section 16.2).
- Proprietary filtering rules (detailed information on their features and settings, see section 16.3).
- Caller ID (detailed information on its features and settings, see section 16.5).
- SPF (detailed information on its features and settings, see section 16.5).
- Delayed response to SMTP greeting (detailed information on their features and settings, see section 16.6).

Each test can be used separately or combined with the others. To achieve better efficiency, it is recommended to combine as many antispam features as possible. The more tests are used, the denser is the antispam filter and the less spam will be delivered to user's mailbox. Also the spam detection will be more successful which will reduce number of messages marked as spam by mistake (so called "false positives").

Each testing type uses specific methods to detect spam. There is, however, a feature most of the tests have in common. For all methods except the Delayed response to SMTP greeting, two actions can be set of what how spam messages would be handled. One action is denial of such messages. The other is to raise the so called spam score (for details, see chapter 16.1). Messages with a score too high awarded by multiple tests are discarded (individual scores are summed). The first alternative may help reduce load on the server, the second one eliminates better possible "false positives".

Warning: When *Kerio MailServer* is connected offline, efficiency of the antispam filter decreases dramatically.

To set *Kerio MailServer's* spam filter, go to *Configuration* → *Content Filter* → *Spam Filter*.

16.1 Spam Rating tab

The *Spam Rating* tab enables/disables spam rating and defines criteria for spam to be blocked in case that the method of spam score raised by multiple tests is used:

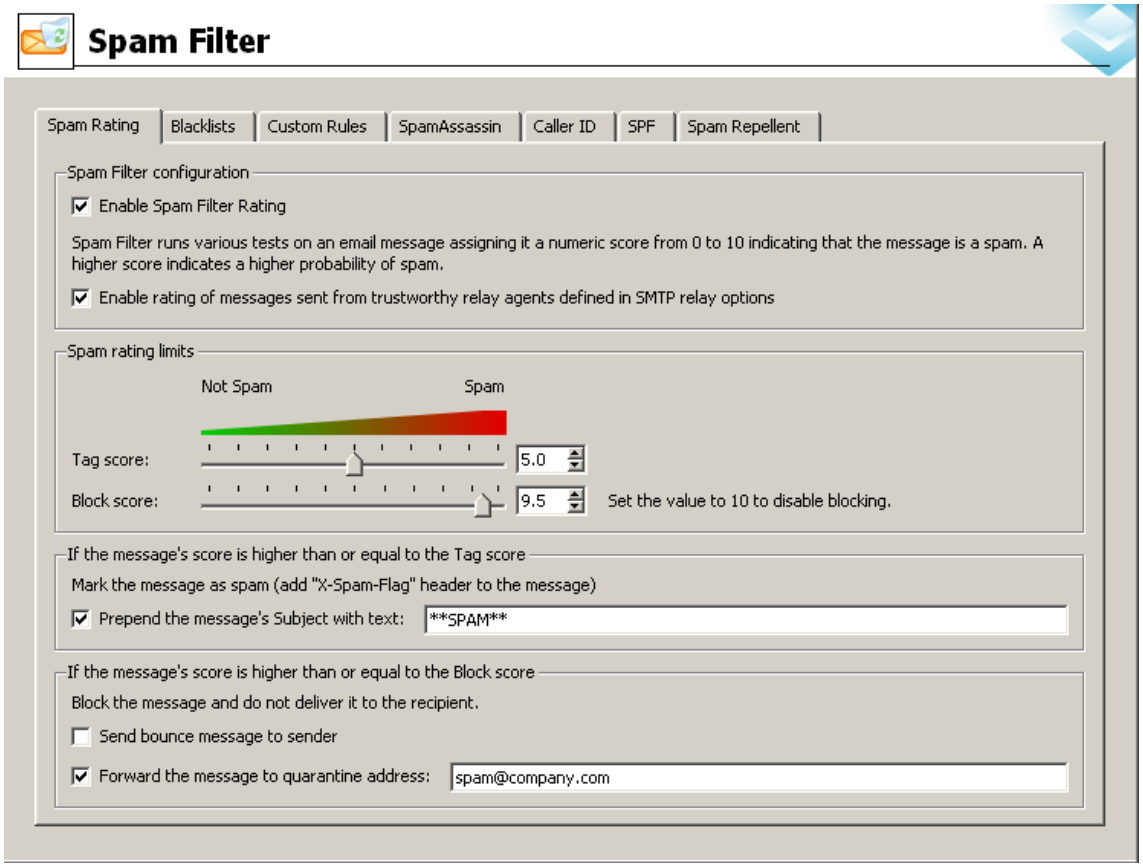

Figure 16.1 Spam Rating tab

Enable Spam Filter Rating

Individual spam tests may rate each incoming message by a value. The higher the result number is, the more probably the message is a spam. The spam rating awarded by antispam tests is called spam score. If a message is tested by multiple tests, spam scores are summed and the result is recorded in `X-Spam-Status`, a special header of the message.

If the spam rating is off, messages are rated anyway. The results, however, are ignored by the spam filter. However, only such tests where message blocking is set will be applied to tested messages.

Enable rating of messages received from ...

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 15.2).

This option is not applied to checking of "email policy" records (see section 16.5) and to "black/white lists" (see section 16.2).

Spam rating limits

Once a message is tested by all enabled tests and filters, it is rated by the result spam score. *Kerio MailServer* then marks the message as spam or delivers it as a legitimate message. The *Spam rating limits* scale allows set manually the limit where messages are already marked as spam and where the spam score is so high that there is no doubt it is a spam and can be blocked:

- *Tag score*
  If the rating reaches or exceeds the value set, the message is marked as spam. *Kerio MailServer* appends a special `X-Spam-Flag` header to the message that informs the email client that the message is a spam.
  Use the entry to specify a number from `0.0` to `10.0` (the lower the number is, the more spam messages will be eliminated).
  We recommend you to use the `5.0` value — statistics claim that 91.12 per cent of spam do not pass through this filter or will be marked as spam. Other 0.62 per cent of legitimate messages, however, will also be marked as spam. 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:
  1. If the value you set will be too low, every message will be considered as a spam.
  2. If efficiency of the spam filter declines, do not lower the tag score or the block score. Better involve multiple tests in the spam filter.
- *Block score*
  If the rating reaches or exceeds the value set, the message is discarded.
  If the value is too low, legitimate messages might be discarded along with spam. Therefore, it is recommended to use the *Forward the message to quarantine address* option when testing and optimizing the spam filter and specify an account where copies of all blocked messages will be delivered and stored. Copy of any message having reached or exceeded the Block score limit will be sent to the specified mailbox. From time to time, simply scan discarded messages to check that there is no legitimate message trapped.
  Maximal block score allowed is `9.9`. If the value is set to 10, the blocking is disabled, so that messages are marked as spam but never blocked.

Note: If values for marking and blocking of the message are equal, all messages marked as spam are discarded automatically.

If the message's score is higher than or equal...

The `X-Spam-Flag` header is appended to the message and the message is delivered to the recipient.

In addition to marking spam messages by the special header, it is possible to prepend message's subject with a text which will inform user or a sieve rule that the message is a spam (such a rule can be created within creation of user accounts in the *Kerio Administration Console* — for details, see chapter 13.2).

The `**SPAM**` string is used as a default text. The string can be modified in the *Mark the message as spam* section (for details, see below).

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 anti-spam protection system is inserted into this textfield. This implies that users can define one of more custom antispam rules (depending on the number of asterisks) in their mail server or in the *Kerio WebMail* interface.

Send bounce message to the sender

The server returns the sender a DNS message informing that the email message cannot be delivered.

It is not recommended to use this option since most of spam message use false sender addresses. This implies that the denial message cannot be delivered (the address to which the DNS message is sent might not exist). Messages with the information about their rejection are then kept in the queue where they must be removed manually. Otherwise, the server attempts to deliver them in intervals set in the queue settings (every 30 minutes for five days, by default). Undeliverable messages are discarded.

Forward the message to quarantine address

Enter an address to which blocked messages will be forwarded (regardless of other settings of the antispam filter). Headers of such messages include information on tests having been applied to the message along with score set by individual tests. If a legitimate message blocked by the tests is included in the box, it is possible to use the information to optimize the tests.

For this purposes, it is recommended to create a special email account (e.g. `spam@company.com`) where copies of spam messages will be delivered and stored.

16.2 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.

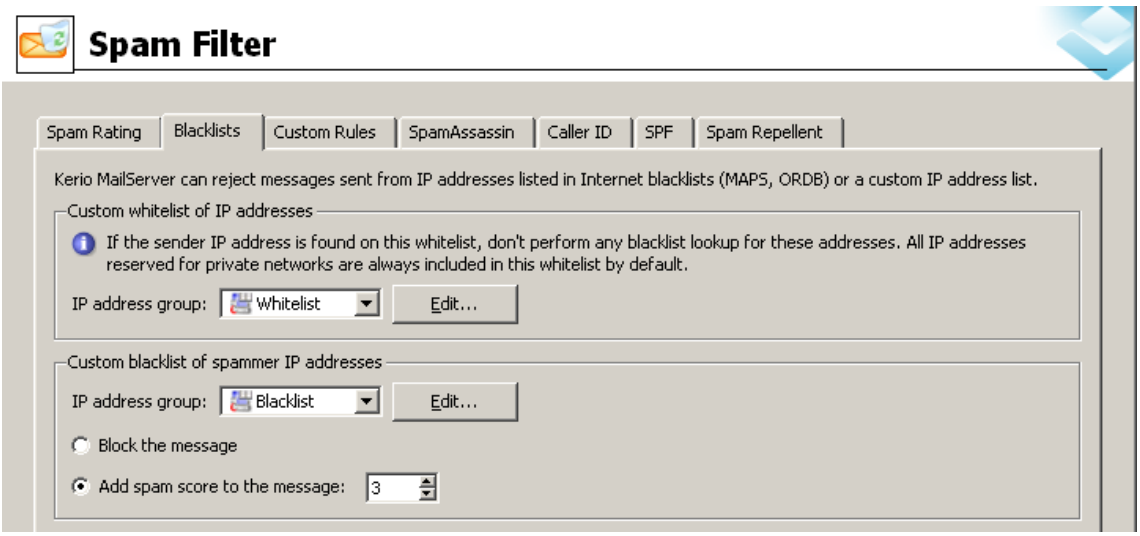

Figure 16.2 Blacklists tab

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 tested against blacklists and they are let in automatically. Other types of antispam tests, however, will not apply to them.

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.

```
127.0.0.1

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:

- *Block the message*
  The message will be blocked on the SMTP level and the sender will be informed that the message cannot be delivered.
- *Add this value to the message's spam score:*
  Set spam score will be added to the message's score.
  In case of blacklist, the recommended score value is from 1 to 4 points.

Internet databases

Kerio MailServer can use various spammer databases (free or paid) available in the Internet. Spammer databases include list of SMTP servers which are known as spam senders. There are multiple online spammer databases available. Some of them are free and some of them must be purchased. Generally, quality of services provided by paid databases is higher and their blacklists of SMTP servers are more reliable.

Online spammer databases work separately and they can be combined.

By default, *Kerio MailServer* contains a few databases which can be downloaded from the Internet for free. It is also possible to define any other databases. This can be done in the *Internet Blacklist* dialog (see figure 16.4) which can be opened by clicking on the *Add* button located below the list of databases. The dialog allows setting of the following options:

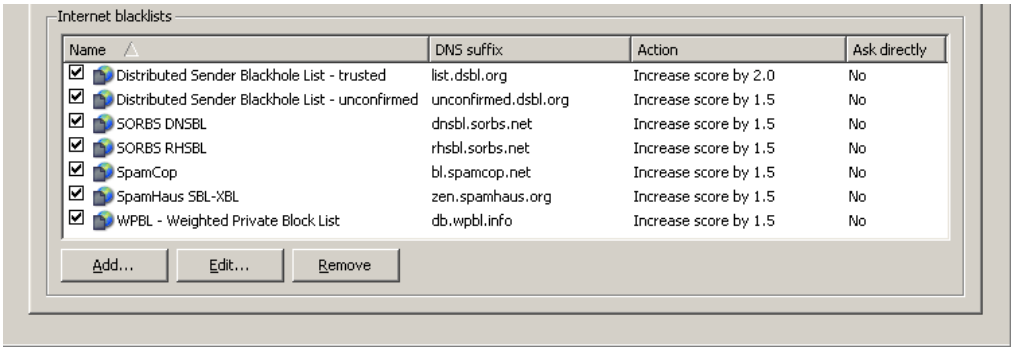

Figure 16.3 Internet databases

DNS suffix

Enter name of the DNS server used by *Kerio MailServer*.

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*. Senders will be informed that their messages cannot be delivered.

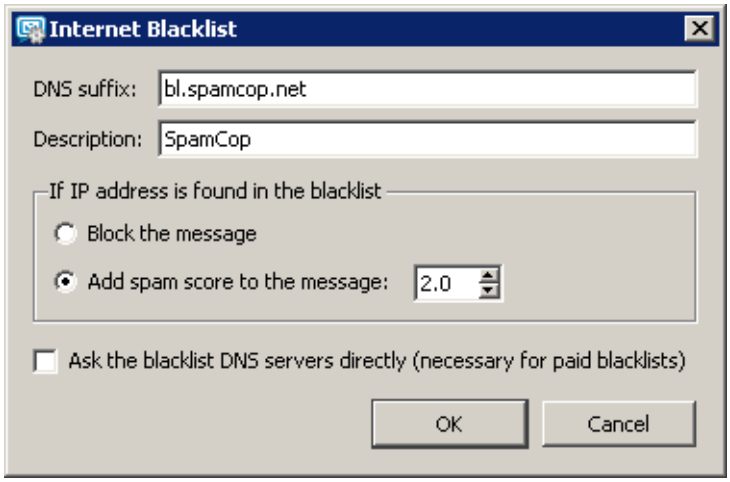

Figure 16.4 Database parameters

Add spam score to the message

The value set here will be added to any message accepted from any server included in the blacklist.

In case of this blacklist, the recommended score value is from 1 to 3 points. The value of the score added depends on level of trustworthiness of a particular database. Generally, paid spammer databases examines more thoroughly SMTP servers to find out whether they really are spam senders or not. Therefore, if you use paid databases, it is possible and even more efficient to set higher scores than in case of free databases. This is, however, only a general

knowledge which cannot be applied without exceptions. If you are familiar with a free database and you are sure that it would be efficient, you can set higher scores for them as well.

If you combine multiple spammer databases, set lower spam scores since individual SMTP servers may be included in multiple databases and their scores are summed.

Ask the blacklist DNS servers...

using of this option is recommended in cases where *Kerio MailServer* uses a paid spammer 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.

Note: Any time a delivered message is sent from an address which matches a blacklist item, the information is recorded in the *Security* log (for details, see chapter 22.4).

Therefore, to test reliability of a new blacklist, include it to the list and set the *Add spam score to the message* option to 0. Email will not be affected and each message matching with the blacklist will be listed in the *Security* log.

Supported databases

SpamCop

Kerio MailServer supports SpamCop, a database of spammer IP addresses. For more information on SpamCop, refer to `http://www.spamcop.net/`

SORBS

Spam and Open Relay Blocking System (SORBS) creates and maintains set of databases of spammer IP addresses and domain names. By default, *Kerio MailServer* includes two aggregate zones of spammer databases containing all basic partial databases addressing certain types of spammer servers:

- *SORBS-DNSBL* — database of spammer IP addresses.
- *SORBS-DNSBL* — database of spammer domain names.

For more information on SORBS, refer to `http://www.de.sorbs.net/`

SpamHaus SBL-XBL

The SpamHaus SBL-XBL database combines a database of spammer IP addresses with a database of illegal exploits performed by third parties:

- *Spamhaus Block List* — SBL is a database of IP addresses of proved spammers. These servers are verified to prove that they really are spammers.
- *Spamhaus Exploit Block List* — XBL is a database of IP addresses of illegal exploits performed by third parties, including open proxy servers, worms and viruses carrying harmful executable codes and other types of Trojan horse.

For more information on SpamHAUS SBL-XBL, refer to http://www.spamhaus.org/

Weighted Private Block List

Weighted Private Block List (WPBL) is a database of spammer IP addresses maintained by a committee scanning for and rating spammer servers. The database is available for free. For more information on WPBL, refer to http://www.wpbl.info/

Distributed Sender Blackhole List

There also exist several types of Distributed Sender Blackhole List (DBSL) databases. By default, *Kerio MailServer* includes the following ones:

- *Distributed Sender Blackhole List — trusted* — the list includes all single-stage spammer relay servers. These servers are verified to prove that they really are spammers.
- *Distributed Sender Blackhole List — unconfirmed* — the list includes any reports on spammer servers received. This means that it includes also servers which are not tested sufficiently for spam-sending. Therefore, it is recommended to set lower score values for this blacklist.

For more information on DSBL, refer to http://dsbl.org/.

16.3 Custom Rules

If *Kerio MailServer's* internal antispam features do not satisfy your needs, it is possible to manually customize rules to create a suitable filter which would complement the internal system and increase the antispam efficiency. These rules can be defined on the *Custom Rules* tab.

The tab consists of two sections. One contains list of rules and their definition tools. The latter covers settings of how messages blocked by server-defined rules would be handled.

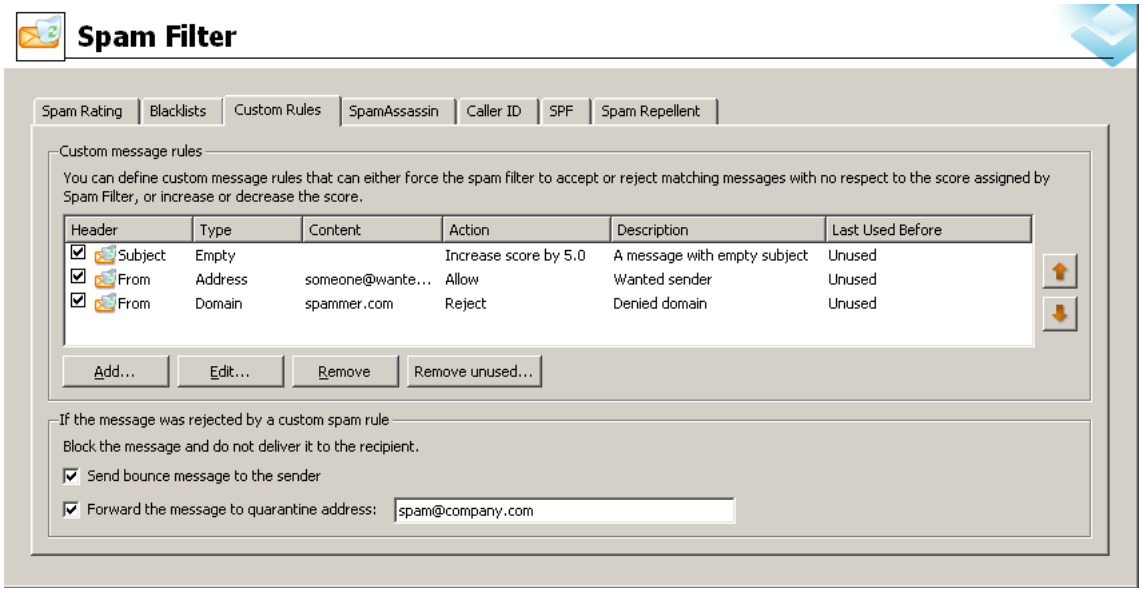

Figure 16.5 Custom Rules

Rule Definition

On the tab, each filtering rule is represented by one line (see figure 16.5). 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.

When creating rules, bear in mind that their order in the list is very important. Individual rules are processed in the same order as listed, downwards. Rules in the list can be reordered by the arrow buttons on the right. Simply select a rule in the list and click the arrows to move it up or down.

Rules can also be moved by the Drag and Drop method, i.e. by dragging and moving rules by mouse.

It is essential to consider twice especially location of denial and allowance rules since once these rules are processed, no other rules are applied. After rules where only score points are added or taken off, other rules are processed unless all of them are applied or unless the message matches a permission/denial rule.

Note: Rules tested against `From` and `To` headers have a peculiarity which might be beneficial. If these rules go before the others, they will be tested on level of SMTP traffic. In case of denial rules, messages matching such a rule are blocked even before accepted to the queue of incoming messages. This decreases the load on the server. It helps the server avoid taking several actions and using of several tools such as antispam tests and antivirus control which is applied once a message is accepted to the queue of incoming messages. In case of permission rules, no other rules are applied if they are tested

on level of SMTP traffic. For detailed description on testing of headers, see below (the *Headers* section).

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.

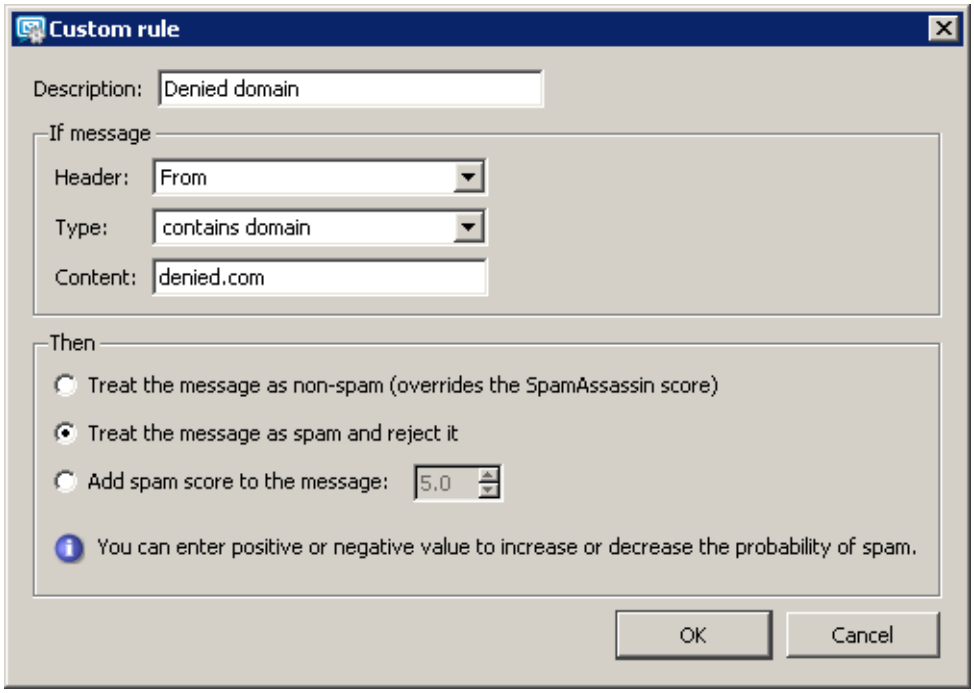

Figure 16.6 Defining rule

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 the following facts:

Any other settings for blocked messages do not apply to messages rejected on SMTP level. Any message meeting the denial rule is rejected and marked with the

standard 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.
To rules regarding *From* and *To* items, a special exception regarding their order in the rule list is applied (see above). If the *From* and *To* rules are starting the rule list (no other rule precedes them), they are executed against the `MAIL FROM:` and `RCPT TO:` headers on SMTP level. If there is even a single rule preceding these rules which is tested against a different header, the message is automatically accepted in the queue of incoming messages while the *From* and *To* rules are tested against `From:` and `To:` headers included inside the message.
The issue will be better understood through the following examples:

- *Example 1:*
  In Example 1 (see table 16.1), rules are ordered so that messages sent from `jwayne@spammer_domain.com` are accepted by *Kerio MailServer*, while any other messages from the `spammer_domain.com` domain are blocked on SMTP level. The third rule allows any messages delivered to the local domain `company.com` on SMTP level.
  Warning: The following testing methods are applied prior to custom rules:
  - *Spam repellent*
  - *Caller ID* and *SPF*
  - Whitelists/Blacklists

  This, however, implies that every message including the `jwayne@spammer_domain.com` address as a sender is tested. If not blocked by the tests listed and having reached custom rules, the permission rule is applied and no additional tests will be applied to the message (actually, they will, but their result scores will be set to 0 points).

Header	Type	Content	Action
From	Address	jwayne@spammer_domain.com	Enable
From	Domain	spammer_domain.com	Decline
To	Domain	company.com	Enable

Table 16.1 Example 1:

- *Example 2*
  Example 2 (see table 16.2) shows a situation where any email addressed to `admin@company.com` is blocked on SMTP level. The next rule blocks any email from the `spam.com` domain except messages where the `test` string is included in the `Subject` header.

Header	Type	Content	Action
To	Address	admin@company.com	Decline
Subject	Substring	test	Enable
From	Domain	spammer_domain.com	Decline

Table 16.2 Example 2

Warning: The examples imply that, when creating rules, it is also necessary to avoid situations where one rule is unexpectedly influenced by another. This might happen for example when users are subscribed in mailing lists and addresses in `MAIL FROM:` and `RCPT TO:` do not match addresses in `From` and `To` headers inside the message.

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 will be applied to it, regardless of the spam filter.

Add this value to the message's spam score

Define score value for SpamAssassin (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 *SpamAssassin* evaluation (negative values protect messages from being considered as spam).
In case of this blacklist, the recommended score value is from 1 to 3 points.

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.

2. A user has demanded regular messages with current special offers. These messages are sent from `info@offer.com` and they are treated as spam by *SpamAssassin*. 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 SpamAssassin score)* option.

If the message was rejected by a custom spam rule

The settings are applied only to custom rules where the *Treat the message as spam and reject it* option is set:

Block the message and do not deliver it to the recipient
: Message will be discarded without notification. This action is not performed if the rule filters the `From` and `To` items (for details, see above).

Send bounce message to the sender
: The server returns the sender a DNS message informing that the email message cannot be delivered.
It is not recommended to use this option since most of spam message use false sender addresses. This implies that the denial message cannot be delivered (the address to which the DNS message is sent might not exist). Messages informing about denial of the original messages are then waiting in a queue where there must be physically removed, otherwise, the server attempts to send them every 30 minutes and discards the messages after two or three days.

Forward the message to quarantine address

The address to which messages will be forwarded and where administrator or another authorized person can check whether there are or there are not legitimate messages included in the spam. Using this option is recommended since it helps you avoid losing of non-spam email without any notification.

16.4 SpamAssassin

To face spam, *Kerio MailServer* uses *SpamAssassin*, a famous antispam filter. *SpamAssassin* consists of several testing methods:

- filter based on statistical evaluation of message content
- Bayesian filter
- SURBL (Spam URI Realtime Blocklist) — this method tests links to websites possibly included inside email against special online databases.

Note: For easier solution of problems regarding *SpamAssassin* that might arise, enable the *SpamAssassin Processing* option in the *Debug* log settings. To read more on the *Debug* log, see chapter 22.8.

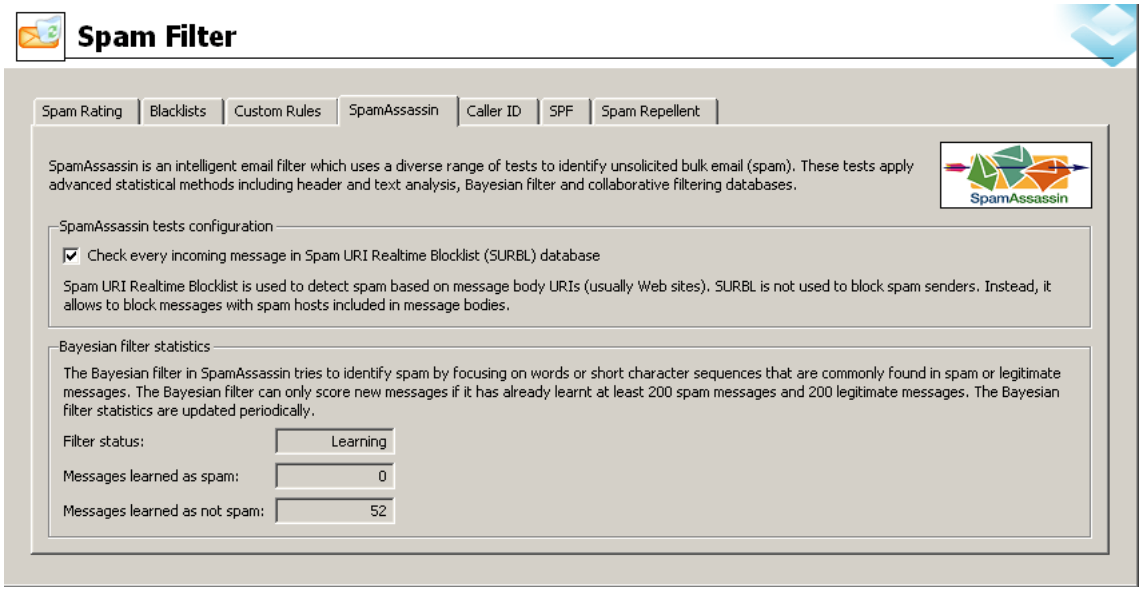

Figure 16.7 SpamAssassin

Content evaluation

Content evaluation is based on statistical filtering using the message's contents (keywords, number of capital letters, message format, 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.

Bayesian filter

Another module involved is the *Bayesian filter*. It is a special antispam filter which is able to "learn" to recognize spam messages. This filter compares the individual spam characteristics with actual messages. The method consists of two concurrent modes:

- "Autolearn" — the filter learns by itself.
- "Learn" — users are involved in the learning process. 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.

200 unique spams and 200 unique hams (legitimate messages) must be collected to make the filter work. This means that such messages must vary. Each spam message is involved only once. Other occurrences of an identical message will be ignored.

Bayesian filter sums spams and hams learned by the learn and autolearn methods. The *SpamAssassin* tab contains statistics that monitor how many messages have been marked as spam or ham and whether the filter is already active or has not learn enough spam and ham messages yet. Once activated, the learning process keeps on introducing new items in the database.

Note: SpamAssassin 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 in the "Learn" mode, 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. Messages that are incorrectly marked as spam can be moved to *Inbox* by hand. Spam messages let in by mistake can be moved to the *Spam* folder manually. This ensures proper and efficient learning and improvement of the Bayesian filter.

Online SURBL database

This part of the filter tests contents of messages (links to websites possibly included in message bodies) against special online databases.

SpamAssassin can use multiple online databases. In *Kerio MailServer*, it, however, uses only the SURBL database since the other databases are already used for other tests.

16.5 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.

Warning: SPF and Caller ID can be applied only to email delivered by SMTP. If email is downloaded from the domain mailbox by POP3 protocol, email policy logs will not work.

Caller ID

The *Caller ID* tab enables users to configure basic settings:

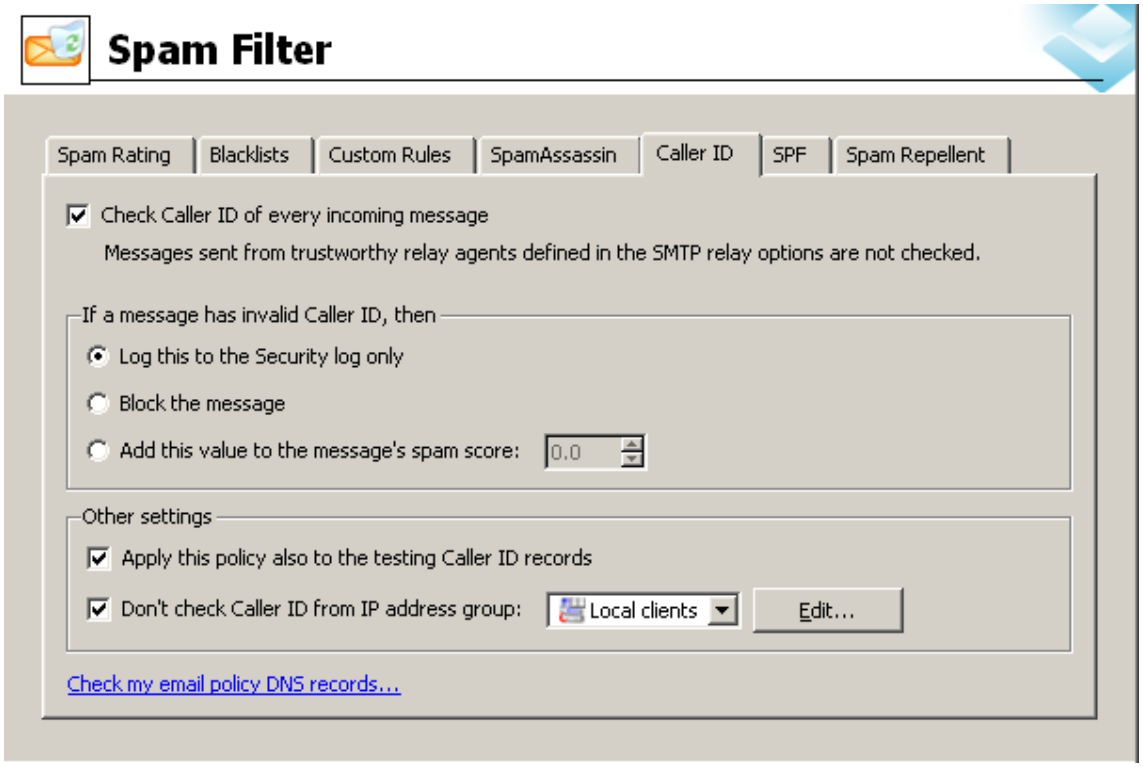

Figure 16.8 Caller ID tab

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 15.2).

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.

Block the message

Message including invalid *Caller ID* will be blocked on SMTP level. Senders are informed that their message cannot be delivered.

Add this value to the message's spam score

The value set here will be added to message's total score (see section 16.1).

In case of the *Caller ID* method, it is recommended to use value from 1 to 3 points.

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*.

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 15.2).

Only log this to the security log

Messages with an invalid SPF record will be only added to the *Security* log.

Block the message

Message including invalid *SPF* will be blocked on SMTP level. Senders are informed that their message cannot be delivered.

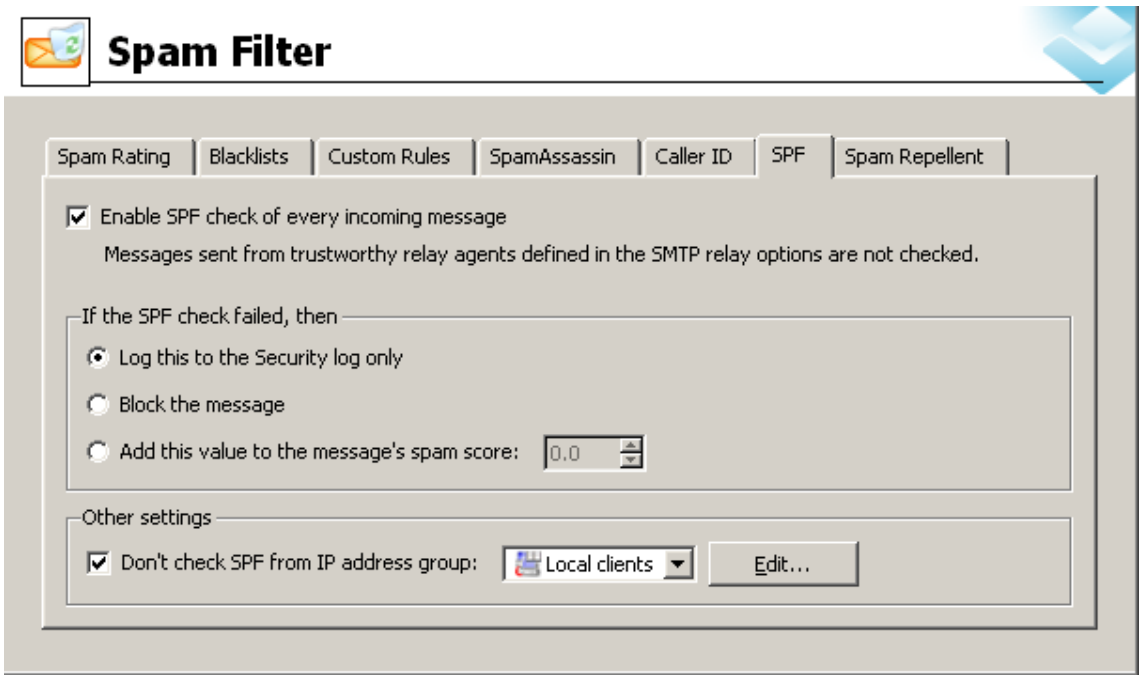

Figure 16.9 SPF

Add this value to the message's spam score

The value set here will be added to message's total score (see section 16.1).
In case of the *SPF* method, it is recommended to use value from 1 to 3 points.

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 22.8).

16.6 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 RFC. Thus, *Kerio MailServer* is able to distinguish them from legitimate SMTP servers.

Kerio MailServer uses two SMTP connection errors to recognize spam servers. These errors occur while establishing SMTP connection. 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*):

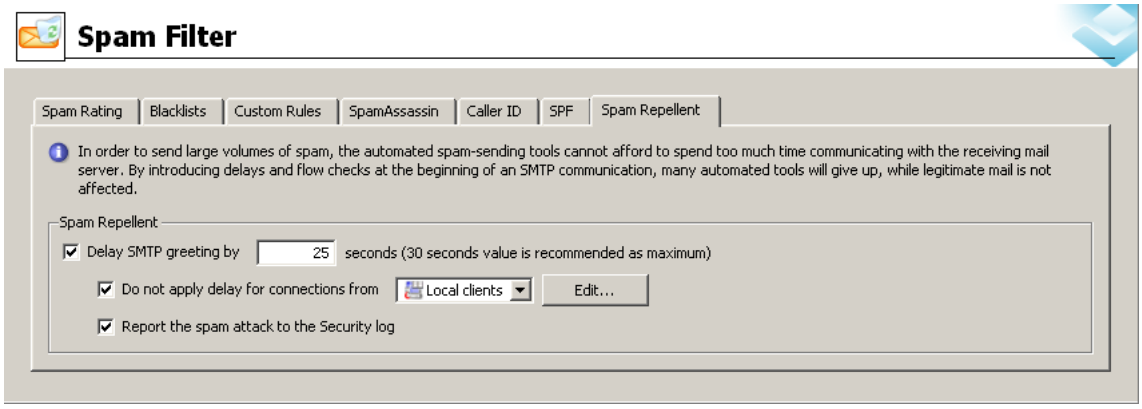

Figure 16.10 Spam repellent

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, etc. 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 22.4).
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.

16.7 Recommended configuration of antispam tests

This section is helpful for anyone who is not sure about proper configuration of antispam filters. The example describes optimal settings of scores for individual types of antispam tests. Notice that almost never the message blocking is not preferred to increasing of spam score:

Spam Rating tab

The essential setting is configuration of the *Spam Rating* tab (for details, see section 16.1). It is recommended to leave most of the settings as predefined by default:

1. Make sure that the *Enable Spam Filter Rating* option is enabled. If the option is inactive, enable it.

   This option makes the filter consider and apply results of individual evaluations (spam scores).

2. Make sure that the *Enable rating of messages sent from trustworthy relay agents defined in SMTP relay options* option is inactive (unless you wish to check even messages sent from trustworthy addresses).

3. Follow these instructions to set resolution of the spam filter scale:

   - *Tag score* — set the value to 5 points.
   - *Block score* — set this value to 9.9 points. This will ensure that only "hundred-percent" spam messages are discarded by the server since users are not even notified that such messages would have been blocked (unless at least one of the

Send bounce message to the sender or *Forward the message to quarantine address* options are enabled).
Note: If you do not wish to block any messages no matter what the score is, set the value to 10.0 points. This disables blocking of messages and keeps active only the feature of marking as spam.

4. Make sure that the *Send bounce message to the sender* option is disabled.

   Since spammers generally use invalid sender addresses in their headers, we will keep this option disabled. It would be impossible to deliver responses to such messages and they would be kept in the queue of outgoing email.

5. Finally, enable the *Forward the message to quarantine address* option and enter an email address where all messages with the score higher than 10 points will be forwarded.

   The option is helpful especially when setting and fine-tuning the antispam system. If there are legitimate messages with their score too high, it will be discovered during an opportune check of the mailbox where spam copies are delivered and stored. Later, this option can be disabled and the mailbox removed.

Blacklists tab

Once the general configuration is completed, it is necessary to set individual testing methods. The first test can be set on the *Blacklist* tab (for details, see section 16.2). The following parameters are to be set here:

1. *Custom whitelist of IP addresses* — this option enables definition of servers to be excluded from the antispam control. For this example, we will make out a business partner whose SMTP server has been included in online spammer databases by mistake. Since we need to communicate with this partner by email, it is necessary to include the address of their SMTP server in the whitelist — at least for the time until the address is left out of the databases:
   - In *Custom whitelist of IP addresses*, create a new IP group called `Whitelist`. To find out how IP groups are created, see section 12.1.
   - Add the IP address of the corresponding SMTP server included in a spammer database to the new IP group and save these settings. Messages sent from this SMTP server will not be checked by any antispam control.
     Warning: Make sure that is no spammer SMTP server is included in the whitelist.

2. *Custom blacklist of spammer IP addresses* — the settings are similar as for whitelists, with reversed reasons and results. Create an IP group where you involve all spammer

SMTP servers you know. This option is helpful especially for cases where antispam tests are not able to recognize these servers.

At this moment, define actions that will apply to messages sent from SMTP servers included in the custom blacklist:

- Two options are available on the *Blacklists* tab. Such messages may be blocked or their spam score may be increased. In this example, the second option was selected and 3 points will be added to the spam score. Three points are enough to learn whether the message really is a spam since the message is evaluated by multiple tests and other points would be added to the score.

3. *Internet blacklists* — check all databases available. Use the *Edit* button to open individual databases and set spam score to 2 points (see figure 16.4).

   Recommendation: Do not set message blocking for Internet blacklists, especially for the free ones. These databases may be updated quite rarely or slowly and the information involved might be unreliable. The lists might include non-spammer servers. Therefore, use these databases better to add spam score to suspicious messages.

Custom Rules

Another test for incoming email is a set of custom rules (for details, see section 16.3). Custom rules can be created as needed:

1. Define corresponding rules for SMTP servers. If possible, set addition of only two or three points for all spam rules. Since there are multiple rules defined, each test adds a score if the message is considered a spam.

2. If there is a rule which blocks spam messages, set an address where copies of blocked messages will be sent (see figure 16.11). The best way to do it is to create a special user mailbox (for detailed information on creating of user accounts, refer to chapter 13).

Figure 16.11 Forward the message to quarantine address

SpamAssassin

It is not necessary to apply any special settings to the *SpamAssassin* filter. Any definitions of the filter may be done on the *SpamAssassin* tab (for details, see section 16.4).

The only setting that needs to be changed on the tab is enabling of the *Check every incoming message in Spam URI Realtime Blocklist (SURBL) database* option.

Caller ID tab

To read more on the *Caller ID* technology, see chapter 16.5. If you decide to use this technology, it is strongly recommended to set the tab as follows:

1. Open the *Caller ID* tab under *Configuration* → *Content Filtering* → *Spam Filter*).
2. Enable the *Check Caller ID of every incoming message* option.
3. In the *If the message has invalid Caller ID, then* section, set spam rating to 3 points (as explained above, spam messages are tested and scored by multiple tests so it is not recommended to block it or to set individual scores too high).
4. It is also recommended to enable the *Apply this policy also to the testing Caller ID records* option since most servers which employ the *Caller ID* technology use its testing mode so far.
5. If you use an alternative (backup) SMTP server, specify its address in the *Don't check Caller ID from IP address group* entry.

SPF

For closer description of the SPF technology, refer chapter 16.5. Recommended settings of the SPF test is almost identical with the *Caller ID* settings. It is as follows:

1. Open the *SPF* tab under *Configuration* → *Content Filtering* → *Spam Filter*).
2. Enable the *SPF check of every incoming message* option.
3. In the *If the message has invalid Caller ID, then* section, set spam rating to 3 points (as explained above, spam messages are tested and scored by multiple tests so it is not recommended to block it or to set individual scores too high).
4. If you use a backup SMTP server, enter its address in *Don't check SPF from IP address group*.

It is also recommended to support *SPF* by adding a record regarding SMTP servers which are allowed to send email from your domains to your DNS records.

Spam repellent

Detailed information on *Kerio MailServer's Spam repellent* technology, refer to chapter 16.6. This technology is not involved in spam rating and it is therefore only mentioned in this section. The technology usually sorts out large volume of spam even before it is accepted in *Kerio MailServer* and thus decrease the load on the antispam tests and on the mailserver in particular.

The optimal settings of *Spam repellent* are as follows:

1. Open the *Spam Repellent* tab under *Configuration* → *Content Filtering* → *Spam Filter*).
2. Enable the *Delay SMTP greeting by ... seconds* option and set the value to 25 seconds.
3. Enable the *Do not apply delay for connection from* option and select the local private network as the IP group. This setting helps avoid delays of email sent from local user accounts and delivery of internal messages.
4. Leave the *Report the spam attack to the Security log* option disabled (unless there is a special reason to enable it). Records pointing at interruptions of SMTP connections would otherwise make a large part of the log.

16.8 Monitoring of spam filter's functionality and efficiency

Kerio MailServer includes several options of how to monitor spam filter's functionality. Standard tools available in the *Kerio Administration Console* are sufficient for this purpose:

Spam Filter statistics

Kerio MailServer maintain spam filter's statistics. The statistics can be found in the *Status* → *Statistics* section (refer to chapter 21.6).

Spam filter's statistics enable find out the proportion of ham (legitimate email) and spam coming in *Kerio MailServer*. The statistics help you recognize whether individual antispam methods are set properly. It is apparent from the facts whether too much spam leaks in user mailboxes and whether too many legitimate messages are marked as spam.

The statistics covers the following items:

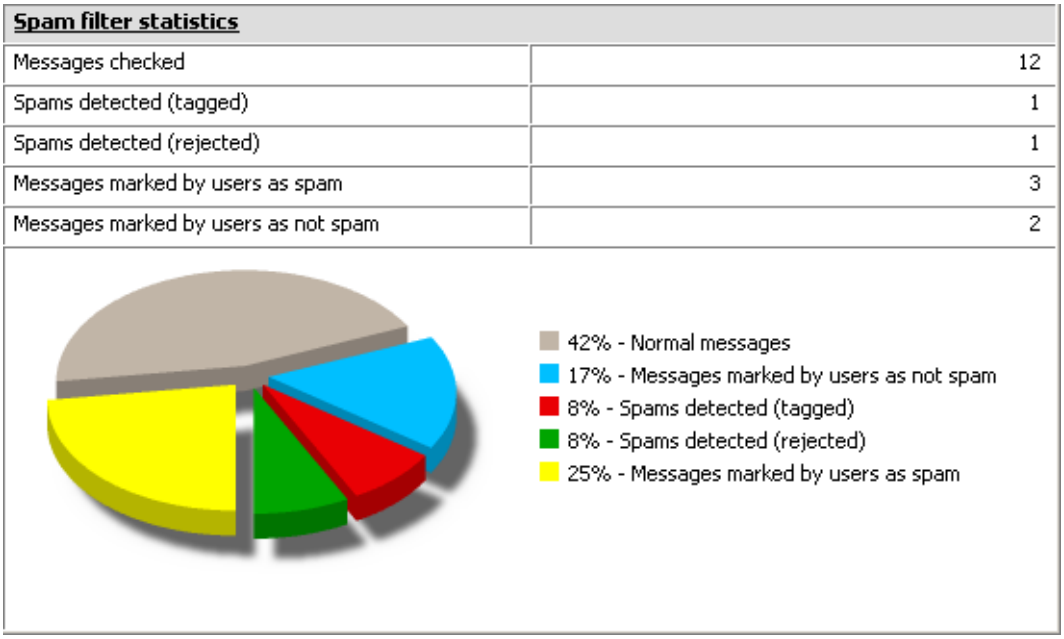

Figure 16.12 Spam Filter statistics

Messages checked
: Total number of all messages that have passed through the antispam filter (messages sent form whitelist domains, for example, are not counted since they are not tested).

Spams detected (tagged)
: All messages detected and tagged as spam.

Spams detected (rejected)
: All messages blocked by the spam filter.

Messages marked by users as spam
: All messages considered by the filter as not spam which were later marked as spam by users (manually, by clicking on *Spam* or by moving it to the *Spam* folder).

Messages marked by users as not spam
: Legitimate messages detected by the antispam filter improperly as spam— so called "false positives".

Graphical overviews

Kerio MailServer also uses traffic charts to trace certain values regarding spam email. There are several spam-related traffic charts which can be found in the *Status* → *Traffic Charts* section of the *Kerio Administration Console* (see chapter 21.5).

The following graphs focus on spam:

Connections/Rejected SMTP
The chart displays number of attempts of SMTP connection were rejected by the *Spam repellent* tool in certain time period.

Messages/Spam
With time dependence, the chart displays how large amount of spam is delivered to *Kerio MailServer* and when.

Logs

Problems that occur regarding the antispam filter might be solved with help of *Kerio MailServer's* logs. In detail, logs are focused in chapter 22.

The following logs might be helpful:

Spam
All messages marked as spam are recorded in this log (for details, see chapter 22.7).

Debug
Logging of particular information can be performed by this special log. Spam issues may be worked out by using of the following information:

- *Spam Filter* — the option logs spam rating of each message which passed through the *Kerio MailServer's* antispam filter.
- *SPF Record Lookup* — the option gathers information of *SPF* queries sent to SMTP servers. It can be used for solving problems with SPF check.
- *SpamAssassin Processing* — the option enables tracing of processes occurred during *SpamAssassin* antispam tests.

To learn where and how to set logging of particular information in the *Debug* log, refer to chapter 22.8.

Chapter 17

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.

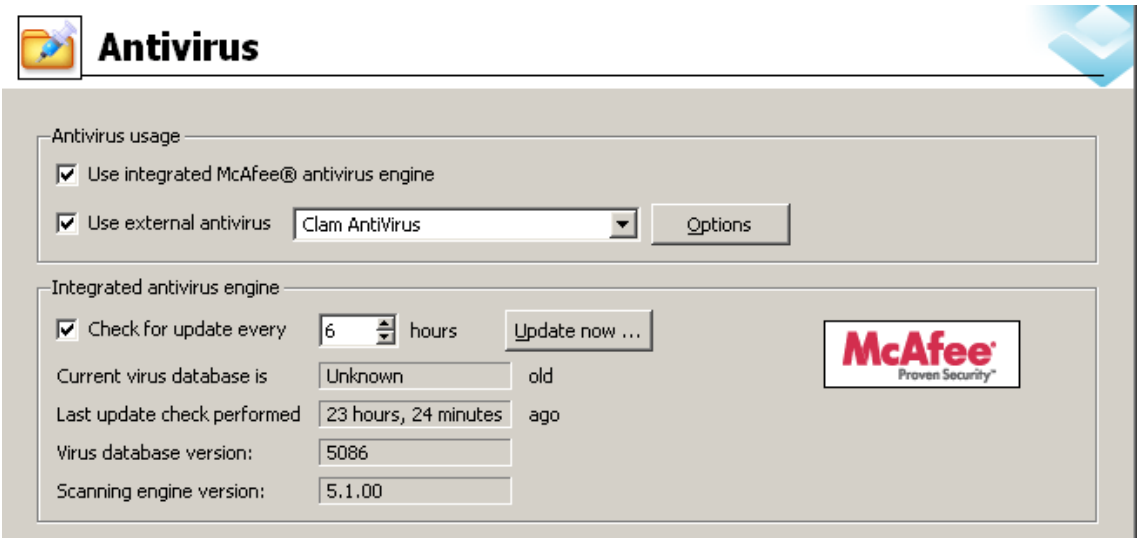

Figure 17.1 Antivirus

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.

17.1 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 22.4).

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 22.4).

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 ...

The time that has elapsed since the last successful update of the virus database (with an accuracy of minutes).

Last update check performed

The time elapsed from the last successful update attempt. The fact whether a new version has been available on the server is irrelevant.

Warning: 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.

17.2 Choosing an external module for an antivirus program

Parameters for antivirus control are set in the *Content Filter* → *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 *Kerio 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 of 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 28.2), 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).

17.3 Examples of configuration of external antivirus modules

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..

Clam AntiVirus

Kerio MailServer supports *Clam AV* for Linux, Mac OS X and Windows.

Warning: Clam AV is available in two basic versions for Windows, but only *Clam AV for Windows* can be used (aka *ClamAV-win32*). Version *ClamWin Antivirus* is not supported by *Kerio MailServer*). *Clam AV for Windows* can be downloaded for free at http://www.sosdg.org/.

To make cooperation of *Clam AV* with *Kerio MailServer* function properly, the following requirements must be met:

- Communication of the antivirus and *Kerio MailServer* must be maintained over a network socket (this can be set in the antivirus configuration file).
- In the *Kerio MailServer's* administration console (*Configuration* → *Content Filter* → *Antivirus* → *the Options button*) in the antivirus settings (see figure 17.2), set an IP address and a port for traffic. If *Clam AV* is running on the same computer as *Kerio MailServer*, it is not necessary to change default settings.
- On Linux operating systems, *Kerio MailServer* is always running under the root user. If *Clam AV* is installed on the same computer as *Kerio MailServer* but it is running under another user, the *UseStreamOutLocalhost* item in the antivirus configuration in the administration console (*Configuration* → *Content Filter* → *Antivirus* → *the Options button*) must be set to the 1 value.

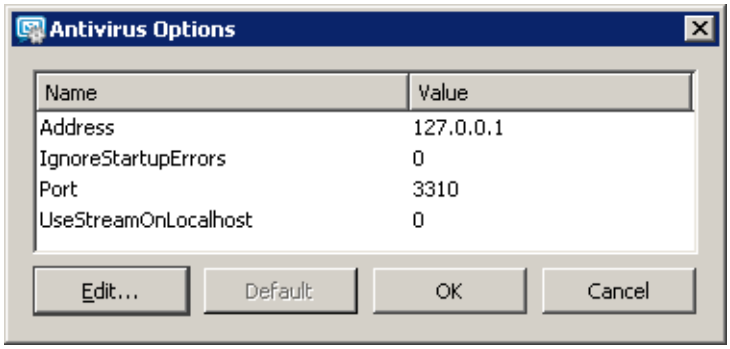

Figure 17.2 Options for Clam AntiVirus

Note: Updates of the virus database must be set by using the *Freshclam* utility.

17.4 Server responses to detection of a virus or a damaged/encrypted attachment

The *Kerio MailServer* administrator can set a detailed course of action for the mailserver if a virus or a damaged attachment is detected in an email. Use the *Action* tab to set this.

Figure 17.3 Server responses to detection of a virus or a damaged/encrypted 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.

17.5 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.

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.

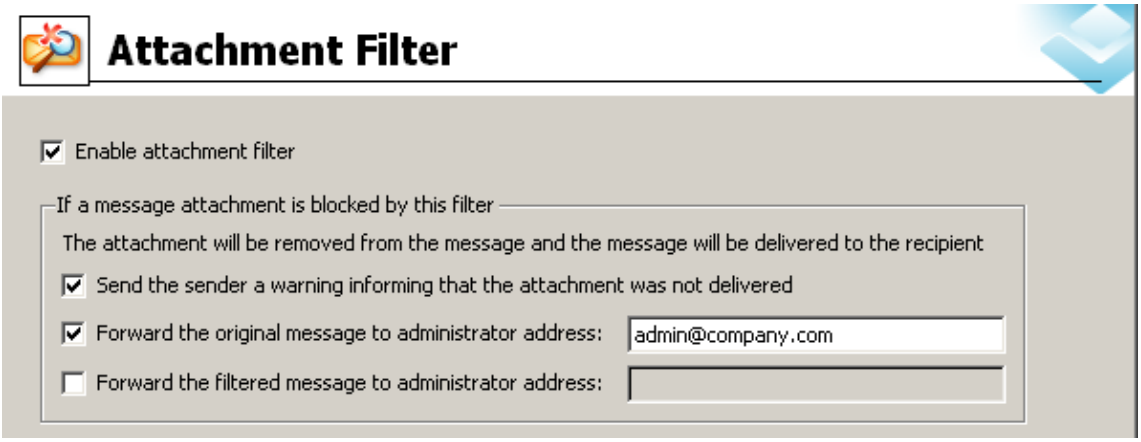

Figure 17.4 Attachment Filter tab

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.

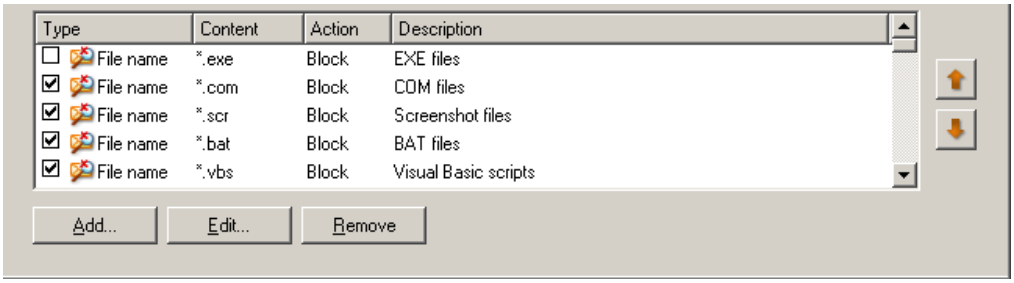

Figure 17.5 List of filters

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 file type 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.

17.6 Antivirus control statistics

Kerio MailServer maintains statistics of virus detection in email. The statistics can be found in the *Status* → *Statistics* section (refer to chapter 21.6).

Statistics of the antivirus control enable monitor how many infected messages come in *Kerio MailServer*.

The statistics covers the following items:

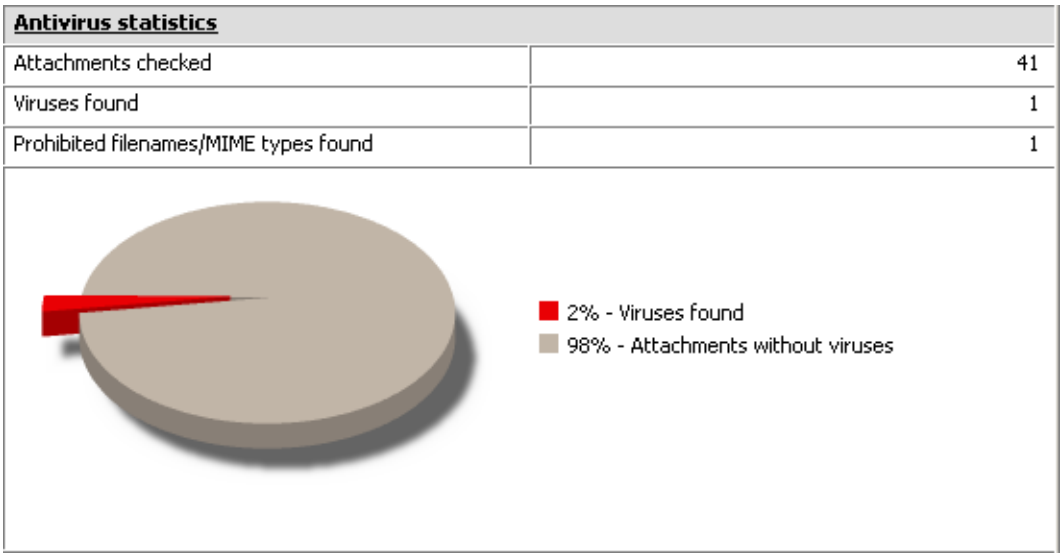

Figure 17.6 Spam Filter statistics

- *Attachments checked* — total number of email messages with attachments checked by an antivirus.
- *Viruses found* — number of detected viruses.
- *Prohibited filenames/MIME types found* — total number of forbidden attachments (see chapter 17.5).

Note: Statistics are created since the last startup of the server.

Chapter 18

Email archiving and backup

18.1 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 7.2).

To configure backups, go to the *Archiving* tab under *Configuration* → *Archiving & Backup*:

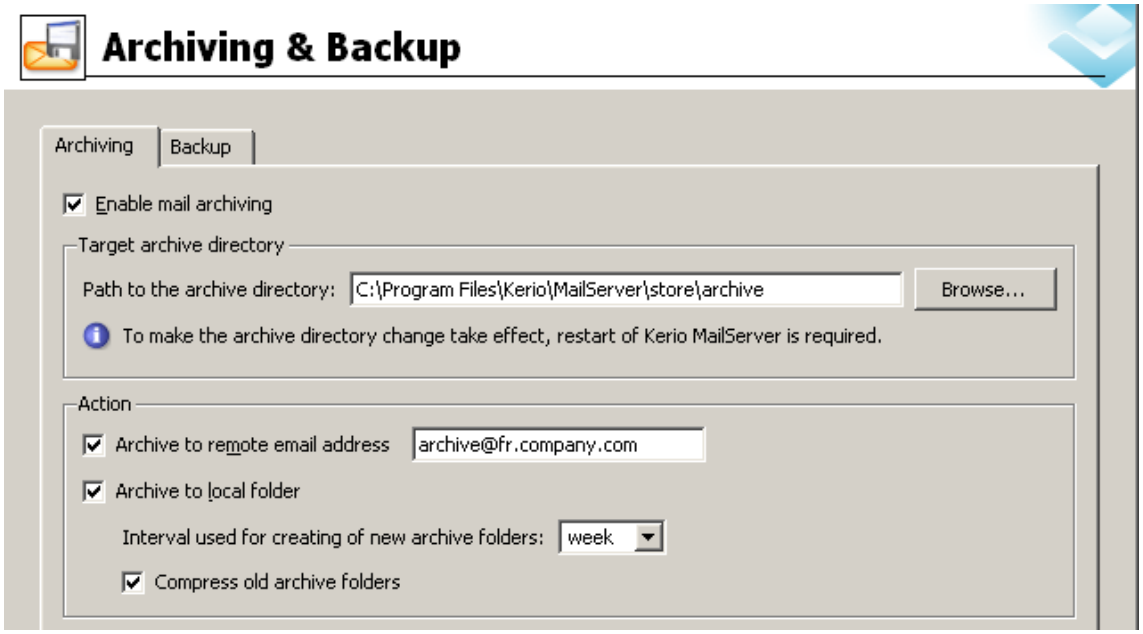

Figure 18.1 Archiving tab

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). By technical reasons, it is necessary to locate the archiving directory locally (i.e. on the server where *Kerio MailServer* is running).
Warning: UNC path is not allowed as path specification.

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 includes year and week number. The week number count starts on January 1 of the particular year. This implies that the count does not necessarily match with the usual calendar week count (if January 1 is included in the 52nd week, the week counts may collide). 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.

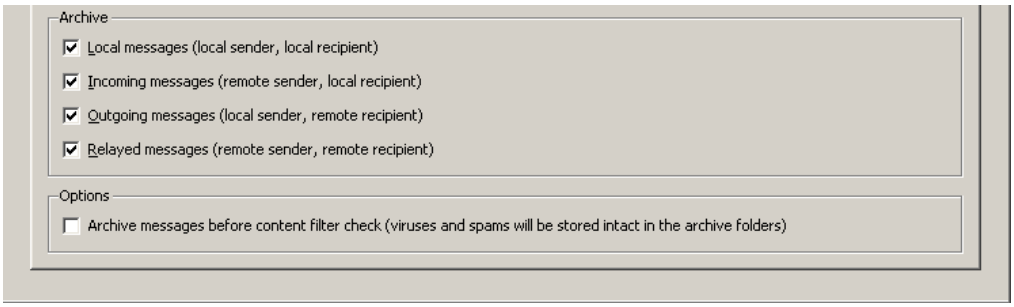

Figure 18.2 Selection of message types to be archived

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 13.1). 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* 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.

Viewing of 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*).

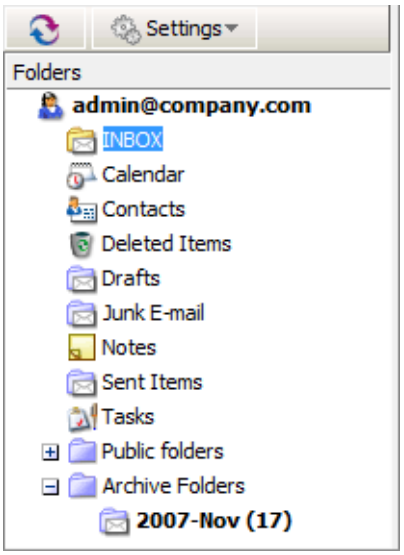

Figure 18.3 Archive folders in the Kerio WebMail interface

Archive folders can also be made available for other users. The sharing is the same as for other folder types. 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.

18.2 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* → *Archiving & Backup*:

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` and `mailserver.cfg` files.

If you do not wish to use *Kerio MailServer's* backup functions, disable the *Enable message store and recovery backup* option. If you remove all items in the backup

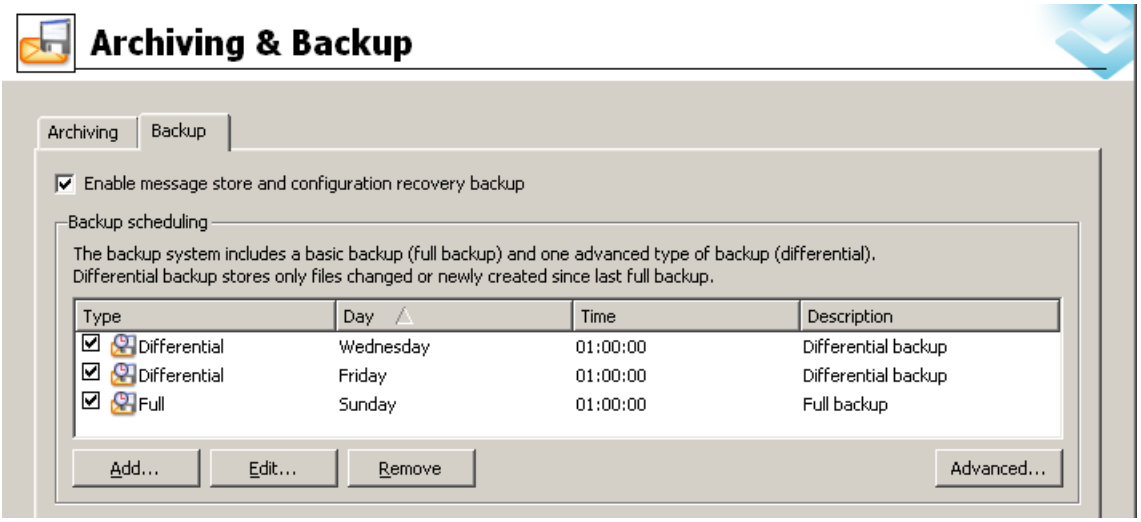

Figure 18.4 Backup of user folders

schedule and leave the option active, the default backup schedule is downloaded and applied upon a *Kerio MailServer's* restart.

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 28.2.
- 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 18.5) that includes the following setting options:

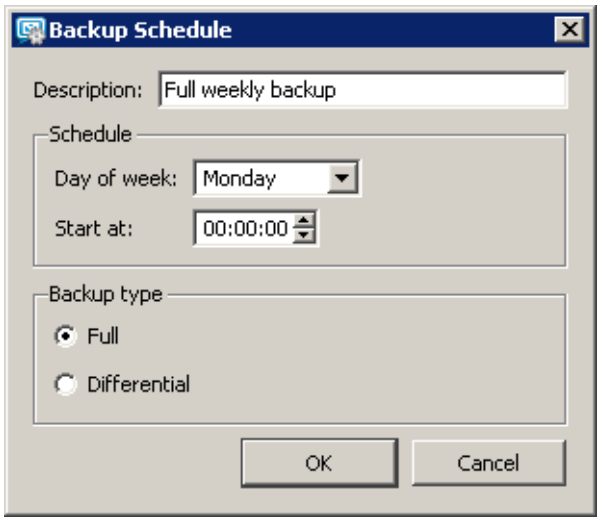

Figure 18.5 A backup task

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 18.6):

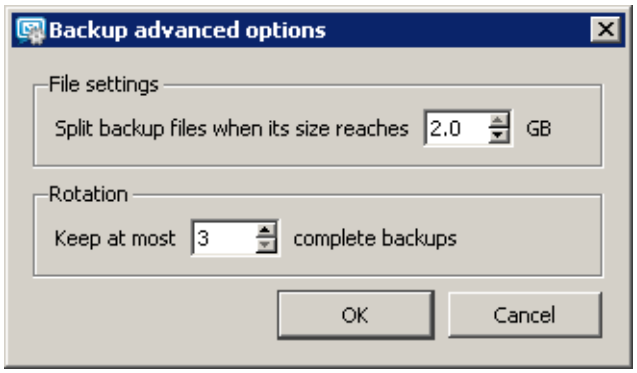

Figure 18.6 Backup advanced options

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.
If *Kerio MailServer* is running on Windows, the path must be specified as UNC (see figure 18.7).

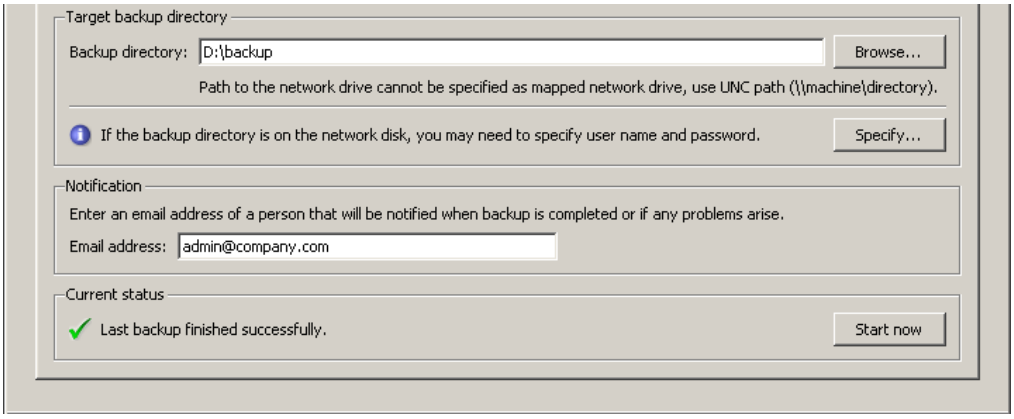

Figure 18.7 Backup directory specification

If *Kerio MailServer* is running on Linux or Mac OS, the following options are allowed:

- Connect the backup server as a directory and specify the path to this directory in the *Backup Directory* entry. Here is an example of a result:

  `/mnt/server-backup`

- Save the backup in a local directory and then, send it to the server (e.g. by using the `rsync` synchronization utility). Here is an example of a result:

  `/backup/kms/backup`

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
  T220007Z — GMT timestamp (22:00:07);it always starts with T and ends with Z.
- Differential backup — `I20060106T220006Z.zip`
  I — differential backup
  2006 — year
  01 — month
  06 — day
  T220006Z — GMT timestamp (22:00:06);it always starts with T and ends with Z.
- Backup copy (manual back up startup) — `C20060117T084217Z.zip`
  2006 — year
  01 — month
  17 — day
  T084217Z — GMT timestamp (08:42:17);it always starts with T and ends with Z.

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 username 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*.

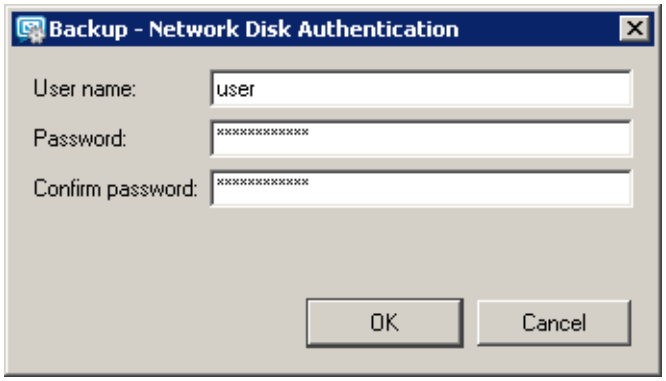

Figure 18.8 Network disk authentication

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>
```

Warning: On Mac OS X and Linux it is necessary to enter a command on the following format, unless having already been introduced in the file of the `path` system variable:

```
./kmsrecover <directory_name>|<file_name>
```

This means that it is necessary to add the `./` string before the utility name that will inform the system that the command to be used is in the current directory.

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:

Windows

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 disk

   `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"
```

Mac OS X

The recovery is performed on a host using *Mac OS X*. 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 of the same computer where the configuration directory, and the backup directory is located on an exchangeable disk. For backup recovery, use the most recent full backup.
Conditions:

1. The configuration data is stored under

   `/usr/local/kerio/mailserver`

2. The *store* directory is located in

   `/store`

3. For security purposes, the backup directory is stored on the removable disk

   `/Volume/backup`

Solution:
The command must be run from the directory where *Kerio MailServer* is installed. Therefore, it is necessary to go to the directory:

```
/usr/local/kerio/mailserver
```

We want to recover the last complete backup (the most recent full and differential backups or the most recent backup copy). Now, the command pattern depends on the fact whether the path to the *Kerio MailServer* directory is included in the path variable or not. If the path is not set there, the command will be as follows:

```
./kmsrecover /Volume/backup
```

Otherwise, it will be like this:

```
kmsrecover /Volume/backup
```

The `kmsrecover` detects the path to the store (`/store`) automatically in the *Kerio MailServer's* configuration file and uses it.

Troubleshooting

For cases when a problem regarding backups occurs and needs to be solved, *Kerio*

MailServer allows logging of backups:

1. In the *Kerio Administration Console*, go to the *Logs* section and select the *Debug* log.
2. Right-click on the log pane to open a context menu, and select *Messages*.
3. In the *Logging messages* dialog box, select *Store Backup*.
4. Confirm changes by OK.

Once your problems are solved, it is recommended to disable the logging.

Chapter 19

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 6) 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.

19.1 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.

19.2 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`
  only the `Contacts` folder of user `jsmith@company.com` will be scanned
- `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.

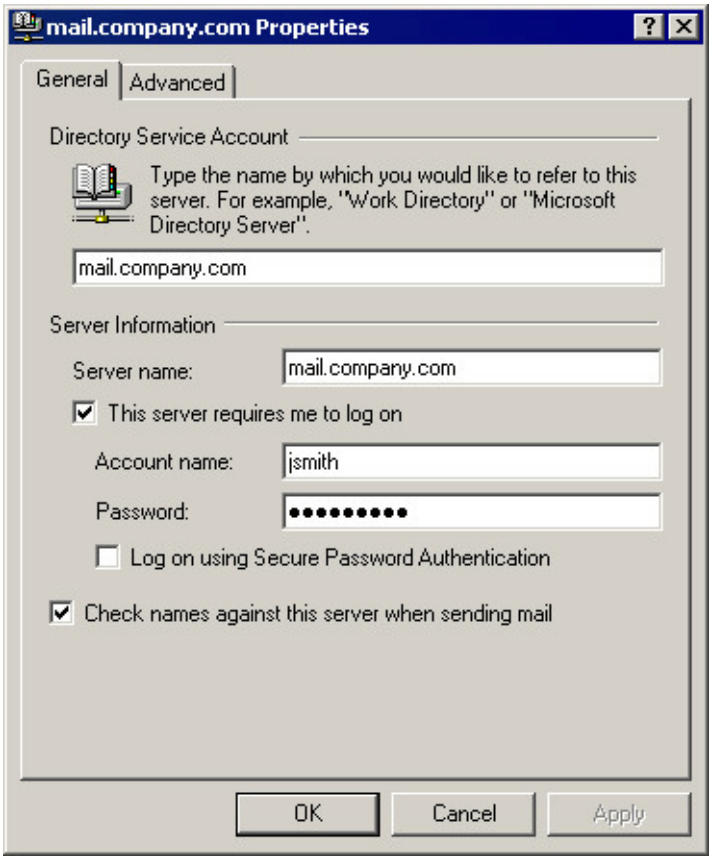

Figure 19.1 LDAP server settings — General tab

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

It is necessary that this option is checked since the LDAP server in *Kerio MailServer* does not allow anonymous access.

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/NTML). 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 *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:

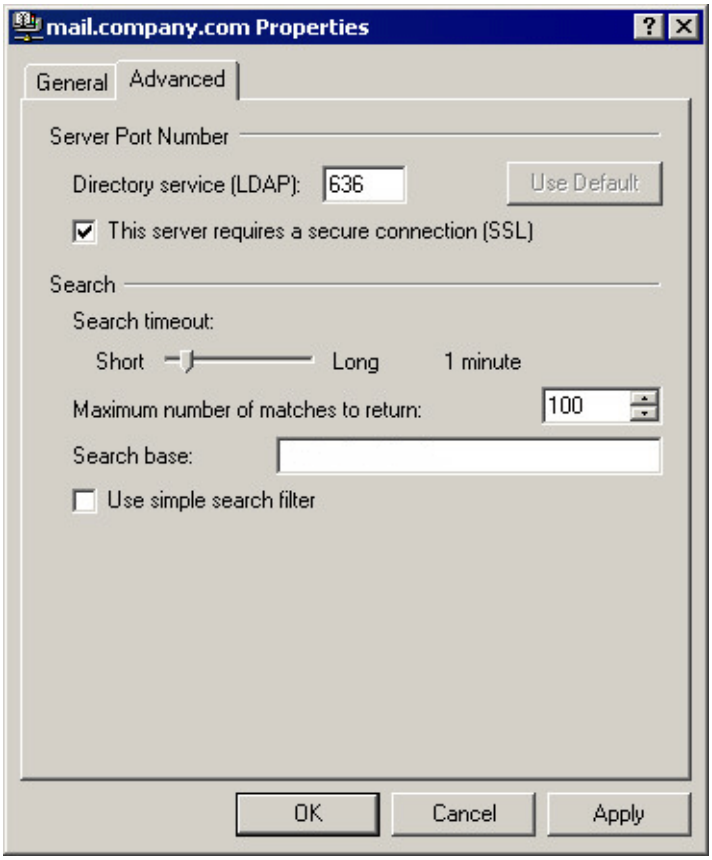

Figure 19.2 LDAP server settings — Advanced tab

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 6) or according to your security policy (see chapter 15.6).

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 20

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.

If any problems regarding mailing lists occur, the *Debug* log may be helpful (see chapter 22.8). To obtain appropriate information, enable the *Mailing Lists Processing* log.

20.1 User Classification

Users of mailing lists may have the following roles:

Administrator

User with *Kerio MailServer* administration rights (read/write access — see chapter 13.1). *Kerio Administration Console* administrators create all mailing lists and define their parameters (e.g. moderators, policies, etc.). For details, see chapter 20.2).

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.)

20.2 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

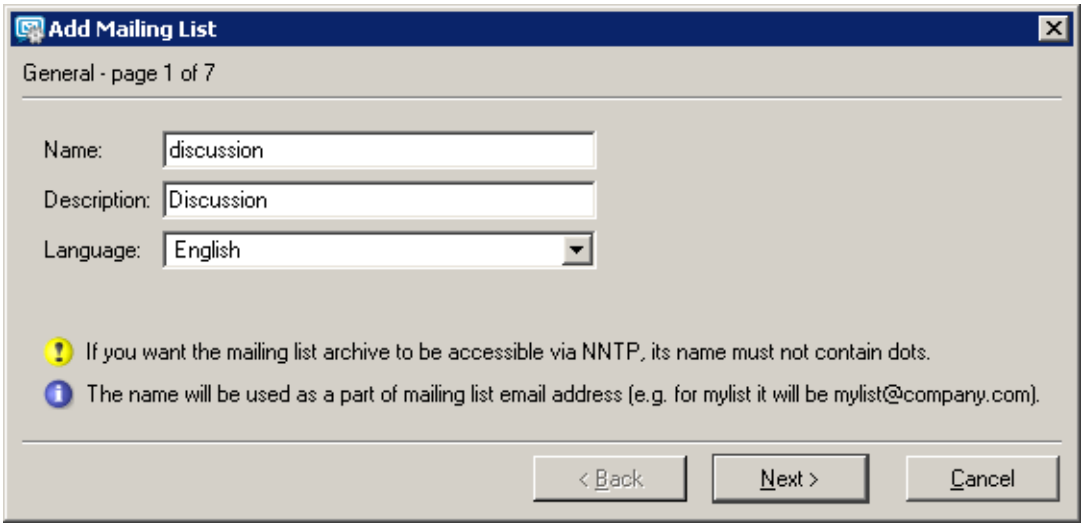

Figure 20.1 Creating a mailing list — basic parameters

suffix is used to subscribe mailing lists). For details, see chapter 20.7, 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 messages will not be delivered to the mailing list at all.

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 anew language report version.

Comment

In step two, any text can be entered that will be delivered to every member newly subscribed in the mailing list (upper entry). In the lower part, text that will be added as a footer to each email sent to the mailing list can be specified. These fields may be left blank.

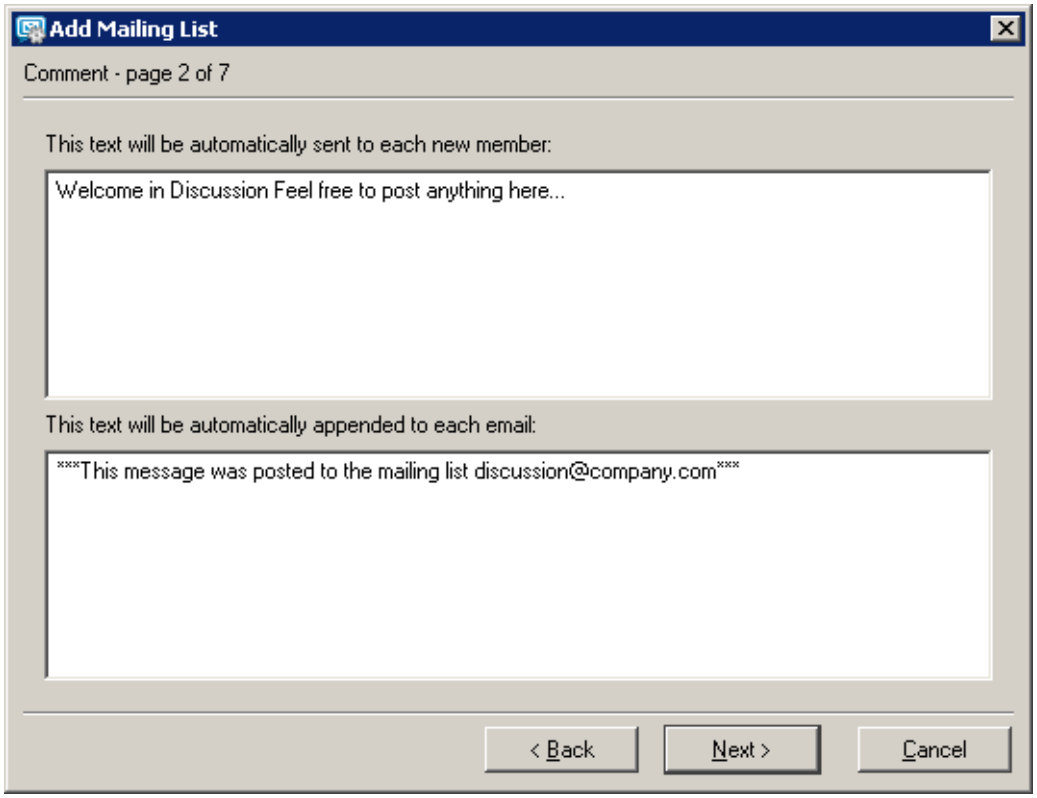

Figure 20.2 Creating a mailing list — comments

Note: A welcome message is sent only to those new members that have subscribed to the list via email (for details, see section sect-mlistusage"/>). 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 20.7.

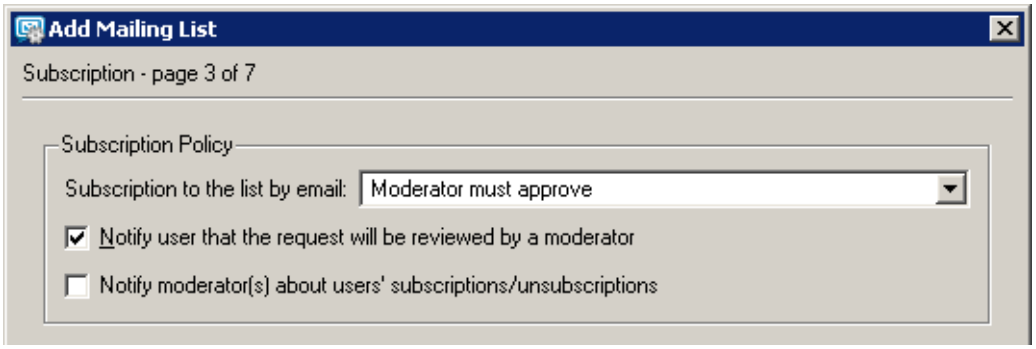

Figure 20.3 Creating a mailing list — subscription

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.

20.3 Posting rules

In step four, rules for posting messages to the mailing list and for automatic modifications of the messages can be defined.

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.

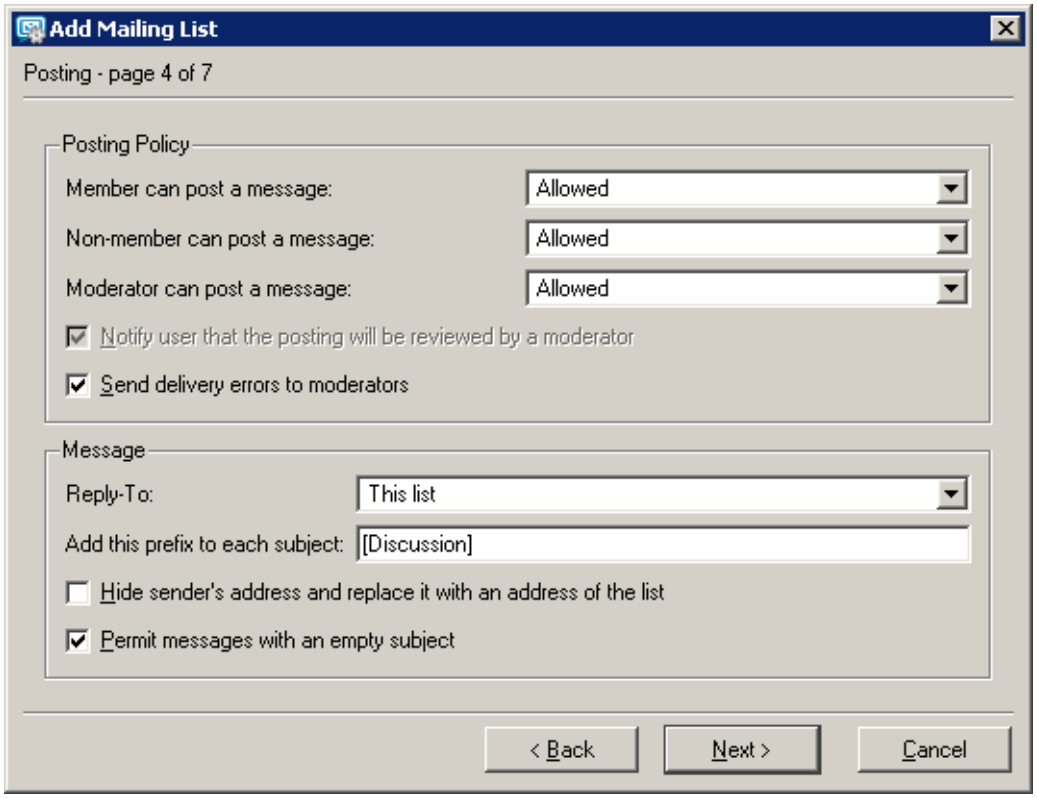

Figure 20.4 Creating a mailing list — posting rules

- *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 to 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.
- *Sender + this list* — this setting enables delivery of email replies to users who are not members of the mailing lists. Two situations may arise:

  1. The user is a member of the mailing list — the reply will be delivered to the

mailing list's address. The sender will obtain only one copy of the reply.

2. The sender is not a member of the mailing list — the reply will be delivered both to the mailing list and to the sender's mailbox. Otherwise, the sender (non-member) would not receive the reply at all.

As implied, the option is beneficial if the mailing list is available both to members and non-members.

Note: Do not combine this option with the *Hide sender's address and replace it with an address on the list* option. The combination would be pointless and *Kerio MailServer* would not allow saving it.

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.

20.4 Moderators and Members

In these two sections, moderators and mailing list members can be defined. The same method is used to add moderators and members.

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).

New moderators/members can be added manually or by selection from the list (see figure 20.5):

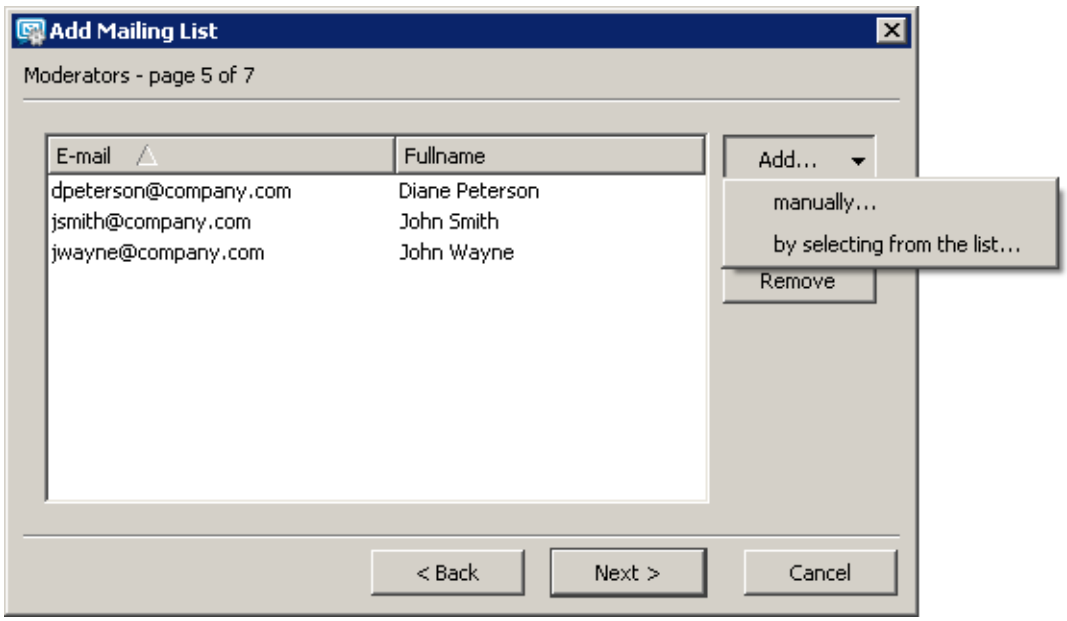

Figure 20.5 Creating a mailing list — adding the mailing list moderators

Adding moderators/members manually

To add a moderator/member manually, follow these instructions:

Figure 20.6 Adding moderators/members manually

1. Click on *Add*.
2. Select *manually...*
3. A dialog is opened where you can specify email address and user's full name (this item is optional). Users that belong to a local domain can be found using the *Find user* dialog which can be opened by the *Select* button.
4. Click *OK*. to confirm changes.

Adding a moderator/member by selection from the list

This option is recommended in cases where there are multiple users added with their accounts in a local domain.

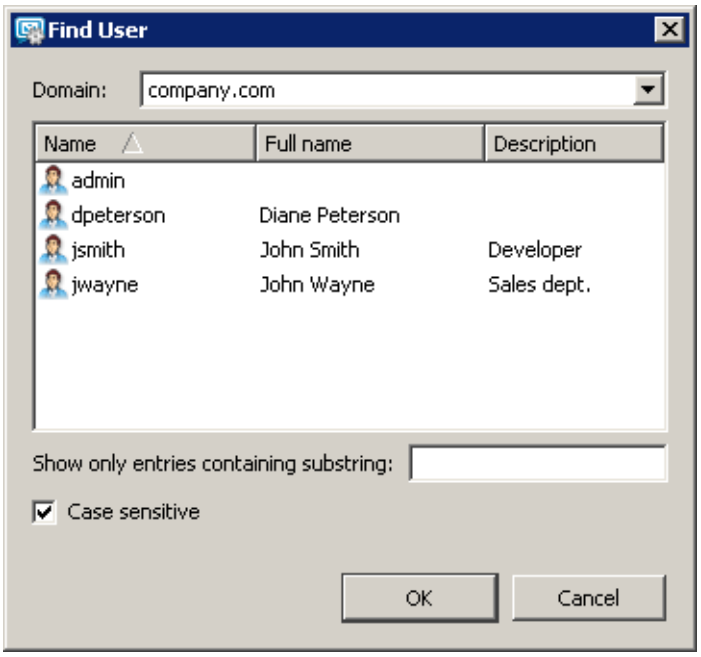

Figure 20.7 Adding a moderator/member by selection from the list

To add a mailing list moderator/member by selection from the list, follow these instructions:

1. Click on *Add*.
2. Select *by selecting from the list...* (see figure 20.5).
3. The *Find user* dialog is opened which includes list of domains and users (see figure 20.7). Multiple users can be selected for a domain by using the default `Ctrl` key (where *Kerio MailServer* is running on Mac OS, use the `Command` key).

   If the user you are searching cannot be found or the user list is to long, the *Show only entries containing substring* entry can be used.
4. Click *OK*. to confirm changes.

Importing users from a CSV file

As already mentioned, even users that have not accounts in *Kerio MailServer* can became members of mailing lists. Users can subscribe to mailing lists by themselves by sending a subscription email message or they can be added manually by the administrator or they can be imported from a file (the latest option may be helpful especially when multiple users are added).

The following technical conditions must be met to enable importing from files:

1. The file including the users must be saved in CSV format (such files can be created in any spreadsheet program).

2. Commas (,) or semicolons (;) must be used as data separators.

3. Headlines of individual columns must correspond with *Kerio MailServer's* items. The following items are supported:

   - Email — user's email address. Required.
   - FullName — user's full name. Optional.

Email	FullName
mking@yahoo.com	Mary King
afieldfare@mymail.com	Allan Fieldfare
opossum@mailer.com	Oliver Possum
etea@hotmail.com	Elizabeth Tea

Table 20.1 Example of a CSV file

Columns can be ordered as wish, there are no rules to be followed. It is also possible to specify only Email. Specification of FullName is optional.

Once the file is properly created and saved, you may continue creating the mailing list or, if the mailing list has already been created and saved, you can open it by clicking on the *Edit* button and switch to the *Members* tab:

1. Click on *Add* and in the button's menu select the *by importing from CSV file* (see figure 20.8).

2. This opens a dialog (see figure 20.9) where file path and encoding type which will be used for saving (generally, the default *Local (System)* option can be kept) can be set.

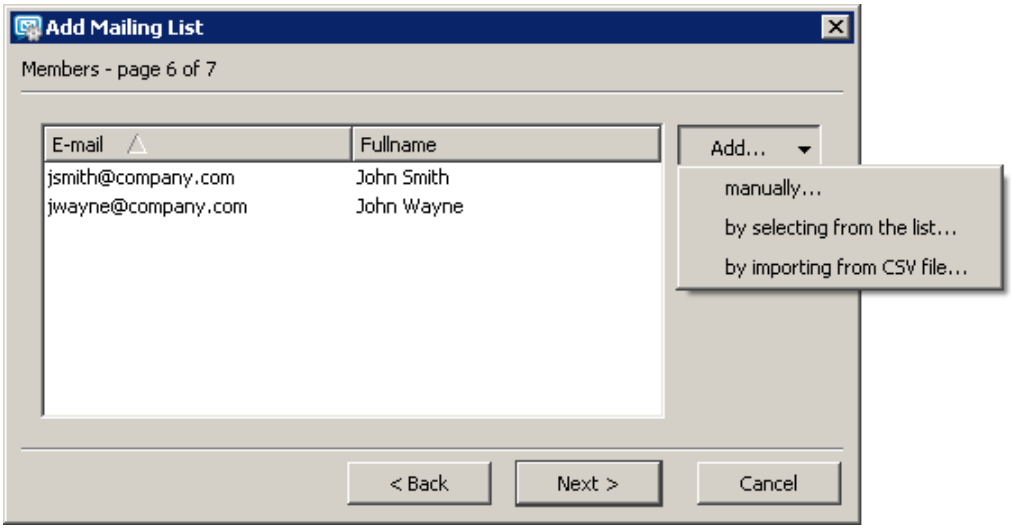

Figure 20.8 Creating a mailing list — adding members to a mailing list

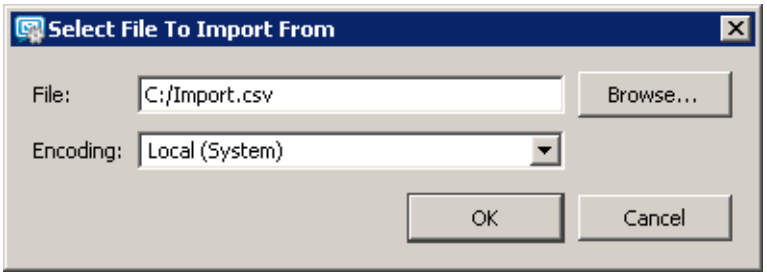

Figure 20.9 Import from a file — file selection

3. Click on *OK* to copy users to the mailing list's user list.

   If problems occur regarding the upload, it might be caused by the following reasons:

   - The file is not saved in the CSV format.
   - Columns in the file are not labeled correctly. CSV file needs to include a line with captions including column names, otherwise *Kerio MailServer* cannot read the data.

     Correct version:

     ```
     Email;FullName
     psycho@yahoo.com;Peter Sycho
     mint@email.com;Maude Int
     ```

     Wrong version:

     ```
     psycho@yahoo.com;Peter Sycho
     mint@email.com;Maude Int
     ```
   - Another separator than comma (,) or semicolon (;) is used as data separator.

20.5 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.

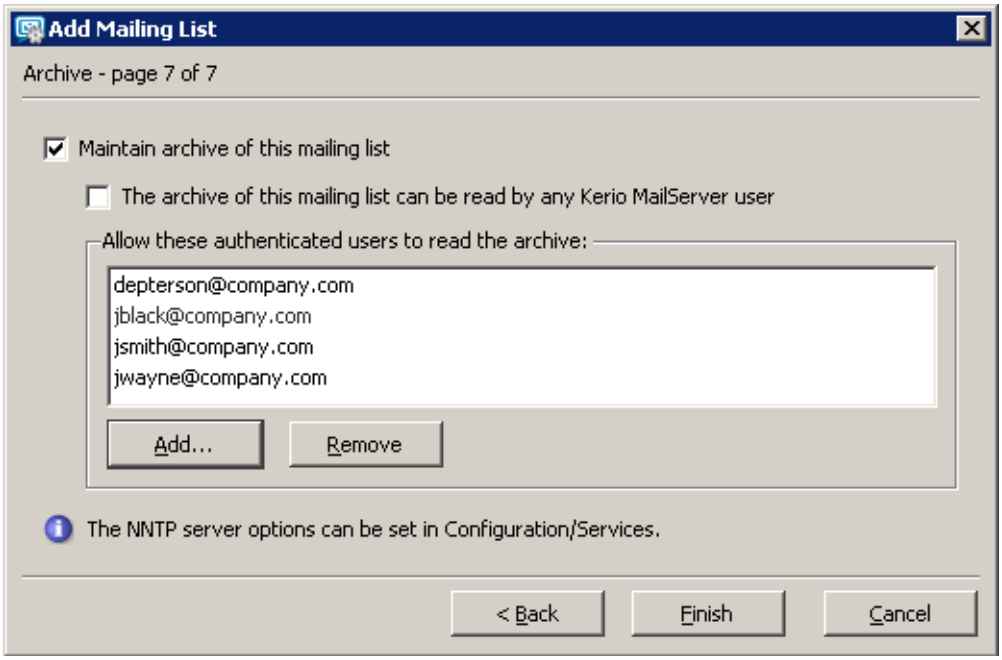

Figure 20.10 Creating a mailing list — maintain archiving

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 6), any user can read the archive (even if they have no account in *Kerio MailServer*).

20.6 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. `de` for German, `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.

20.7 How to use Mailing Lists

Member Subscription/Unsubscription

If allowed by the list policy (see chapter 20.2), 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 20.2) 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 21

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 22.
- 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.

21.1 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 8 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.

In addition to message queue, the tab includes also statistical data regarding current number of messages in the queue and their total size.

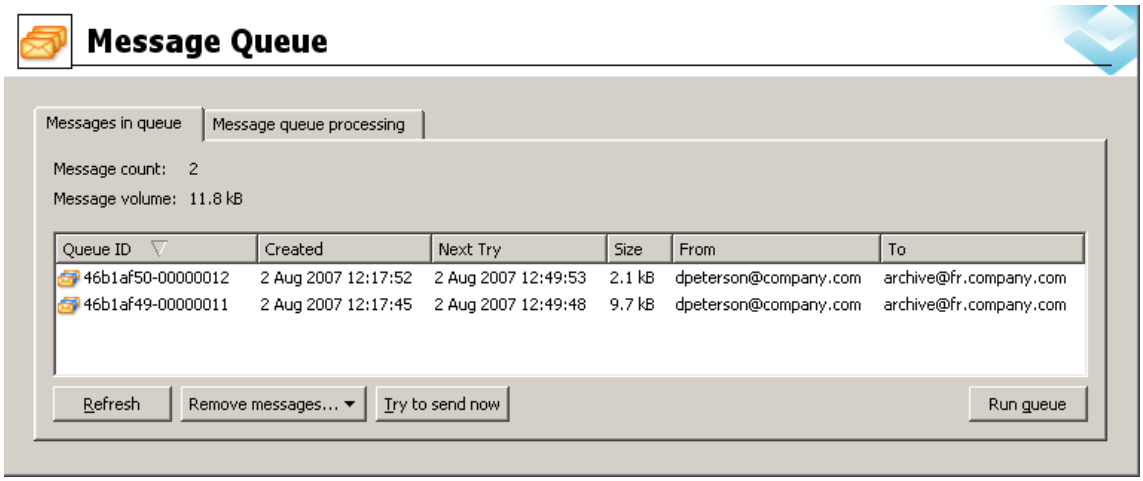

Figure 21.1 Messages in queue

Each line of this window contains information about one message in the queue. The columns contain the following information:

ID queues
: 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 15.2). *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.

21.2 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 *32*).

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.).

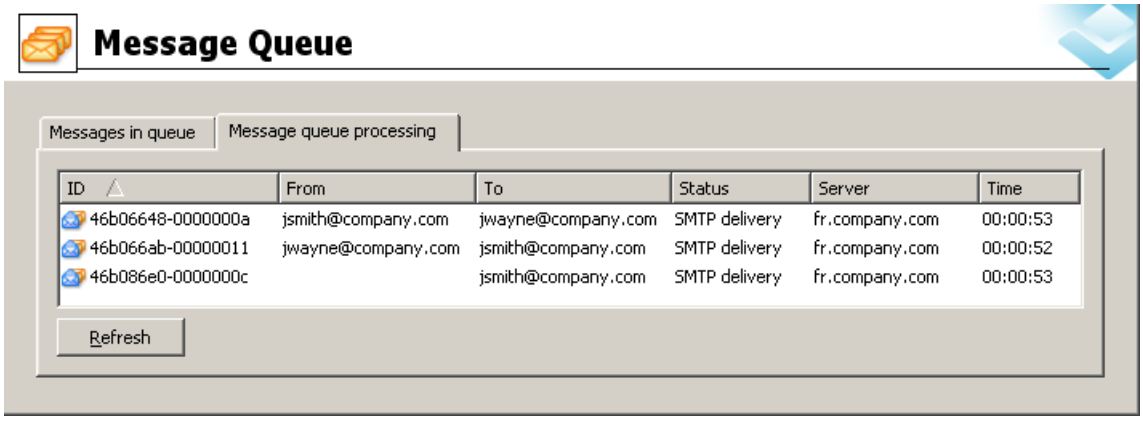

Figure 21.2 Message queue processing

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.

21.3 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:

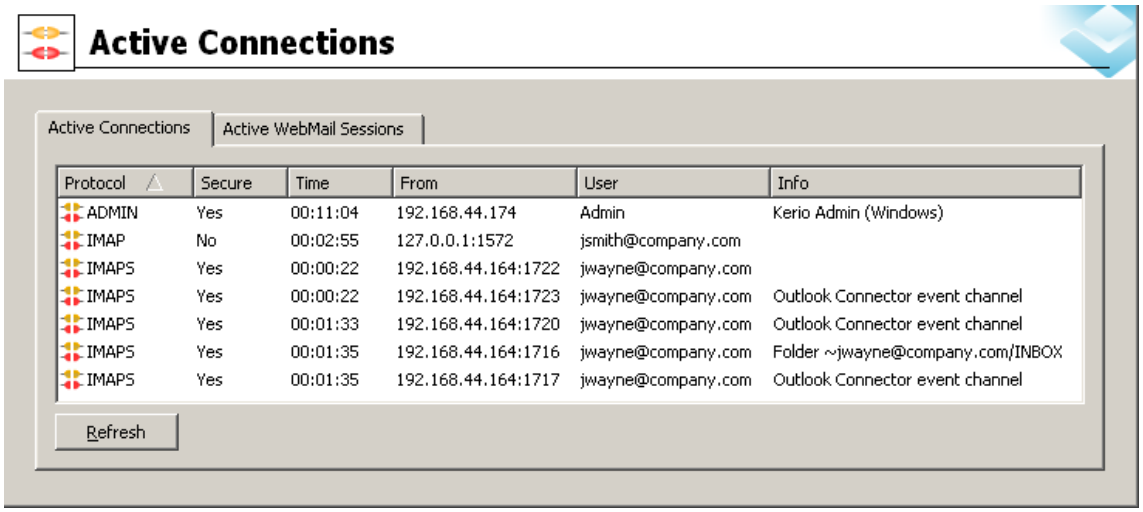

Figure 21.3 Active Connections

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 15.6). 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.

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).

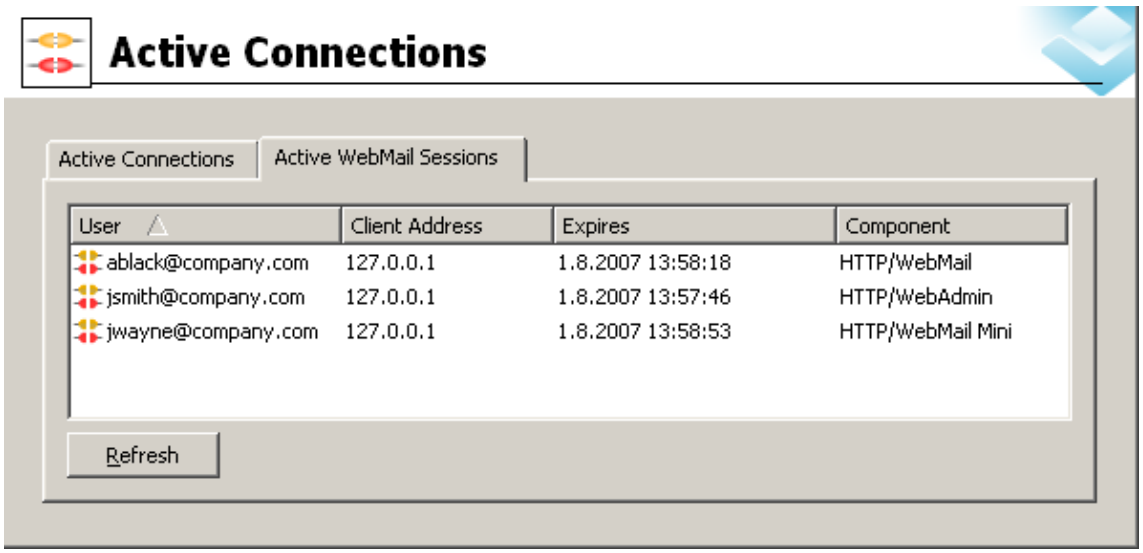

Figure 21.4 Active WebMail Sessions

21.4 Opened Folders

The *Status* → *Opened Folders* include all users who have any folders open in their email clients.

This section provides the following information:

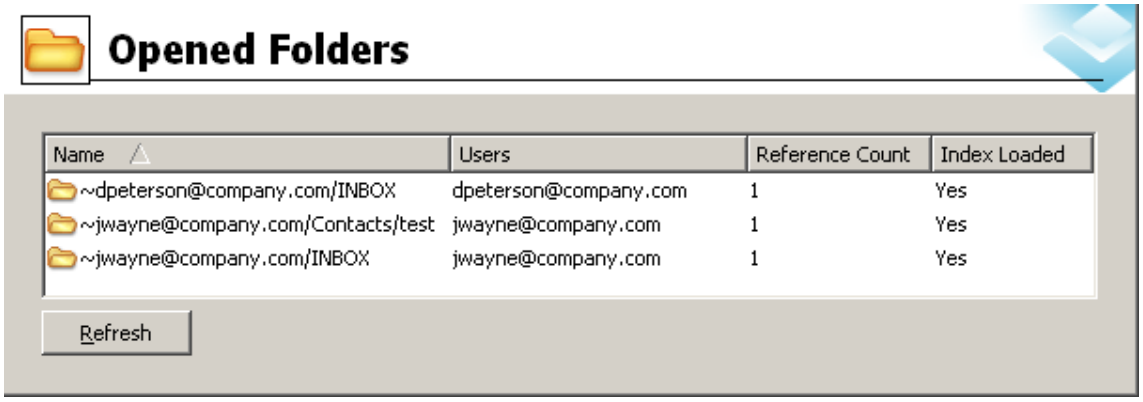

Figure 21.5 Opened Folders

Name

Name of the user folder following the `~user_name@domain/folder name` pattern

User accounts

All users whose folder is currently opened are involved. Multiple users can be listed in case of public or shared folders.

Reference count

Total number of users whose folder is currently opened. Multiple users can be listed in case of public or shared folders. It is also possible that a folder is opened more than once by a user.

Index loaded

This item informs if the `index.fld` file has been uploaded by the server. This file allows various additional information display properly (flags, read-unread information, etc.).

You can use the *Refresh* button to manually refresh the page listing open folders.

Note: It is also possible to set an interval for automatic refreshing. These settings can be performed in the context menu (right click on the pane to open the menu).

21.5 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.

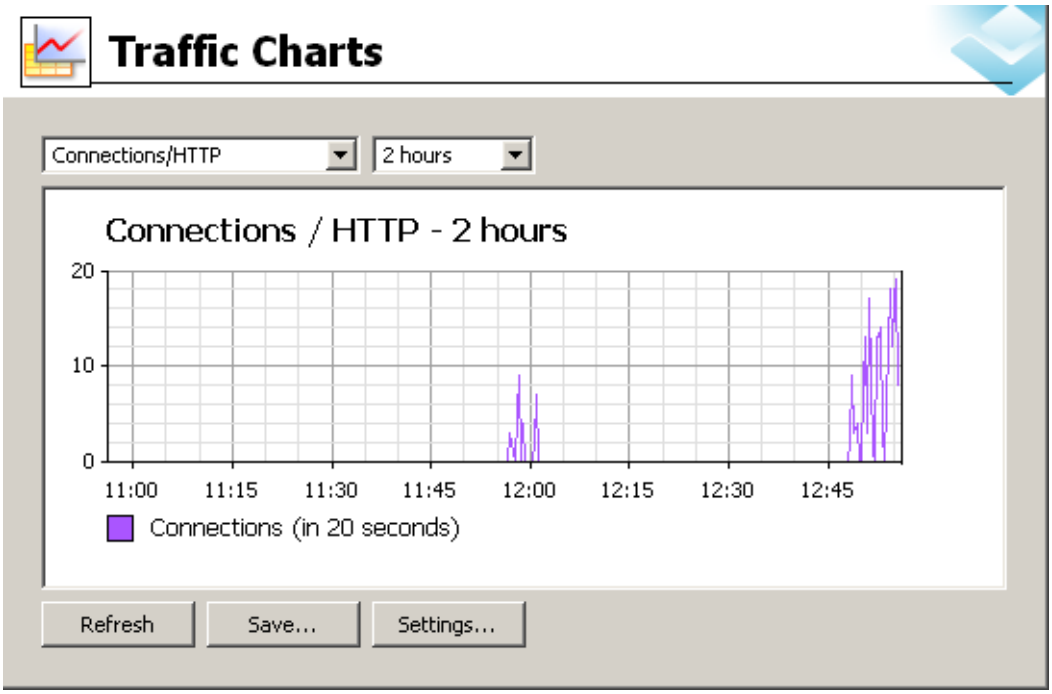

Figure 21.6 Traffic Charts

The graph allows the following parameter settings:

Monitored parameter

Use the first field to choose the monitored parameter:

- *Connections / HTTP* — the number of connections to the *HTTP* service
- *Connections/IMAP* — the number of connections to the *IMAP* service
- *Connections / LDAP* — the number of connections to the *LDAP* service
- *Connections / NNTP* — the number of connections to the *NNTP* service
- *Connections / Outgoing SMTP* — the number of outgoing connections of the *SMTP* service
- *Connections / Rejected SMTP* — number of rejected connections to the *SMTP* service (connections blocked by the *Spammer repellent* filter)
- *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)
- *Messages / Spam* — number of messages marked as spam by the antispam filter

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 following buttons are available below the graph:

- To refresh the graph, click on *Refresh*.
- Click on the *Save* button provided below the graph to save the graph as PNG.
- The *Settings* button opens the dialog where the detailed settings of a chart can be defined.

  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.

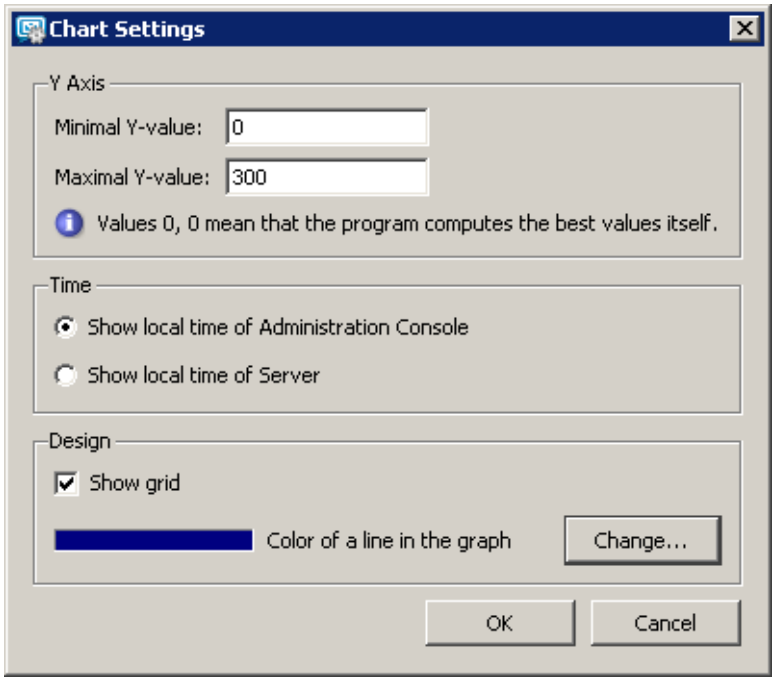

Figure 21.7 Chart Settings

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.

21.6 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.). In each table, data of the same topic are gathered.

The *Statistics* section includes several buttons:

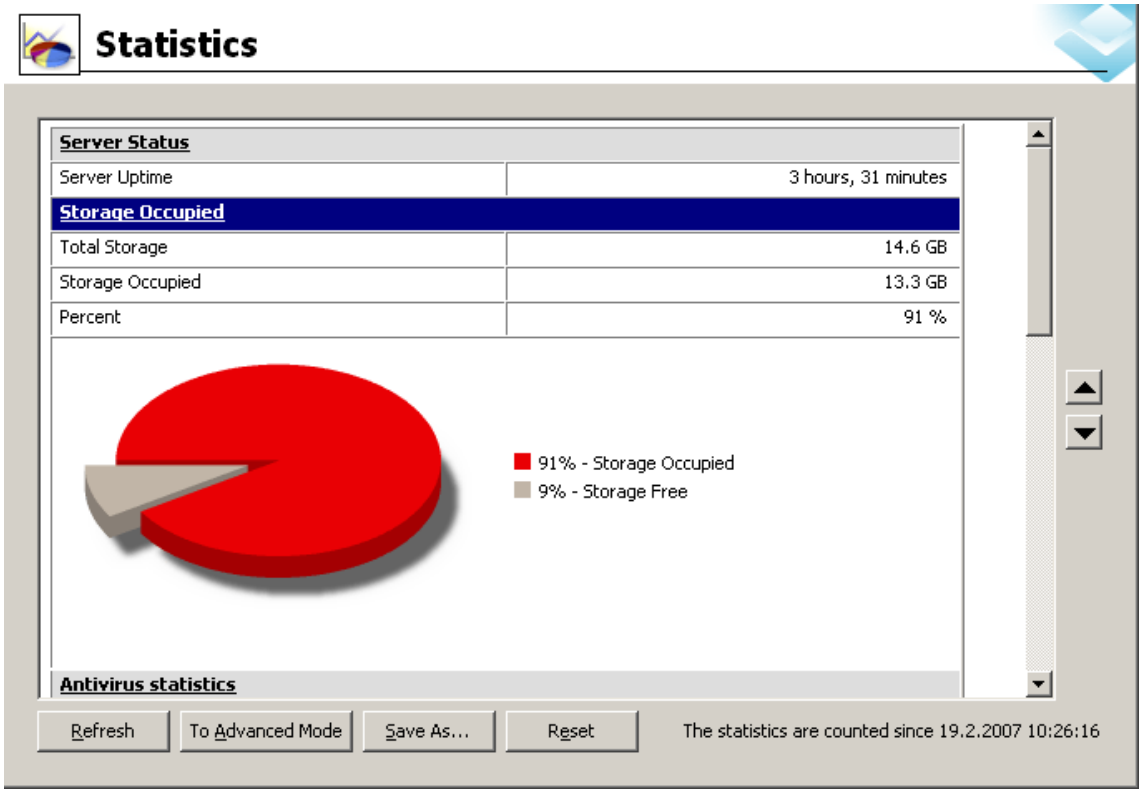

Figure 21.8 Statistics

Refresh

This button refreshes data provided in the statistics.

HINT: Individual statistics can be refreshed separately by clicking on their captions.

Basic/Advanced mode

The statistics work in two modes:

- *Basic mode* — this mode involves only four most popular statistics — *Server Status*, *Storage Occupied*, *Antivirus Statistics* and *Spam Filter Statistics*.
- *Advanced mode* — includes all statistics.

Save as

This button saves statistics in HTML format.

Reset

This button resets the counter. This implies that all statistics are set to zero and restarted upon clicking on this option.

Warning: All statistics are started upon the first startup of *Kerio MailServer* or the last reset of the statistics. In the lower right-hand corner in the *Statistics* section, date and time when the statistics were started is provided.

Chapter 22

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*).

22.1 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).

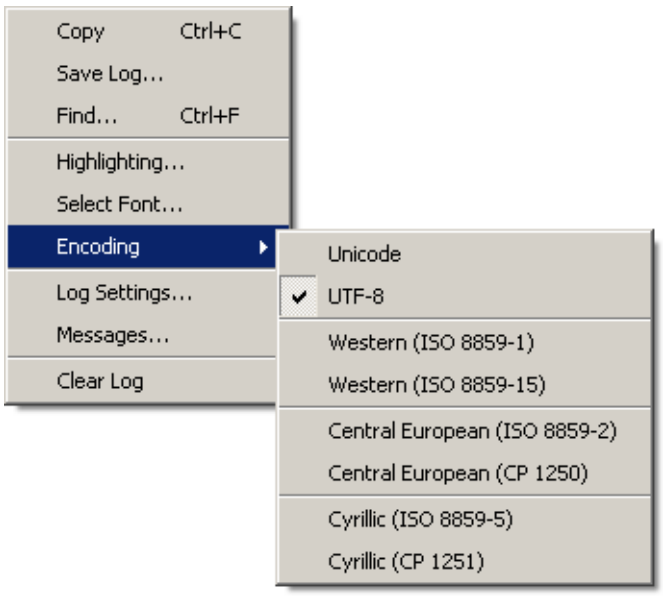

Figure 22.1 Context menu

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).

Save log

The *Save log* option enables saving of the entire log or its selected part in any file on the disk.

The dialog options are as follows:

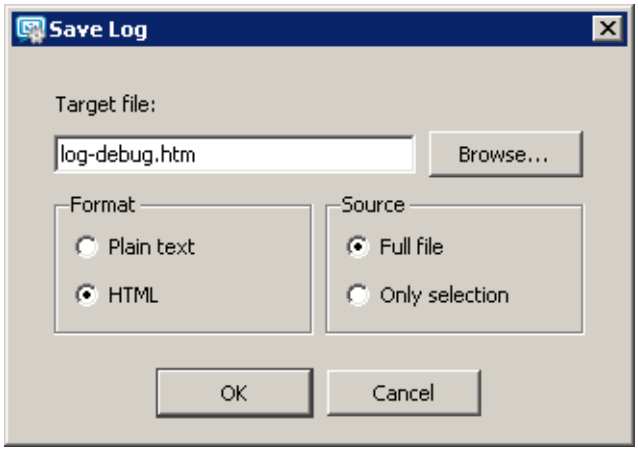

Figure 22.2 Save log

- *Format* — the log may be saved as in plain text (TXT) or in hypertext (HTML). If the log is saved in HTML, the encoding and colours (where highlighting was used) will be saved. If it is expected that the log would be processed by a script, it might be better to save it in plain text.
- *Source* — the option enables saving of the entire log or a selected part of the text.
  The *Only selection* option is not active by default. Once a part of the text in the log is selected by the pointer, the option becomes active and the selected text can be saved.

Find

Use this option to find a particular log row. Insert search criteria into the *Find* entry (words, numerals, characters).

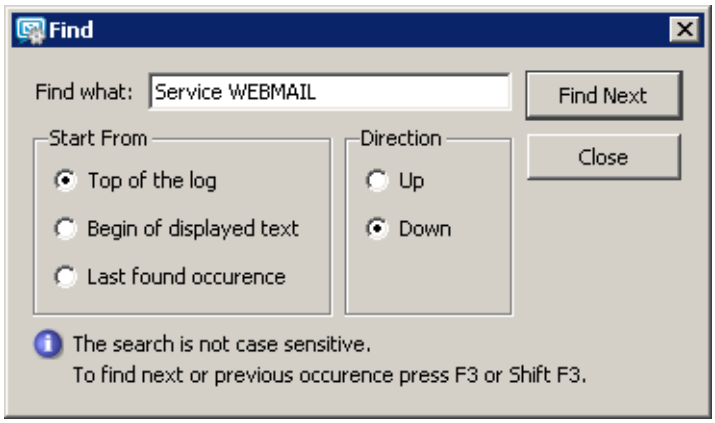

Figure 22.3 Search

- *Start from* — text can be scanned either from the start of the log or from the start of the selected text (only text displayed in the window is scanned) or from the last found occurrence of the string.
- *Direction* — set whether the log will be scanned upwards or downwards (*Up*, *Down*).

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.

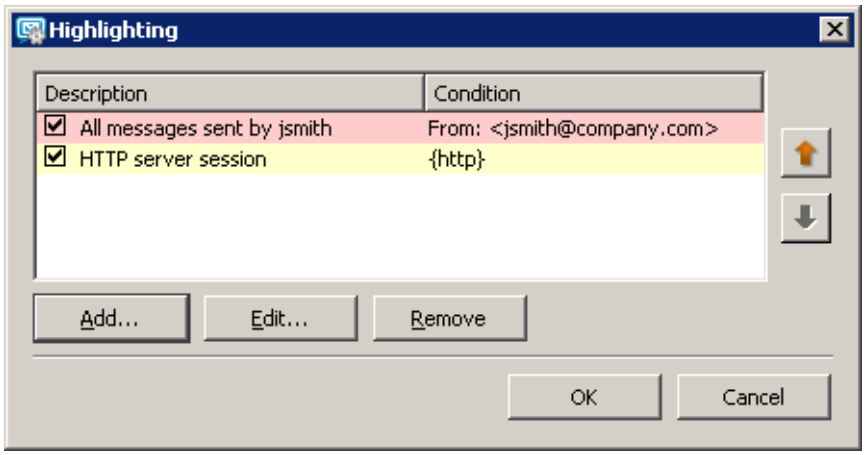

Figure 22.4 Highlighting

New highlighting can be set in the *Add highlighting* dialog box (see figure 22.5):

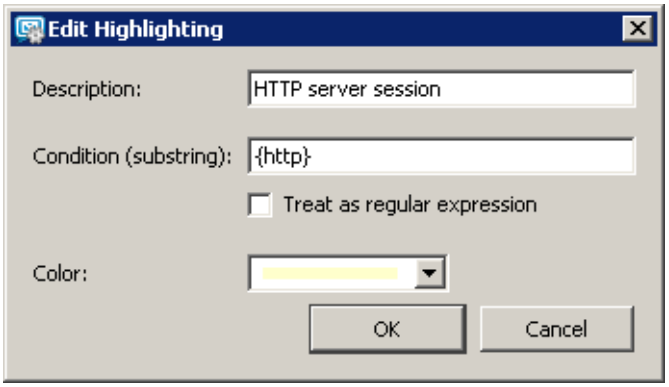

Figure 22.5 Add highlighting

- *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 *Debug Log* dialog where you can set parameters for clearing or saving logs.

The File Logging tab

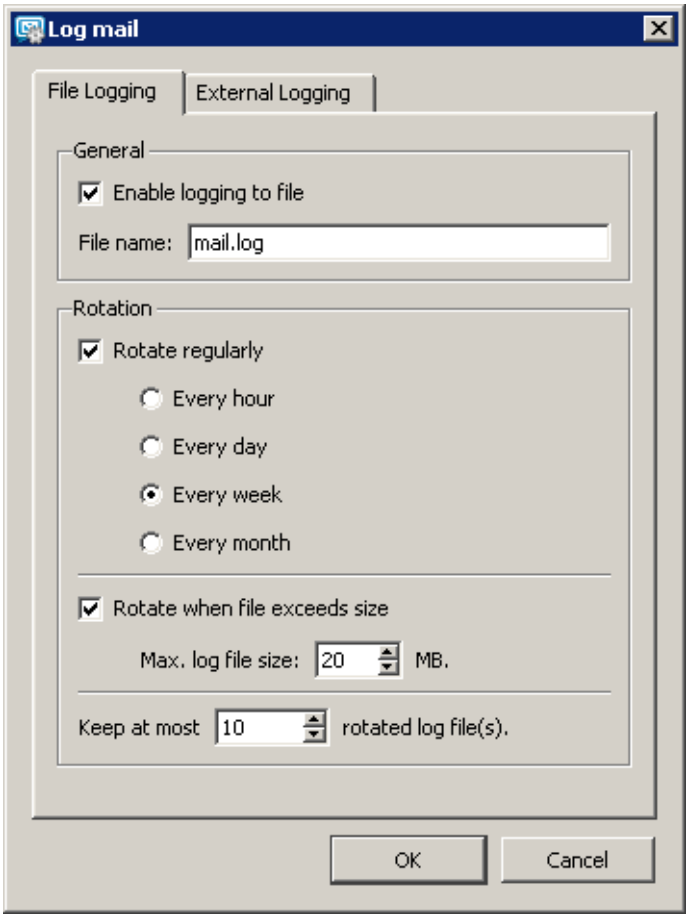

Figure 22.6 File Logging

- *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.

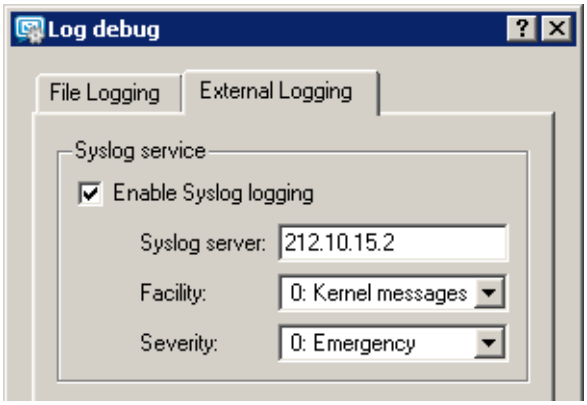

Figure 22.7 Storing logs on Syslog server

- *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.

22.2 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='tjones', Domain='company.com', Account_enabled='1',
Auth_type='0', Password=xxxxxx, 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

22.3 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,
[30/Nov/2005 17:57:14] Recv:  Queue-ID: 438dd9ea-00000000,
Service:  SMTP, From:  <jwayne@company.com>, To:
<jwayne@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:  <jsmith@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. Received).
- `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 and 1893). 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: <jwayne@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:  <mailinglist-bounce@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` — the number generated by the server in the queue of outgoing messages.
- `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).

22.4 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` — *SpamAssassin* 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 22.5).

```
[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 15.2, 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.

Wipe

User's mobile device got lost or stolen and the administrator wiped all user data out of the device (for details, see section 36.5).

Three types of records regarding wipe are used in the *Security* log. The first record informs about initiation of the wipe process. This record is always included. At this stage, the wipe process can be stopped. The second record type appears if the wipe process is stopped and cancelled. The third record is logged if the wipe process is completed successfully. The wipe is applied upon the next connection of the device to the server.

- An example of a record of an initiation of the wipe process is provided below:

  ```
  [22/Aug/2006 12:30:23] Device with id
  C588E60FCF2FB2C107FBF2ABE09CA557(user:  jwayne@company.com)
  will be wiped out by request Admin
  ```

- An example of a record of a cancellation of the wipe process is provided below:

  ```
  [22/Aug/2006 12:36:51] Wiping out of the device
  C588E60FCF2FB2C107FBF2ABE09CA557 (user:  jwayne@company.com)
  has been cancelled by Admin
  ```

- The third example shows information about successful wipe-out of the data on the device:

  ```
  [22/Aug/2006 12:31:11] Device C588E60FCF2FB2C107FBF2ABE09CA557
  (user:  jwayne@company.com), connected from:  192.168.44.178
  has been irrecoverable wiped out
  ```

22.5 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.

22.6 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.

22.7 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:  jwayne@company.com, Message size:  342,
From:  jsmith@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 jsmith@company.com marked a message
as spam, Folder:  ~jsmith@company.com/INBOX, Size:  462,
From:  "John Wayne" <jwayne@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:

```
[06/Sep/2004 08:43:32] User jwayne@company.com marked a message
as not spam, Folder:  ~jwayne@company.com/Junk E-mail, Size:  500,
```

`From: "John Smith" <jsmith@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.

22.8 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 MailServer's* 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 *Messages* option in the context menu of the *Debug* window.

The *Logged messages* dialog box where several options to enable particular logs are available:

Services

The *Services* section allow logging any information associated with services started in *Kerio MailServer*:

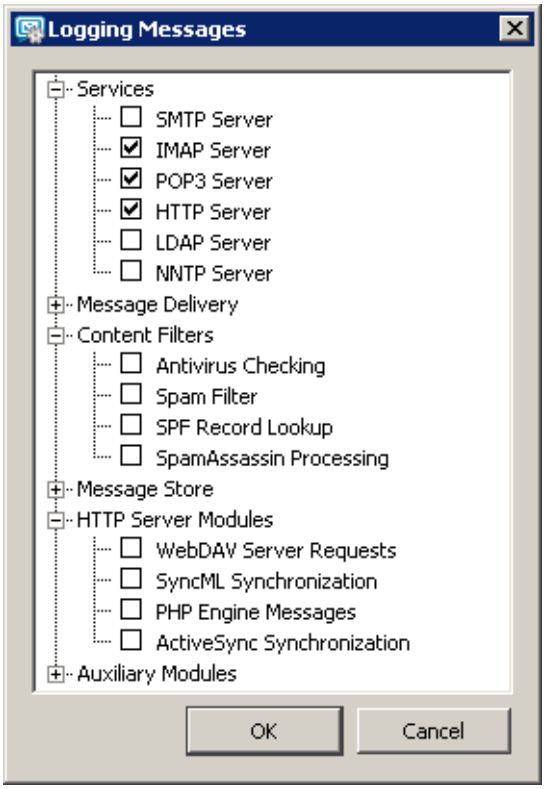

Figure 22.8 Debug log settings

- SMTP Server — detailed information about communication between clients and the SMTP server. This log can be helpful when you experience problems with MX records.
- IMAP Server — detailed information about communication between clients and the IMAP server. The log also provides information on communication via the MAPI interface.
- POP3 Server — 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 — communication between clients and the HTTP server for the *Kerio WebMail* interface.
- LDAP Server — detailed monitoring of communication between clients and the LDAP server, and search for contacts in the database.
- NNTP Server — detailed information about communication between clients and the news server.

Message Delivery

The *Message Delivery* section provides options for logging while message delivery is in progress:

- Queue Processing — processing of the Mail Queue (sending and receiving messages, re-scheduling, etc.)
- 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 Expansion* can be helpful when you experience problems with domain mailbox.
- SMTP Client — 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.
- Mailing List Processing — mailing lists monitoring (logins, logouts, message sending, moderators performance, etc.).
- Alias Expansion — 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.
- Sieve Filters — filtering messages according to user filters.

Content Filters

The *Content Filters* section includes options for enabling/disabling logs tracing antivirus and antispam control:

- Antivirus Checking — 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.
- Spam Filter — the option logs spam rating of each message which has passed through the *Kerio MailServer's* antispam filter.
- SPF Record Lookup — the option gathers information of *SPF* queries sent to SMTP servers. It can be used for solving problems with SPF check.
- SpamAssassin Processing — the option enables tracing of processes occurred during *SpamAssassin* antispam tests.

Message Store

The *Message Store* section enables logging of operations associated with data store, searching, backups, etc.:

- Message Folder Operation — operations with user and public folders (opening, saving messages, closing)
  This log can be used for example to resolve problems regarding mapping of public folders.
- Searching and Sorting — this log includes operations that server performs while

searching in email, calendars, contacts and tasks folders. Also operations performed during sorting (e.g. alphabetical sorting of email messages, sorting by date of reception, etc.) are logged.
- Quota and Login Statistics— the log may be helpful especially where a problem regarding user quotas and related issues occurs.
- Store Backup — 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.
- Messages decoding — this log may be helpful where problems regarding decoding of TNEF or uuencode messages occur.

HTTP Server Modules

The *HTTP Server Modules* provides options that enable logging information regarding traffic over an HTTP interface:

- WebDAV Server Requests — the log lists all operations related to the WebDAV interface. It is useful especially for solving communication issues between *Kerio MailServer* and *MS Entourage*, *NotifyLink*, *Kerio Sync Connector* and iCal clients.
- SyncML Synchronization — this option reports any activity that occurred between *Kerio MailServer*and *Kerio Synchronization Plug-in* during synchronization.
- PHP Engine Messages — the log gathers information related to the *Kerio WebMail* interface. This information is an extension to the *Error* log and it can be used for troubleshooting of *Kerio WebMail* issues.
- *ActiveSync Synchronization* — this log lists *ActiveSync* traffic performed between mobile devices and *Kerio MailServer*.

Auxiliary Modules

The *Auxiliary Modules* section provides the following logging options:

- User Authentication — 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.
- DNS Resolver— finding target domain SMTP servers through DNS MX record lookup
- 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.
- Update Checker Activity — monitors communication with the *update.kerio.com* server where new versions of *Kerio MailServer* are stored.
- Thread Pool Activity — describes establishing, progress and closing of any threads processed by *Kerio MailServer*.

- Administration Console Connections — logs connections and activity of the *Kerio Administration Console*.

22.9 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 2.4). *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.

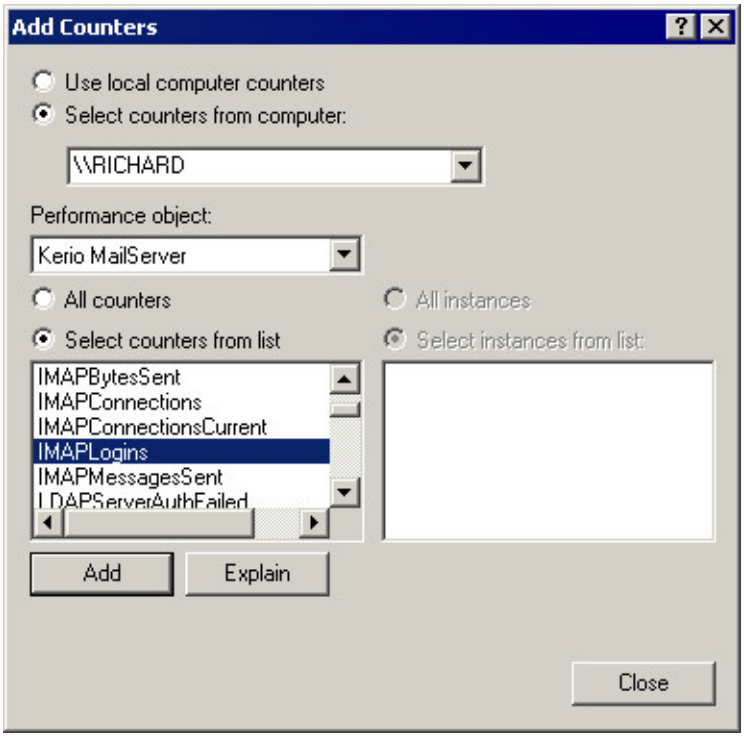

Figure 22.9 Performance Monitor

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 21.6, 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 2.4).
- For detailed information about *Performance Monitor* see Help in Windows.

Chapter 23

Public folders

Public folder is a special folder type. This folder is automatically available for reading to all users of the domain or of entire *Kerio MailServer*.

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. `Admin` is allowed to grant administrator rights to other users.

Publish folders can be administered from the following interfaces and email clients:

- Kerio WebMail
- Kerio Outlook Connector (Offline Edition)
- Kerio Outlook Connector

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.

Once a new folder is created, read rights are automatically set for all users in the domain or in entire *Kerio MailServer*. Under *Configuration* → *Domains* in the administration console, it is possible to set whether public folders will be available for the entire server or folders will be created for each domain. In this section, click on *Advanced* to make the settings.

Public folders will be shared automatically with all selected users as subfolders of *Public folders* (see figure 23.1)..

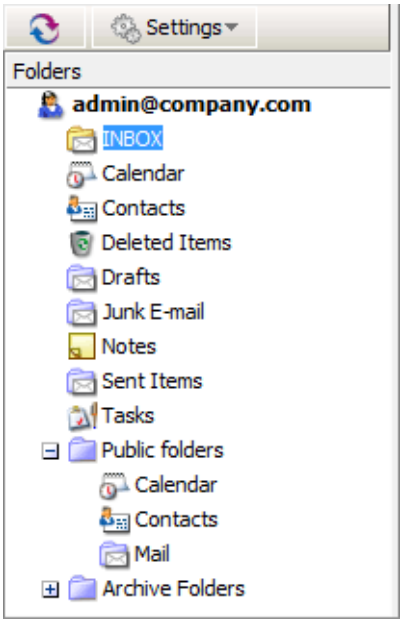

Figure 23.1 Public folders in the Kerio WebMail interface

23.1 Viewing public folders in individual account types

The table shows which public folders can be viewed by a particular user, depending on the email account type or client.

Account	Email	Contacts	Calendar	Tasks	Notes
Kerio Outlook Connector (Offline Edition)	YES	YES	YES	YES	YES
Kerio Outlook Connector	YES	YES	YES	YES	YES
Kerio WebMail	YES	YES	YES	YES	YES
Kerio Synchronization Plug-in + IMAP	YES[a]	YES	YES	NO	NO
Kerio Synchronization Plug-in + POP3	NO	YES	YES	NO	NO
an account of the Exchange in MS Entourage type	YES	YES[b]	YES[b]	NO	NO
an account of the Exchange in Apple Mail type[c]	YES	YES	YES	YES	YES
IMAP (any client that supports the IMAP protocol)	YES (if the client can show them)	NO	NO	NO	NO
POP3 (any client that supports the POP3 protocol)	NO	NO	NO	NO	NO

[a] If subscribed.
[b] Only for *MS Entourage 2004 sp2*.
[c] Only if the full support for IMAP is set in the *Kerio MailServer's* configuration file (for details, see chapter 41).

Table 23.1 Viewing public folders in individual account types

Chapter 24

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 4120.

Kerio MailServer includes support for Kerberos V5.

Note: The following logs may be helpful while solving configuration issues:

- *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: Settings of logging at the server's side is regards Kerberos MIT (US implementation of Kerberos applied in the *Active Directory* and the *Apple Open Directory*). Setting of Kerberos Heimdal logging (European implementation of Kerberos which can be found in several Linux distributions) may be different.[3]
- *Mac OS X Server* — logs in the *Server Admin* application (see chapter 24.4)
- *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 (*User Authentication* must be running). For detailed description on individual logs, refer to chapter 22.

[3] The Kerberos Heimdal's client is also included in the Linux installation packages of *Kerio MailServer*. It is, however, not important which version is used on the server (Key Distribution Center) and which is used at the client (*Kerio MailServer* in this case) since the protocol is the same and no problems should occur in the cooperation of the server and the client side.

24.1 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 24.1).

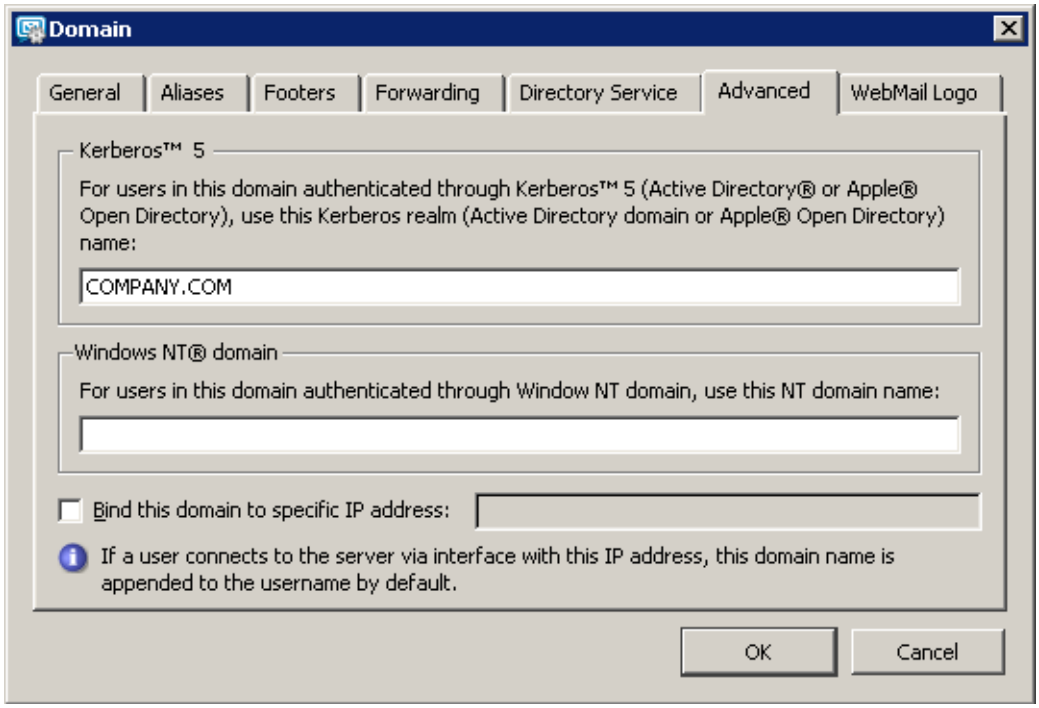

Figure 24.1 Setting the Active Directory domain in Kerio MailServer

Specify the domain name in the *Advanced* dialog (see figure 24.1) 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. In this case, however, a special configuration of DNS servers is required. Either it is necessary to set DNS servers to forward queries to each other

(if the query is not found in the proper database, it is forwarded to the domain controller) or all DNS servers must share the same primary parent DNS server.

3. time of *Kerio MailServer* and *Active Directory* is synchronized — this should be done automatically by adding a host to the domain (see item 1).

Authentication against Open Directory

For authentication with *Open Directory*, *Kerio MailServer's* Kerberos realm must be specified (e.g. `COMPANY.COM`).

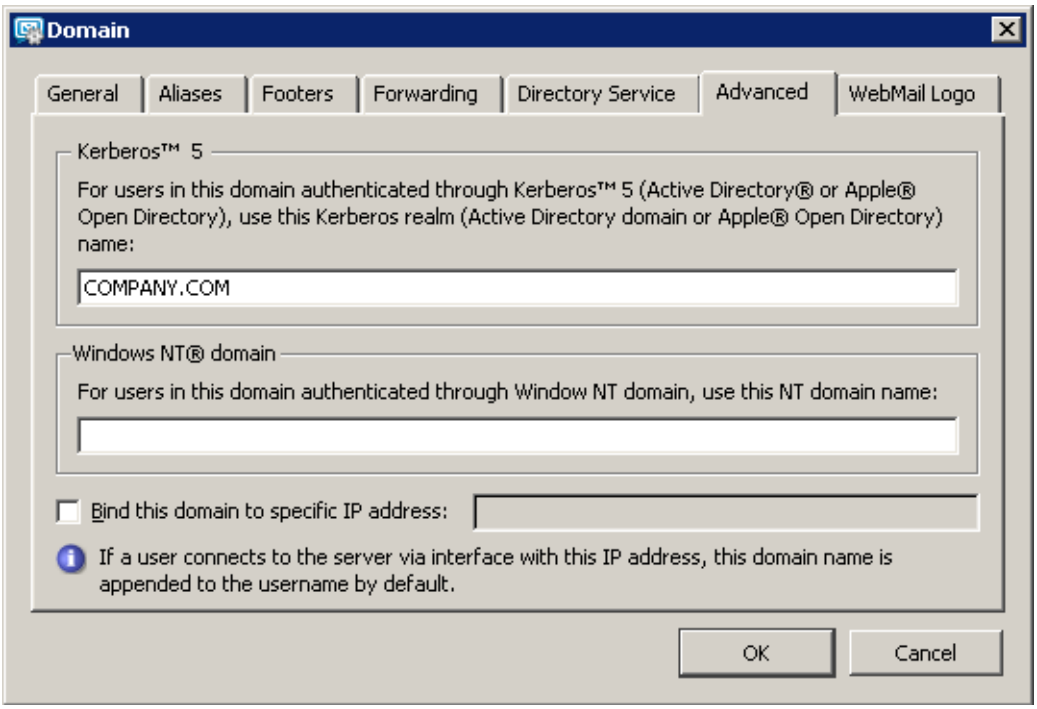

Figure 24.2 Specification of Kerberos realm in Kerio MailServer

Specify the *Open Directory* domain name (Kerberos realm) in *Kerio MailServer* and ensure that:

1. *Kerio MailServer* is a member of the *Open Directory* 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* 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*.

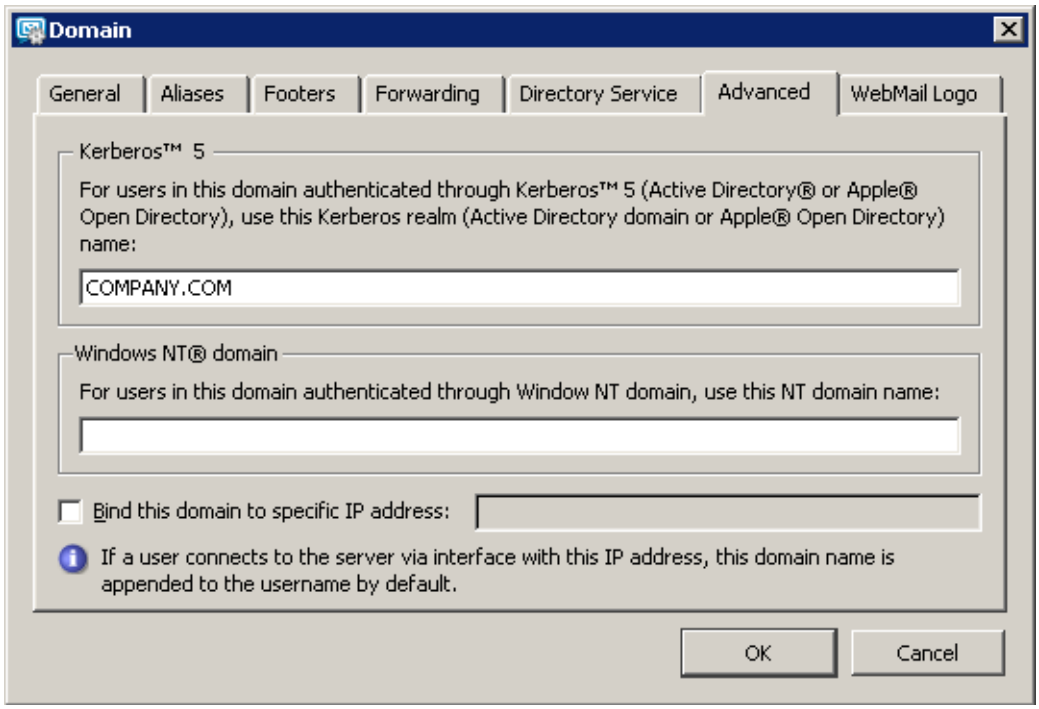

Figure 24.3 Specification of Kerberos realm in Kerio MailServer

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. Usernames and passwords of all users created in *Kerio MailServer* must be defined in the *Key Distribution Center* (required for authentication in Kerberos).

2. DNS server 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.

Using the `Kerbtray` utility, it is possible to test whether *Kerio MailServer* is able to authenticate against the *Key Distribution Center*.

This can be checked from the computer where *Kerio MailServer* will be installed. To check authentication from *MS Windows*, use the *Kerbtray* utility (see figure 24.4) which

can be downloaded for free at the *Microsoft's* website. If no allocated tickets are found by *Kerbtray*, authentication does not work and it is necessary to enable it in KDC and start it.

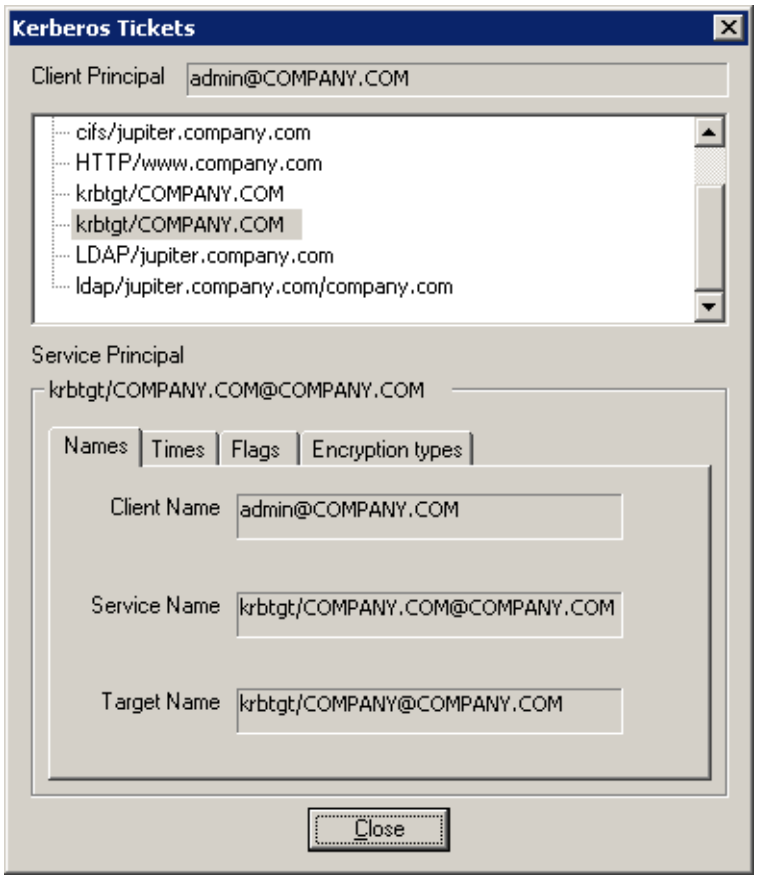

Figure 24.4 Kerberos tickets displayed in Kerbtray

When the previous steps are followed successfully, set authentication in *Kerio MailServer* on the *Advanced* tab under *Configuration* → *Domains*, (see chapter 7.7).

24.2 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*).

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.

For proper authentication, define the `/etc/krb5.conf` file.

Example of `krb5.conf` file's configuration:

```
[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 7.6 and 7.7).

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 on the *Kerio MailServer's* host.

3. time of the *Kerio MailServer* host and the *Open Directory* must be synchronized.

For proper authentication, define the `/etc/krb5.conf` file.

Example of `krb5.conf` file's configuration:

```
[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 7.6 and 7.7).

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,
   - usernames and passwords of all users created in *Kerio MailServer* must be defined in the *Key Distribution Center* (required for authentication in Kerberos).

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.

For proper authentication, define the `/etc/krb5.conf` file.

Example of `krb5.conf` file's configuration:

```
[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
 }
```

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.

Then, perform corresponding settings in *Kerio MailServer* (see chapter 7.7).

24.3 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 24.5)

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.

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 24.6). Enter authentication name and password. The user who makes changes in the application needs administration rights for the system.

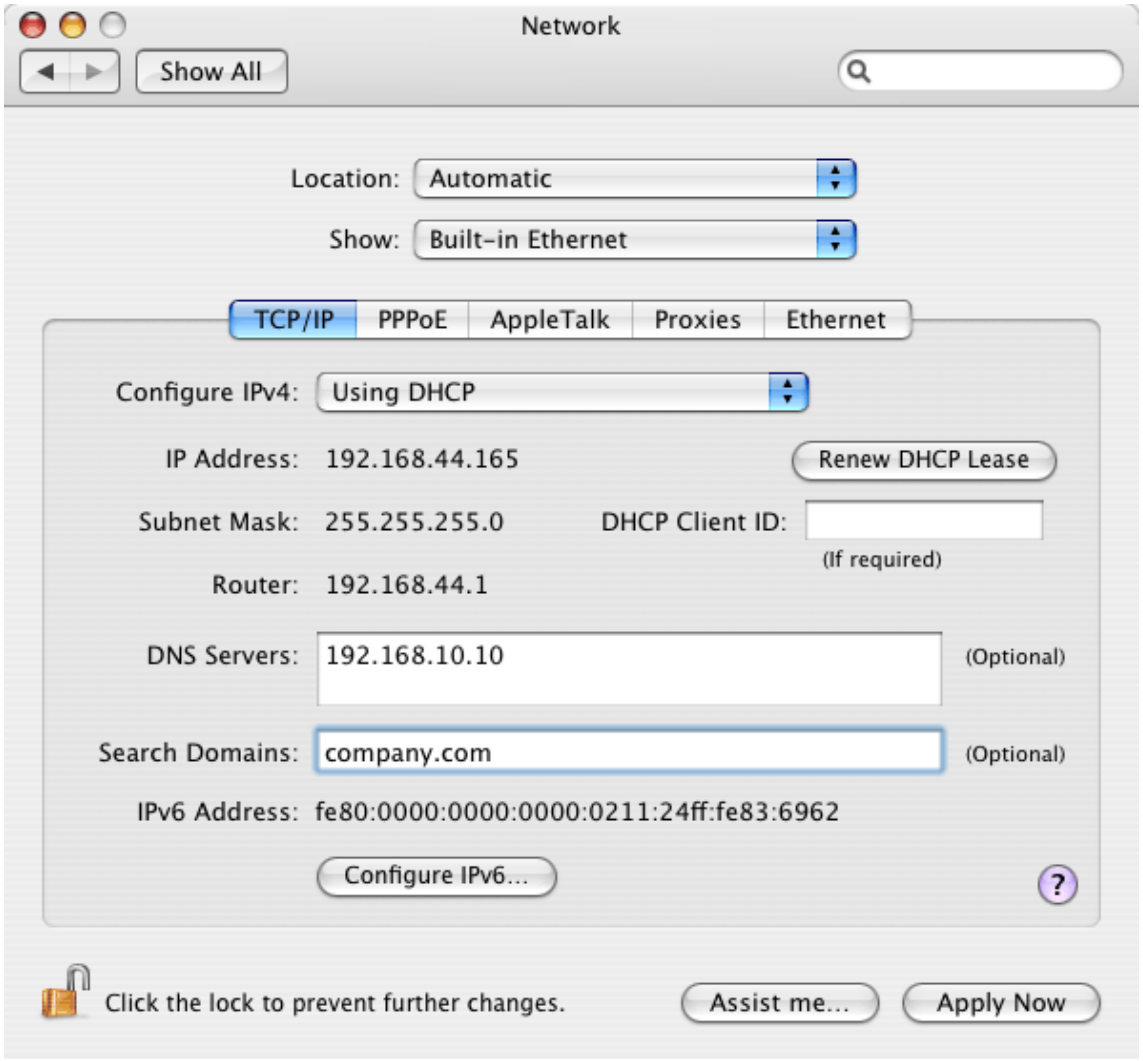

Figure 24.5 DNS configuration

2. Enable the service, click on *Configure* and specify the *Active Directory* domain name (see figure 24.7).

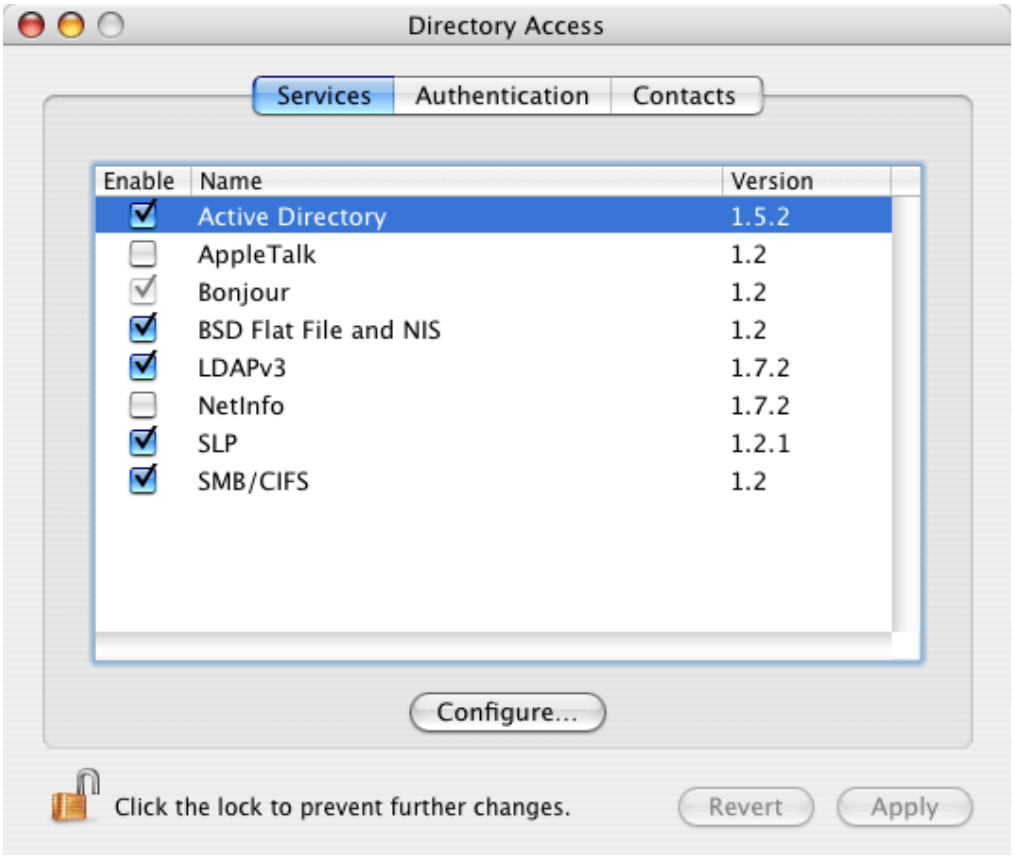

Figure 24.6 Directory Access — Services

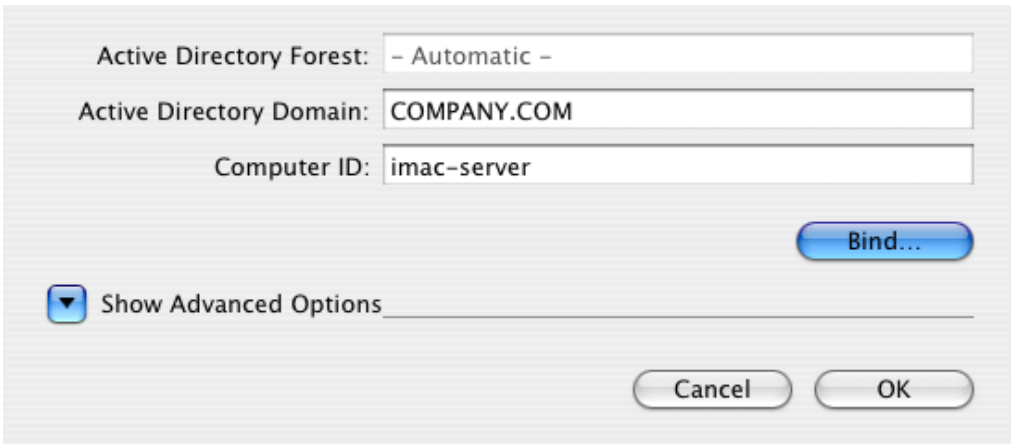

Figure 24.7 Directory Access — configuration

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 24.8).

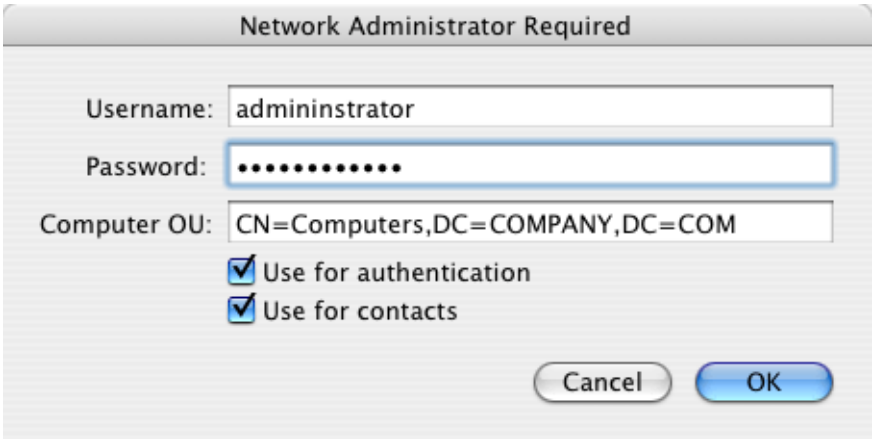

Figure 24.8 Directory Access — specification of administrator's login data

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 = server.company.com.
        }
```

Using the `kinit` utility, it is possible to test whether *Kerio MailServer* is able to authenticate against the *Active Directory* 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 Extensions* 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* and higher. 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 24.9).
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 the *Apple Open Directory* service 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.

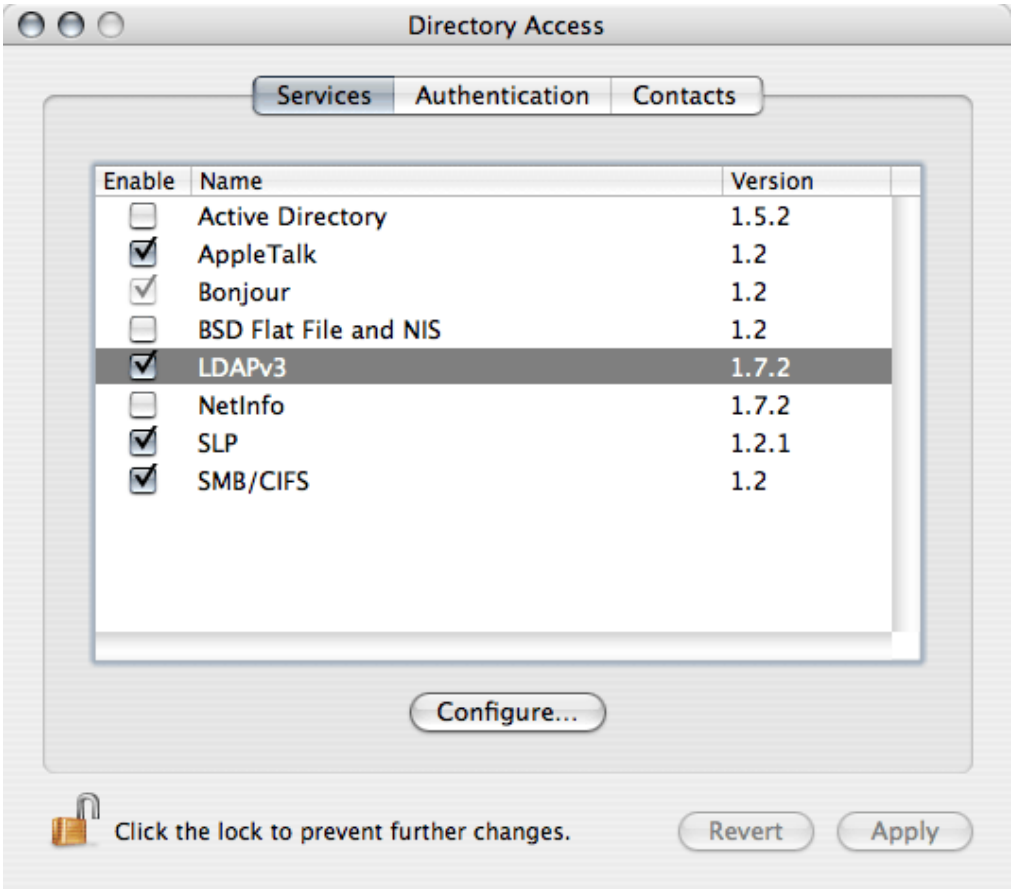

Figure 24.9 Directory Access — checking LDAP

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 24.10:

   `od.company.com` → `dc=od,dc=company,dc=com`

   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 24.11).

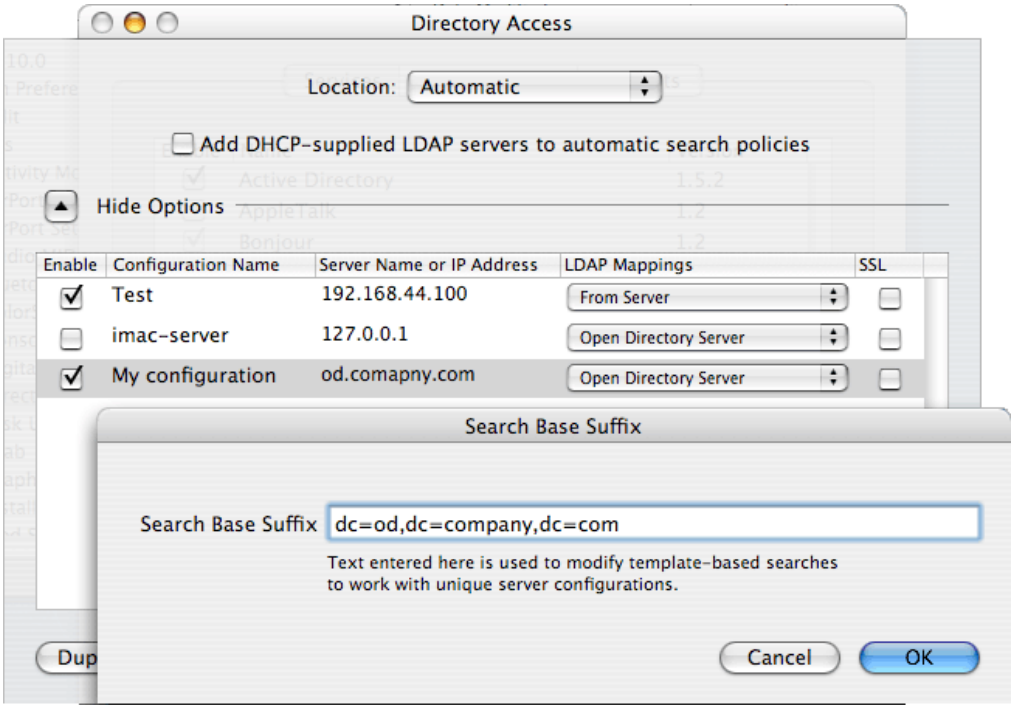

Figure 24.10 Directory Access — configuration of the Open Directory server

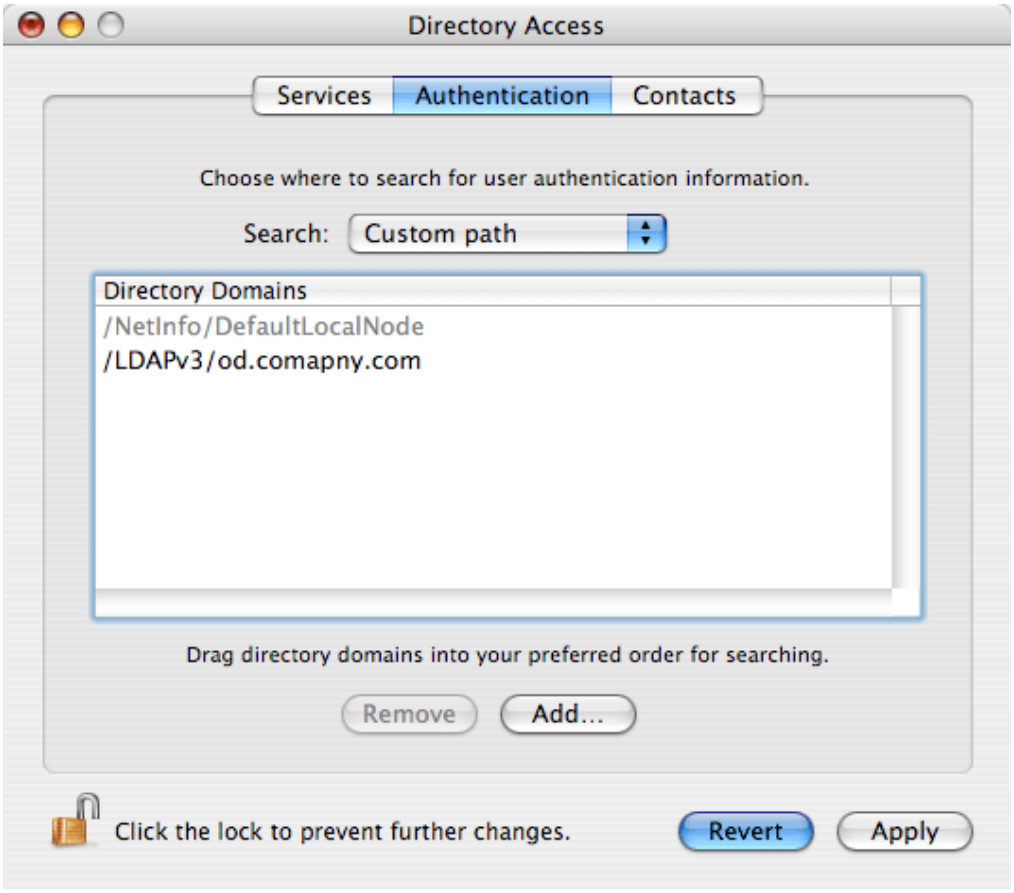

Figure 24.11 Directory Access — Authentication settings

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 Open Directory
# do not make changes to this file;
# autogenerated from : /Open 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/KMS_hostname@KERBEROS_REALM username@REALM
```

for example:

```
kinit -S host/od.company.com@COMPANY.COM thenry@COMPANY.COM
```

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)
  Warning: Kerberos realm specified on the *Advanced* tab must be identical with the name of the Kerberos realm specified in the `/Library/Preferences/edu.mit.Kerberos` file. In particular, it must match the `default_realm` value in this file. By result, the line may be for example `default_realm = COMPANY.COM`
- 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,
- usernames and passwords of all users created in *Kerio MailServer* must be defined in the *Key Distribution Center* (required for authentication in Kerberos).

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.

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 KERBEROS
# do not make changes to this file;
# autogenerated from : /KERBEROS/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/KMS_hostname@KERBEROS_REALM username@REALM
```

for example:

```
kinit -S host/mail.company.com@COMPANY.COM
```

If the query was processed correctly, you will be asked to enter password for the particular user. Otherwise, an error will be reported.

When the previous steps are followed successfully, set authentication in *Kerio MailServer* on the *Advanced* tab under *Configuration* → *Domains*, (see chapter 7.7).

24.4 Starting Open Directory and Kerberos settings

In *Open Directory*, it is possible to authenticate users against the password server (refer to chapter 7.6) or the Kerberos server (for details, see chapter 24). As mentioned in chapter 7.6, 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 24.12).

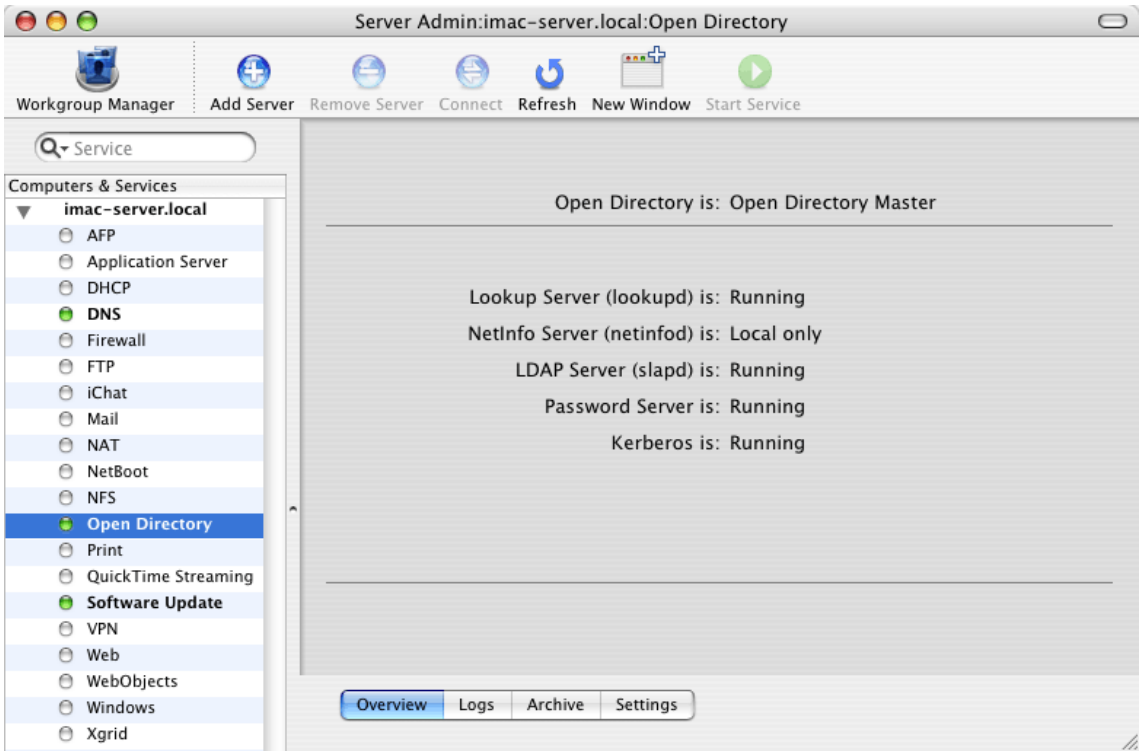

Figure 24.12 The Open Directory service

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 24.12). 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 24.13).

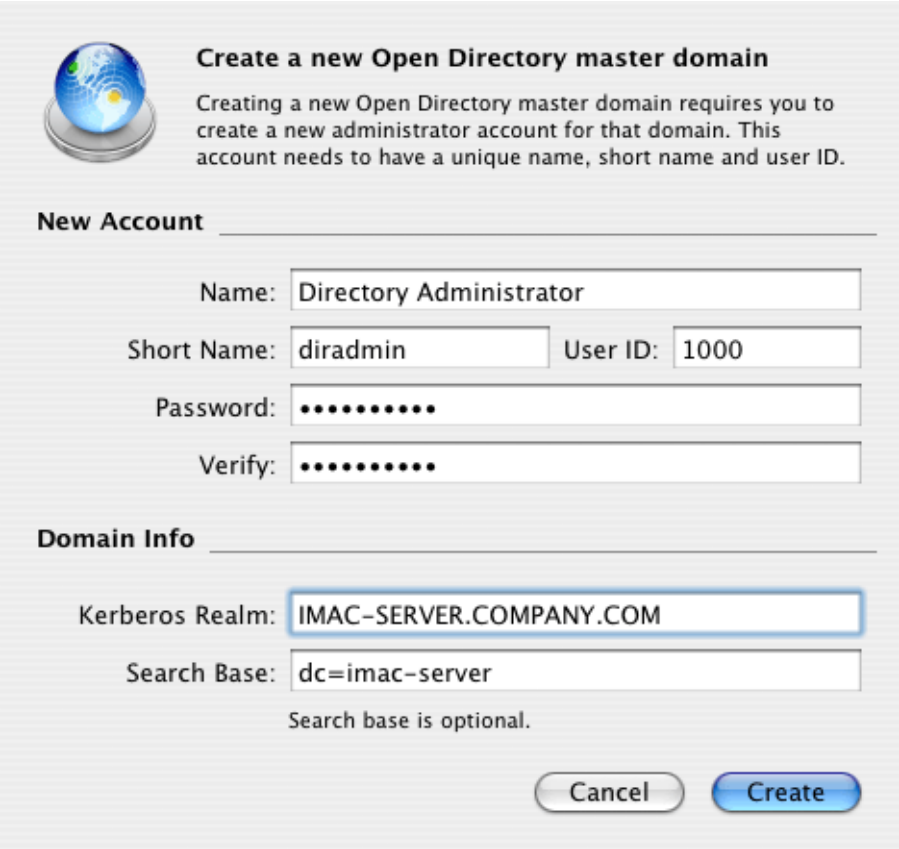

Figure 24.13 Setting of administration username and password

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 25

NTLM authentication settings

NTLM (NT LAN Manager) is an authentication type used on Windows for authentication against an Active Directory (or NT) domain.

First, the following conditions must be met:

- NTLM authentication 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* (see chapters 7.6 and 13.10).
- In order for the NTLM authentication to be functional, both computers as well as user accounts have to belong to the domains used for authentication.
- To make NTLM relevant it is necessary that users use clients with support for NTLM (SPA) authentication (e.g. *MS Outlook*).

Warning: NTLM authentication is not available if *MS Outlook* extended by the *Kerio Synchronization Plug-in* is used.

NTLM authentication in *Kerio MailServer* must be set correctly, as follows:

1. In the administration console, go to *Domains* (*Configuration* → *Domains*). Open the dialog with domain settings details and switch to the *Advanced* tab (see figure 25.1). Use the *Windows NT Domain* entry to specify NT domain name (the name usually matches the Active Directory domain name without the first level domain — NET, COM, etc.).

2. In the administration console, go to *Configuration* → *Advanced Options* and enable the *Allow NTLM authentication for users with Kerberos authentication (for Active Directory users)* option on the *Security Policy* tab. Enable this option to allow *Active Directory* domain users to authenticate at *Kerio MailServer* upon their logon.

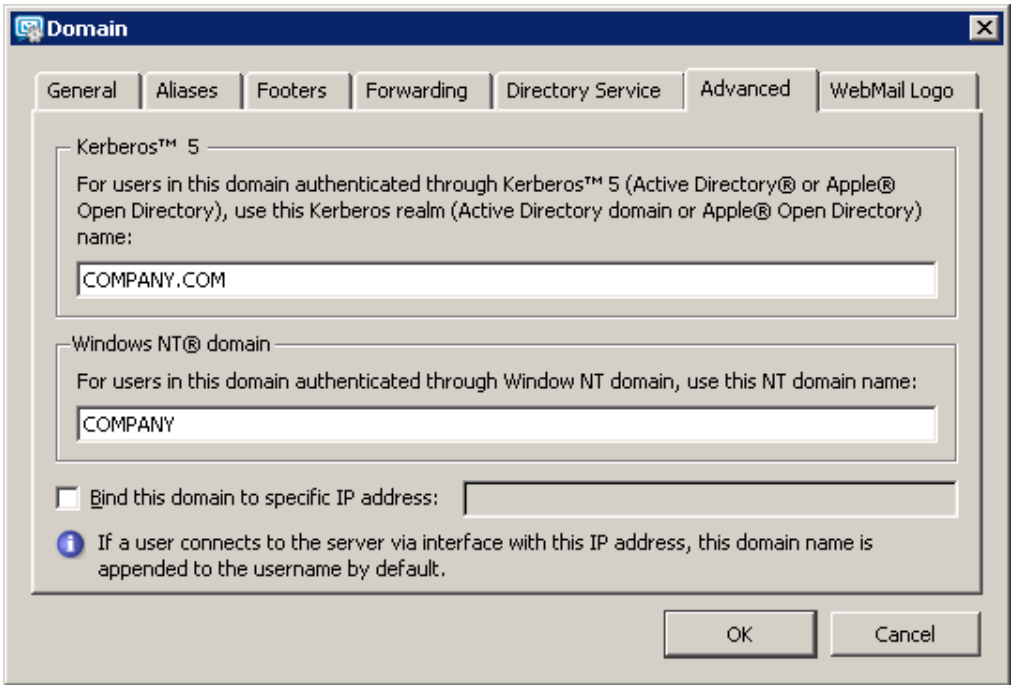

Figure 25.1 Setting Windows NT domain name

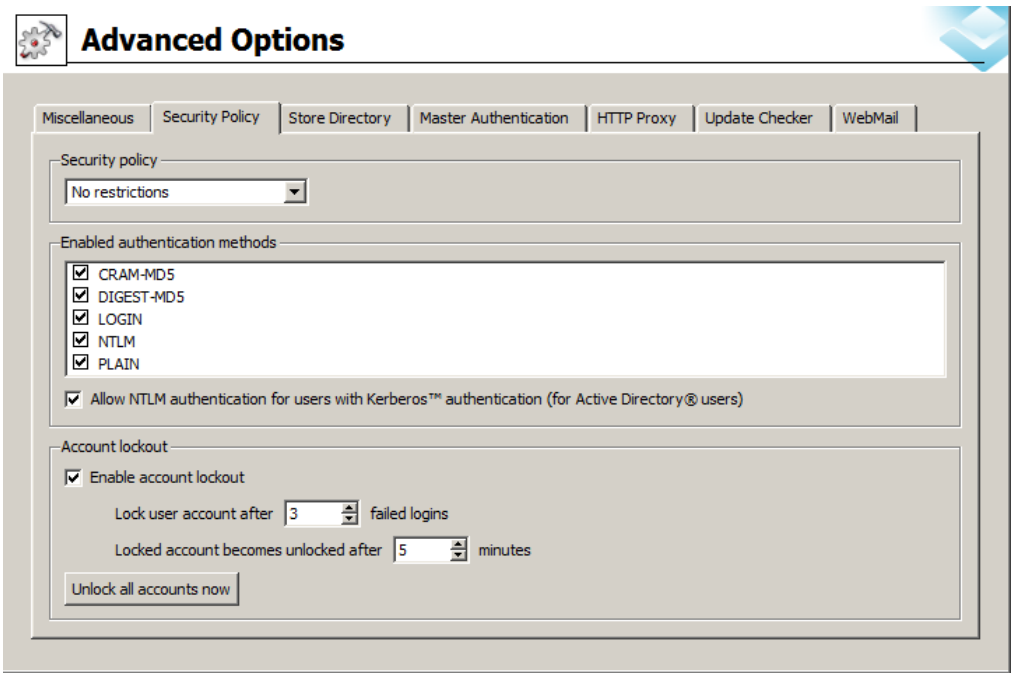

Figure 25.2 Enabling the Allow NTLM authentication for users with Kerberos authentication option

3. In the administration console, open the *Domain Settings* → *User Accounts* section

and set the *Windows NT Domain* option for user authentication. These parameters can be set on the *General* tab (see figure 25.3).

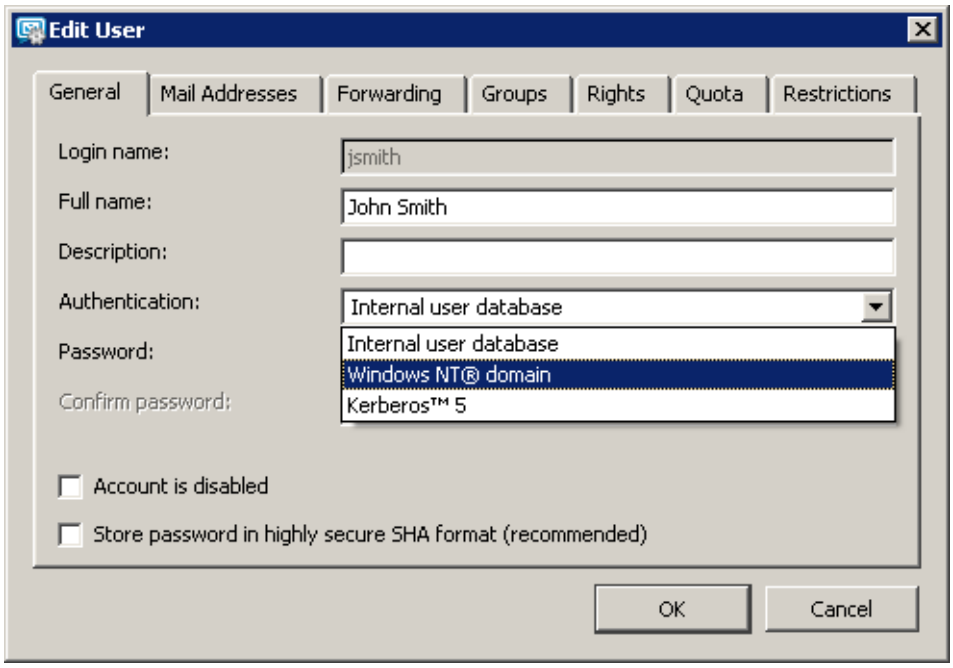

Figure 25.3 User authentication settings

25.1 Setting NTLM in MS Outlook extended by the Kerio Outlook Connector

It is also necessary to enable NTLM (SPA) authentication in email clients. These settings are generally performed in user's email account configuration. The following section provides instructions on how to set for example *MS Outlook* extended by the *Kerio Outlook Connector*:

1. In the *Tools* → *E-mail Accounts* menu, select *View or change existing e-mail accounts*.
2. Select a Kerio (MAPI) account and click on *Change* (see figure 25.4).
3. In the account settings just opened, go to the *Account* tab and enable the *Secure Password Authentication* option (see figure 25.5).

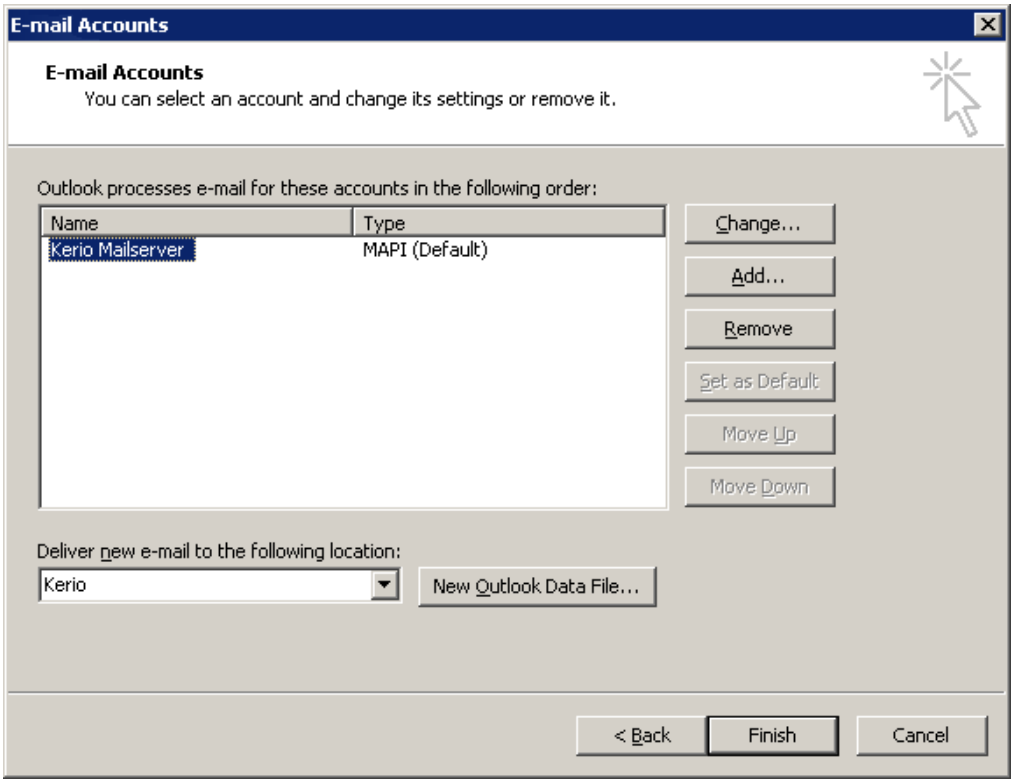

Figure 25.4 Editing an e-mail account

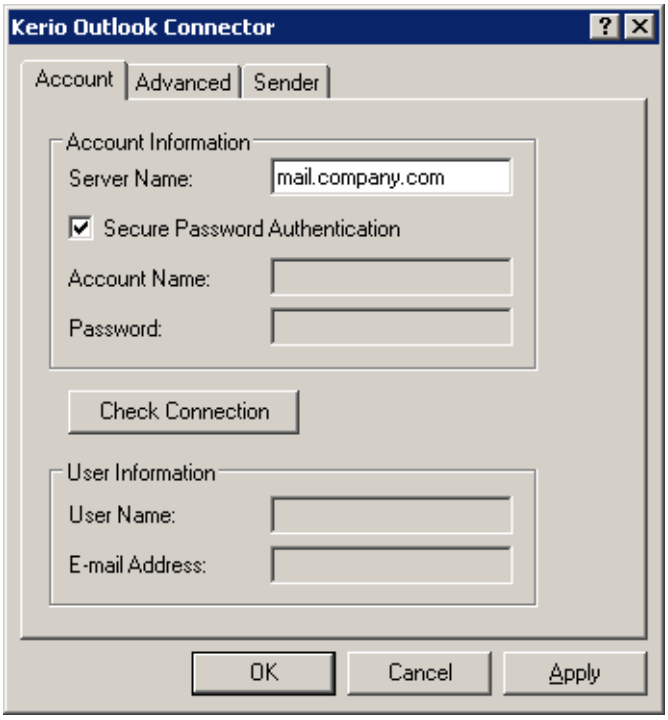

Figure 25.5 NTLM authentication settings

Chapter 26

Kerio MailServer Environment

26.1 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 *MS 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@company.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.company.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.company.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 16) as well as relay control — sending email to any domain is not permitted from the client's IP address (see chapter 16). 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 19).

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.

26.2 Web browsers

Recommended browsers for the full version of *Kerio WebMail* are as follows:

- *Internet Explorer* versions 6 and 7
- *Firefox* versions 1.5 and 2
- *Safari* 1.3, 2 and 3 on Mac OS X 10.5 Leopard

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.

26.3 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 16) and relay control (see chapter 15.2), 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. 636, 443, 993, 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 27

Deployment Examples

This chapter shows how to set *Kerio MailServer* in different conditions. Each example is essentially an applied *Quick Checklist* (see chapter 1.2) for a given situation. These examples should help you set up *Kerio MailServer* quickly and easily for your company.

27.1 Persistent Internet Connection

Information and Requirements

1. The company has the domain `company.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.company.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@company.com` and the sales department will have the address `sales@company.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 `company.com` and enter the server's DNS name `mail.company.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. On the *SMTP delivery* tab in the *Configuration* → *SMTP server* 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* → *Content Filter* → *Antivirus* section, enable antivirus control and choose the *AVG 7.0* module. In *Configuration* → *Content Filter — Attachment Filter*, enable filtering and set 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.

27.2 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. On the *SMTP Delivery* tab in the *Configuration* → *SMTP server* 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*.

27.3 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. On the *SMTP Delivery* tab in the *Configuration* → *SMTP server* 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*.

27.4 A company with multiple sites

Information and Requirements

The company in our example uses the only domain called `company.com`. Supposing a company has its headquarters in New York and a branch office in London. *Kerio*

MailServer is installed both at the headquarters and the branch office (two separate licenses). The headquarters' server uses DNS name `mail.company.com`. The branch office's server uses DNS name `mail-ldn.company.com`.

We want the email transferred among local users in the branch office to be delivered locally, while the email addressed to users in the headquarters is really sent to the headquarters. The same thing should be guaranteed for the communication in the other direction — messages sent from the headquarters to the branch office must be delivered to the branch office's server.

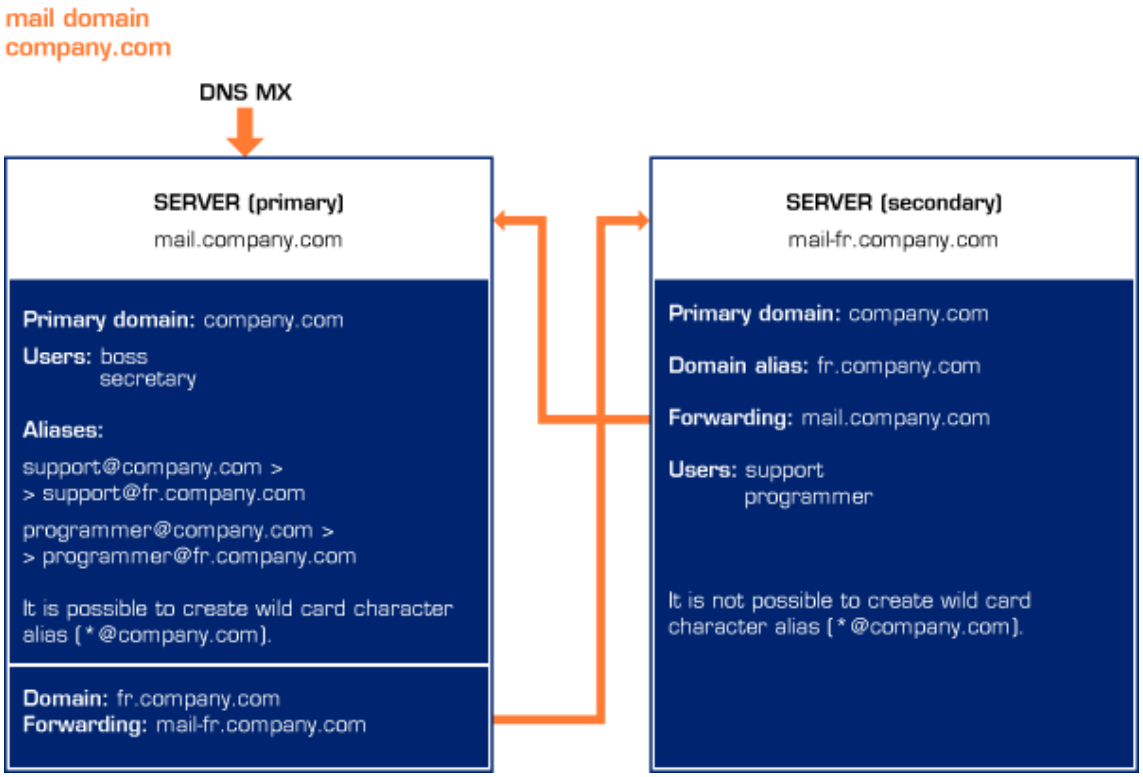

Figure 27.1 A company with multiple sites

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 (see figure 27.2).

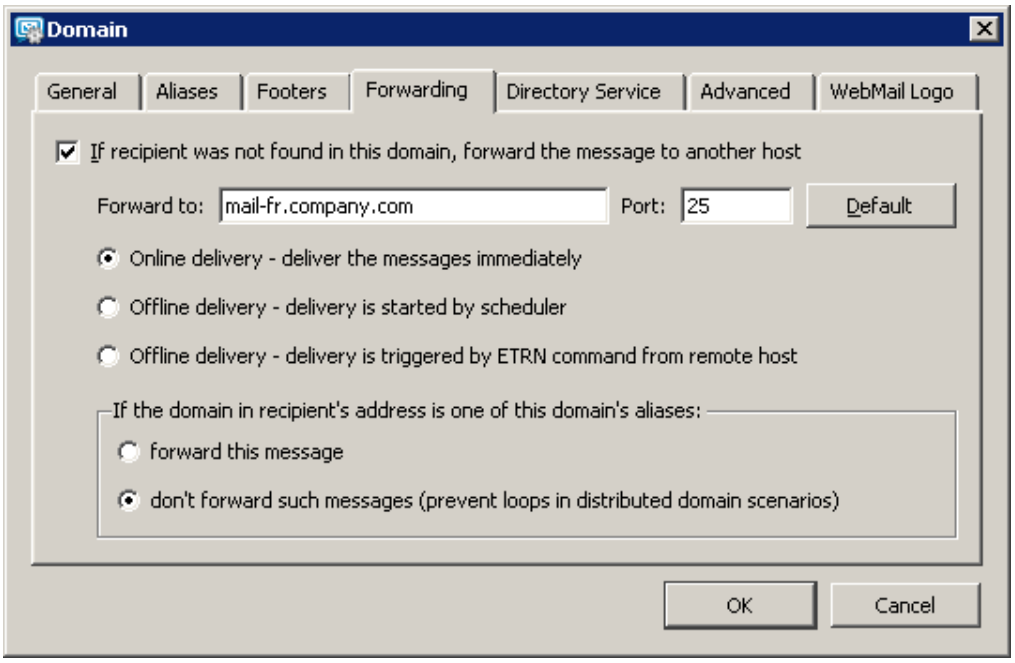

Figure 27.2 Forwarding settings

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`.

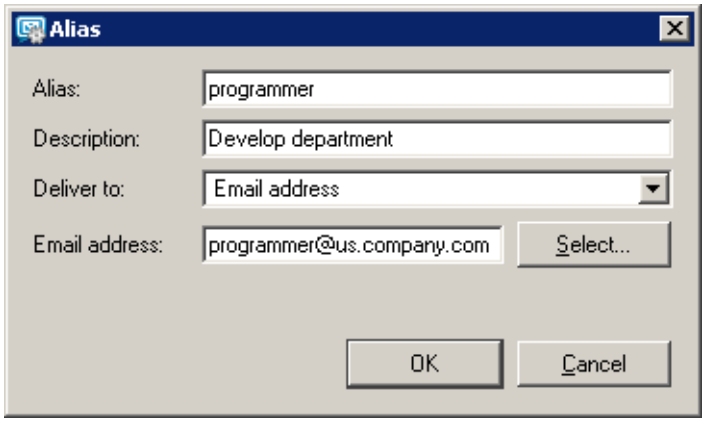

Figure 27.3 Alias settings

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 other site).

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.

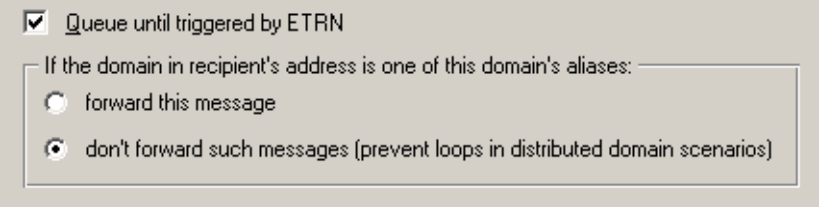

Figure 27.4 Anti-Loop settings

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.

27.5 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 7.5), specify message forwarding to the `mail1.company.com` primary mailserver (see picture 27.5).

   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 15.5). 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 want to use this method of email forwarding, allow the *Offline delivery — delivery is triggered by ETRN command from remote host* option (see figure 27.5) the `company.com` domain on the backup server in the administration console (*Configuration → Domains*).

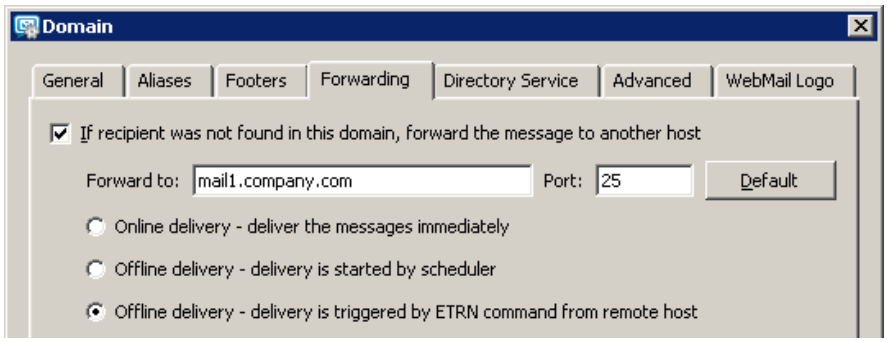

Figure 27.5 Setting up the backup server — the ETRN command

It is also necessary to enable using the ETRN command in the primary mailserver (see chapter 15.5) and schedule sending the ETRN command (see chapter 9).

- Another possibility is setting up the rules for outgoing messages (see chapter 15.2). 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.

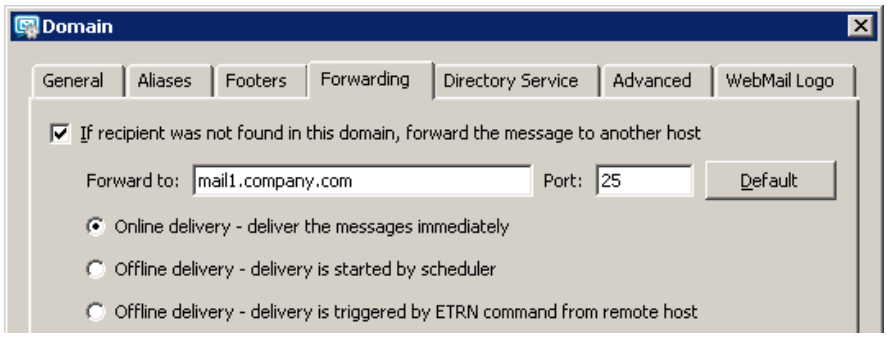

Figure 27.6 Setting up the backup server — mail delivery follows rules for queue of outgoing messages

In the domain configuration window, it is necessary to set name or address of the primary server, traffic port and the *Online delivery — deliver the messages immediately* (see figure 27.6).

- 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* (for details on scheduler's settings, refer to chapter9).

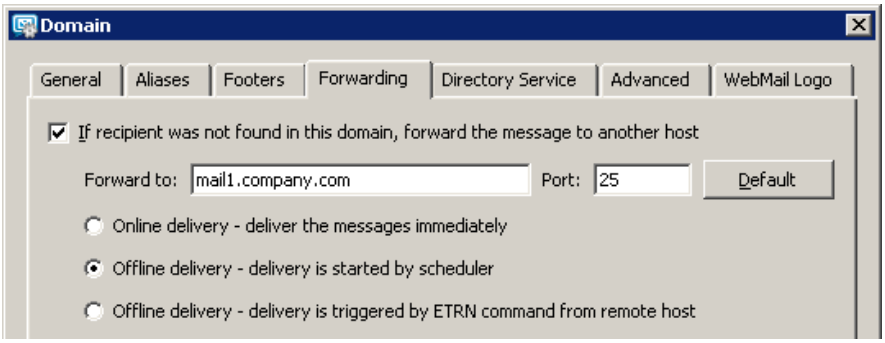

Figure 27.7 Setting up the backup server — mail delivery is controlled by the scheduler

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 15.2).

Chapter 28

Troubleshooting in Kerio MailServer

28.1 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 discrapancies 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, tasks and notes are saved to a store as a 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 special `index.fld` 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 `index.fld` file and the `#msgs` directory are saved in every folder created in each user account. The following path can be used as an example:

`\Kerio\MailServer\store\mail\company.com\nmandela\INBOX`

Solution

The solution might be easy:

1. Stop the *Kerio MailServer Engine*.
2. Under the `store` directory in the *Kerio MailServer's* store, find the domain of the users who have problems with their folders. Find the user's folder labeled by their

username. In this folder, the entire email account of the particular user is saved. User-created subfolders are included in main folders — they are ordered in the same way as displayed in *Kerio WebMail*.

3. Select the problematic folder, open it and change the filename from `index.fld` to `index.bad`

4. Run the *Kerio MailServer Engine*.

The file is automatically regenerated upon the first logon of the user to their mailbox — this happens in accordance with the current status of the folder and the file also takes over any flags (marks that inform form example whether the message was marked as deleted or if it was removed) from the original file renamed to `index.bad`.

Upon starting *Kerio MailServer*, the following record is written in the *Error* log:

```
[23/Jun/2005 12:12:47] mail_folder.cpp:  Folder
~jwayne@company.com/Contacts has corrupted status and index files,
going to restore them.  Some flag information may be lost
```

28.2 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`.

Warning: On *Mac OS X* and *Linux* systems, files can be maintained only if the user is logged in as the root user.

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` a `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. It is also necessary to make backups of the `myspell` folder if other than default dictionaries are used in *Kerio WebMail* (for details on this topic, see section 11.3).

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 43.1).

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 2.4)
2. Stop the *Kerio MailServer Engine*
3. Copy the archived `mailserver.cfg` and `users.cfg` files (and optionally also the `sslcert` and `license` directories and files of the `myspell` directory) into the *Kerio MailServer* installation directory.
4. Run the *Kerio MailServer Engine*

Chapter 29

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
: *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.

29.1 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).

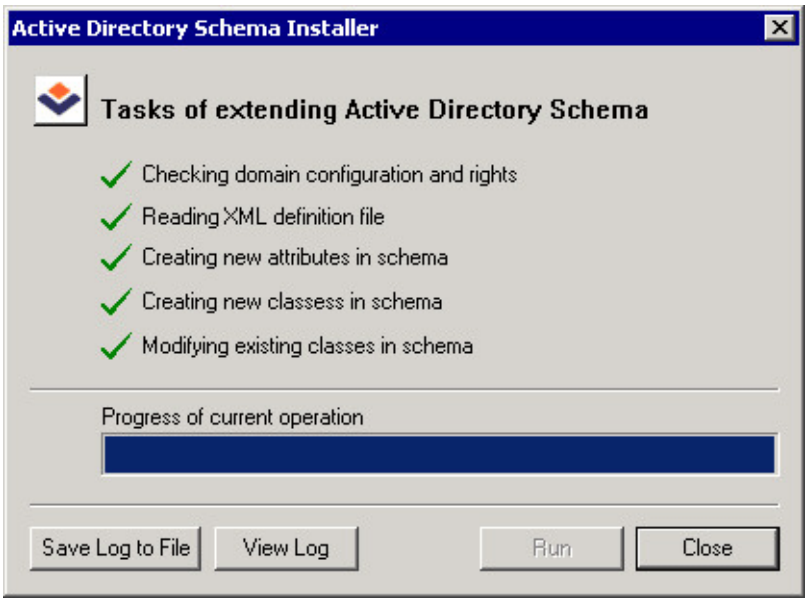

Figure 29.1 Installation process

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.

29.2 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 7.6). 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*.

29.3 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:

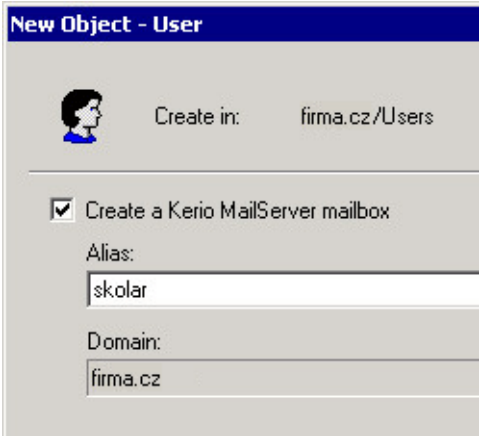

Figure 29.2 User account definition

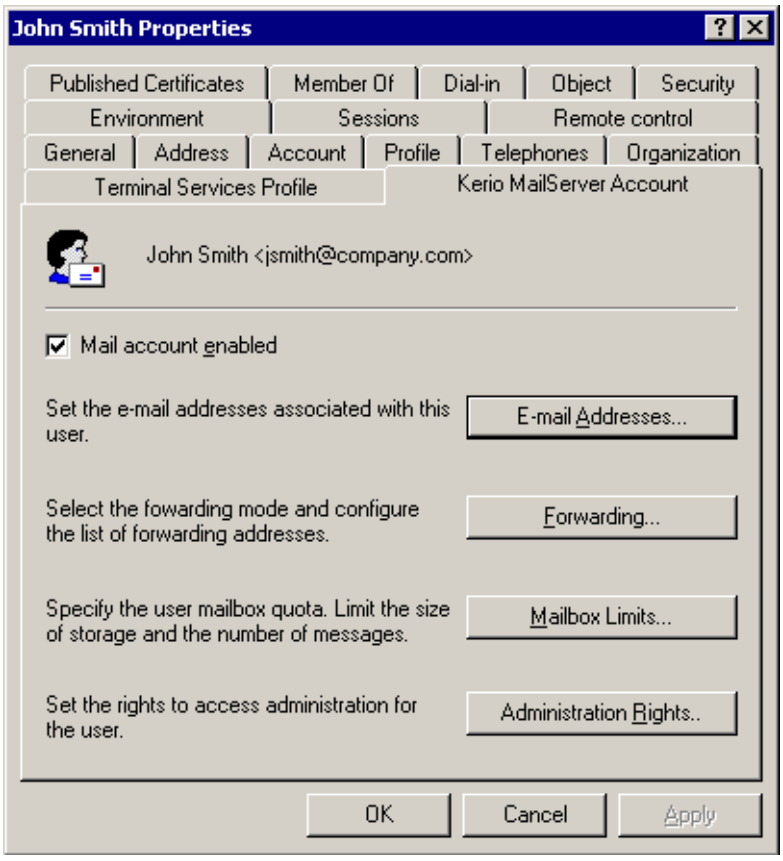

Figure 29.3 Kerio MailServer Account tab

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 29.4 Mailbox Limits

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 13.2). 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.

29.4 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 29.3.

Chapter 30

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.

30.1 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.

30.2 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 13).

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.

30.3 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 7.6).

2. User authentication via *Kerberos* must be set in domain settings (for more information, see chapter 7.7).

3. User authentication via *Kerberos* must be set in user settings (for more information, see chapter 13.2).

Chapter 31

KMS Web Administration

KMS Web Administration is a web interface for access to administration of the domain, i.e. of local user accounts, groups and aliases included in the domain. 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 cannot be edited in the web interface. In *KMS Web Administration*, these accounts are for reading only.

31.1 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* versions 6 and 7
- *Firefox* versions 1.5 and 2
- *Safari* version 1.3, 2 and 3 on Mac OS X 10.5 Leopard

To use the secured access to the *KMS Web Administration* 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 and JavaScript killers

If any *Pop-up* and/or JavaScript killer is installed and running, specify an exception for *KMS Web Administration*.

KMS Web Administration includes a utility able to detect *Pop-up* killers and JavaScript blockers. Before the first startup of the *KMS Web Administration* welcome page, this utility checks whether the exception for *Kerio MailServer* is set (see figure 31.1). If not, a warning and instructions how to set the exception is shown on the page with the login dialog (see figure 31.2).

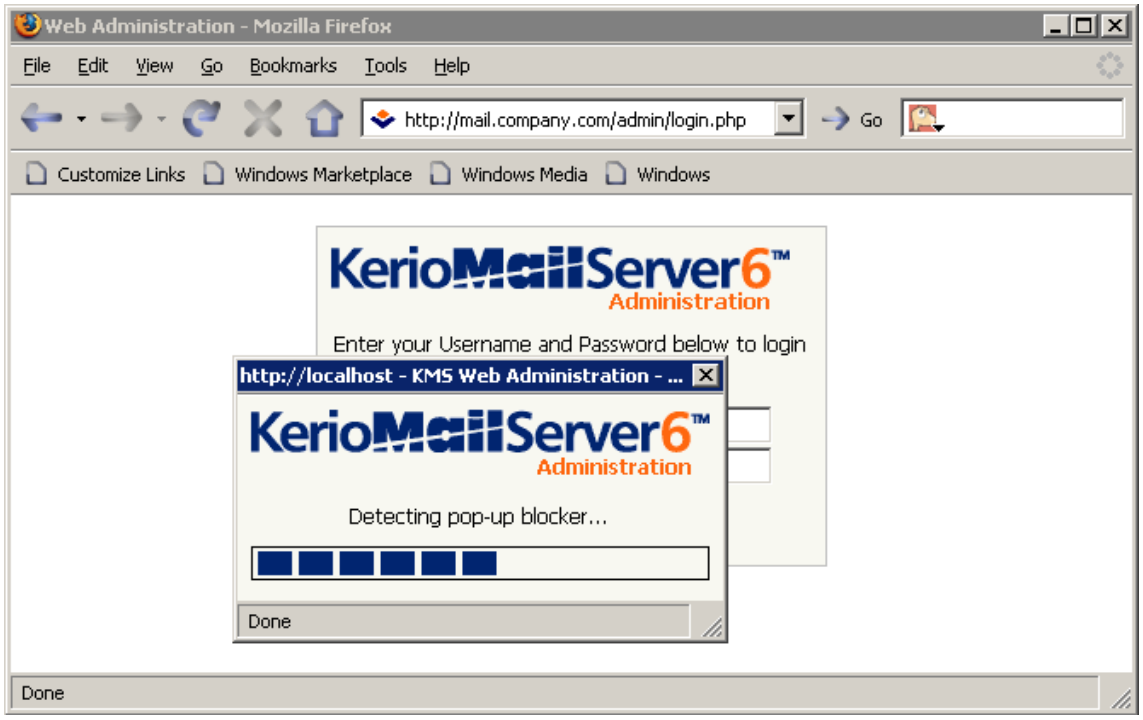

Figure 31.1 Pop-up killer detection

Figure 31.2 Welcome page with instructions how to set an exception for Kerio Web Administration

31.2 Setting access rights to the web interface

Special access rights which can be 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 particular domain. Besides users with special access rights, all users with full (read and write) rights for *Kerio MailServer* are also allowed to access the *KMS Web Administration*.

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.

Settings

KMS Web Administration access rights can be set as follows:

1. In the administration console, open the *Domain Settings* → *User Accounts* section.
2. Use the mouse pointer to select a user to whom the rights will be assigned.
3. Click on *Edit* to open the *Edit User* dialog and go to the *Rights* tab.

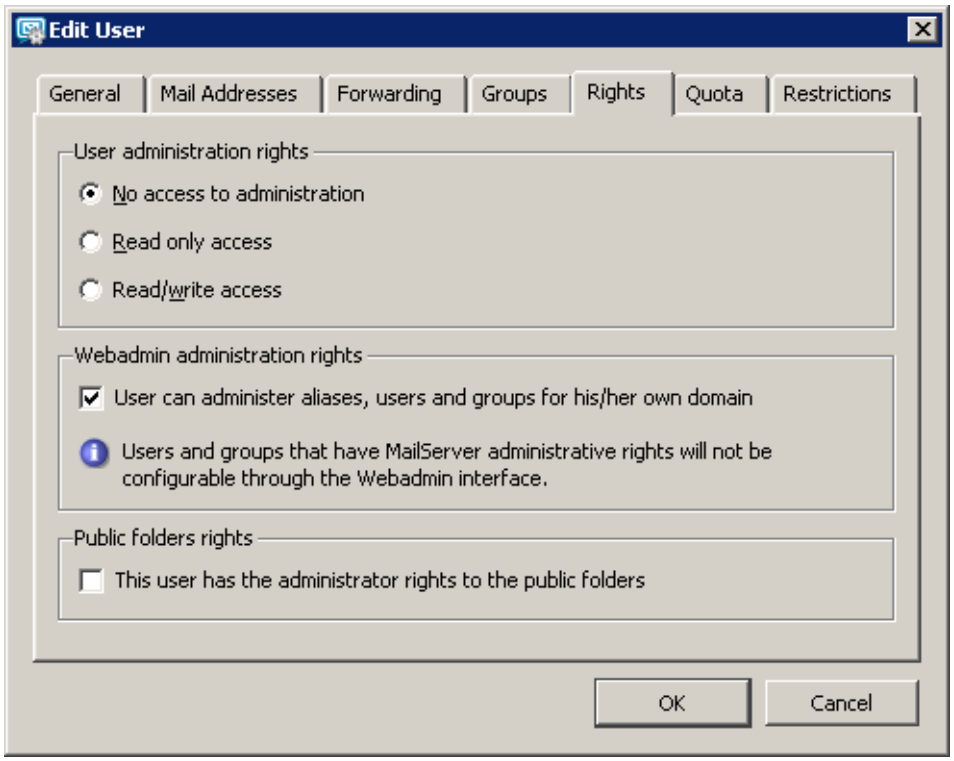

Figure 31.3 Setting user access rights for KMS Web Administration

4. Enable the *User can administer aliases, users and groups for his/her own domain* option (see figure 31.3).

5. Click *OK* to confirm changes.

31.3 Settings allowing 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 6) 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 12.3).

3. Web administration rights must be assigned to the user. To set these rights, go to the *Domain Settings* → *User Accounts* section. 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 31.2).

   The same right may be assigned also to an entire group of users (*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 7.2).

31.4 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 recommend 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).

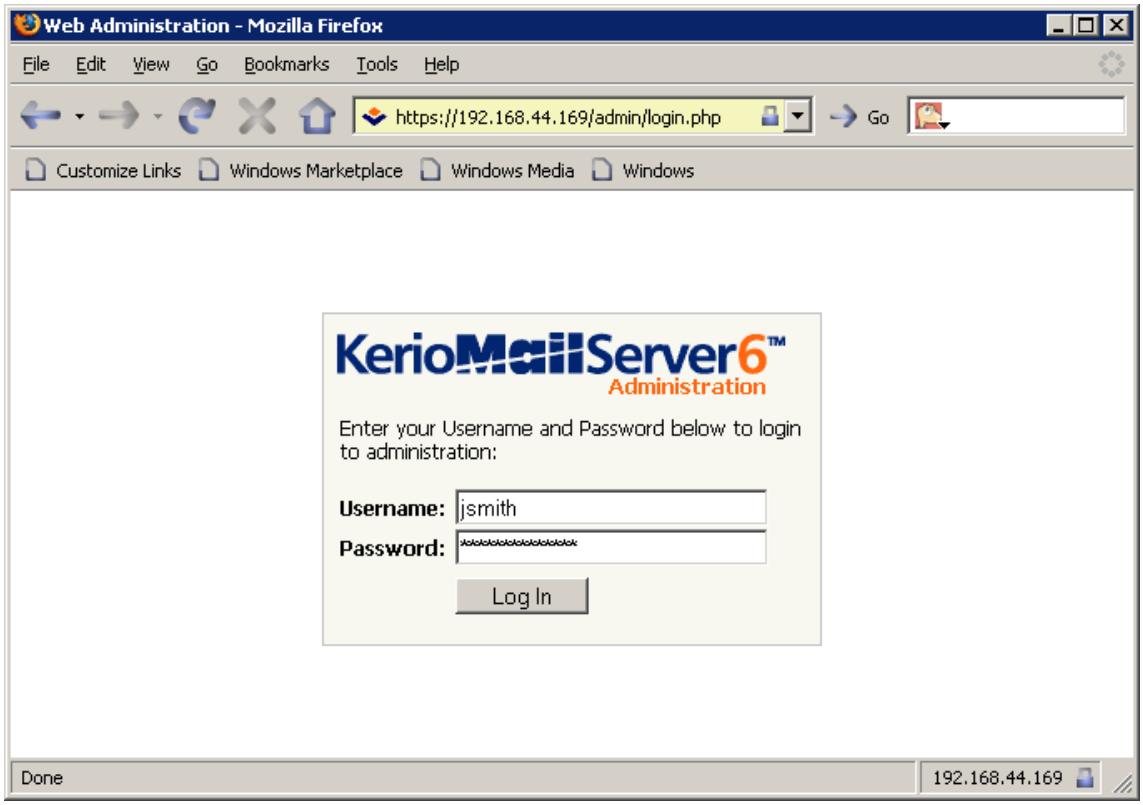

Figure 31.4 Web Administration Login

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.

31.5 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 upper right-hand corner, information is provided about the user and the domain which the user is allowed to administer (the user needs a valid account in the domain).

31.6 Welcome page

After a successful login to *KMS Web Administration*, the *Kerio MailServer* welcome page is opened. This page is divided into two parts:

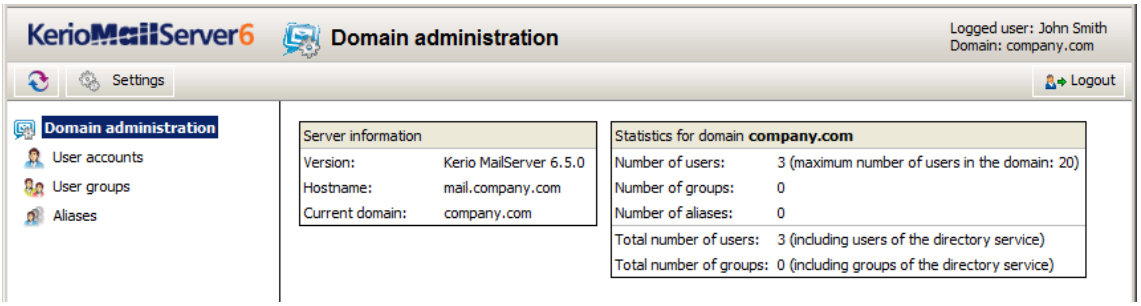

Figure 31.5 Main page

- The left pane of the window including a tree of sections does not change. The main section (the page that appears upon each connection) called *Domain administration* shows general information about the domain. The section includes three subsections — *User accounts*, *User groups* and *Aliases*.
- The right pane lists contents of the section previously selected in the left pane.

Domain administration

The *Domain administration* section contains two sections:

- Server information

  Version

  Kerio MailServer version information. To see more detailed information, click the *About* button on the left side of the toolbar.

  Host server 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.

- Statistics for domain
  A number of users, groups and aliases (only the aliases specified directly in the *Aliases* section are considered).

Below these tables, simple key for other *KMS Web Administration* subsections can be found.

Localizations of KMS Web Administration

KMS Web Administration interface is available in several language versions. Language can be switched after using the *Settings* button which can be found on the *KMS Web Administration* toolbar (see figure 31.6).

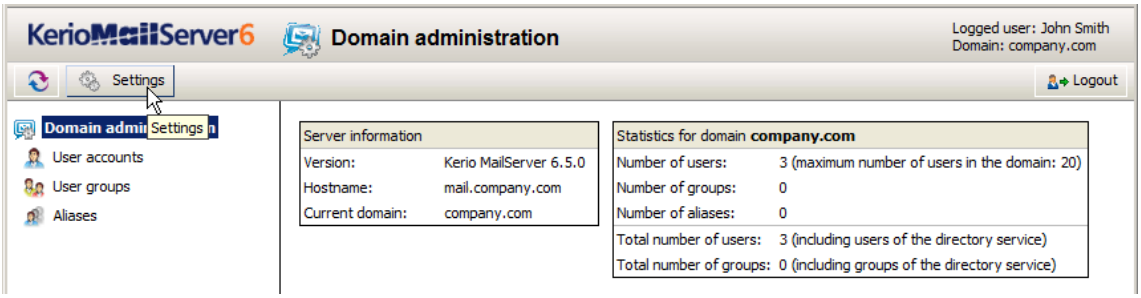

Figure 31.6 The Settings button

Click on the button to open the *Settings* dialog box (see figure 31.7) and select one of the following language versions:

- English
- Czech
- Chinese
- Italian
- Japanese
- German
- Portuguese
- Russian
- Slovak
- Spanish
- Dutch
- French

Save changes by the *OK* button.

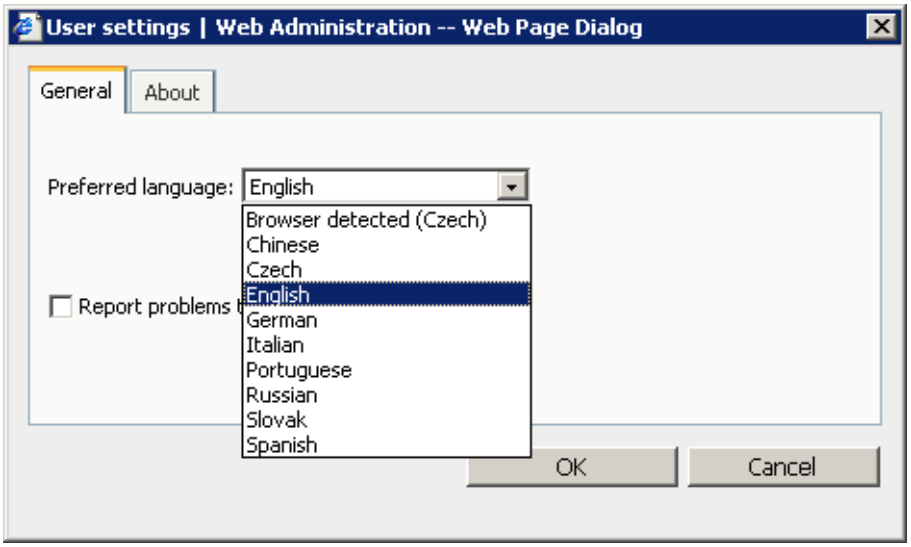

Figure 31.7 The Settings dialog box

31.7 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.

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:

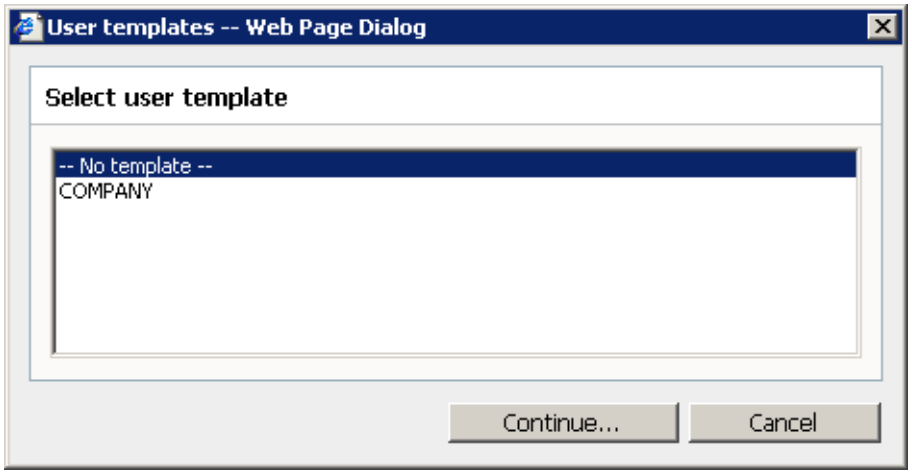

Figure 31.8 Template selection

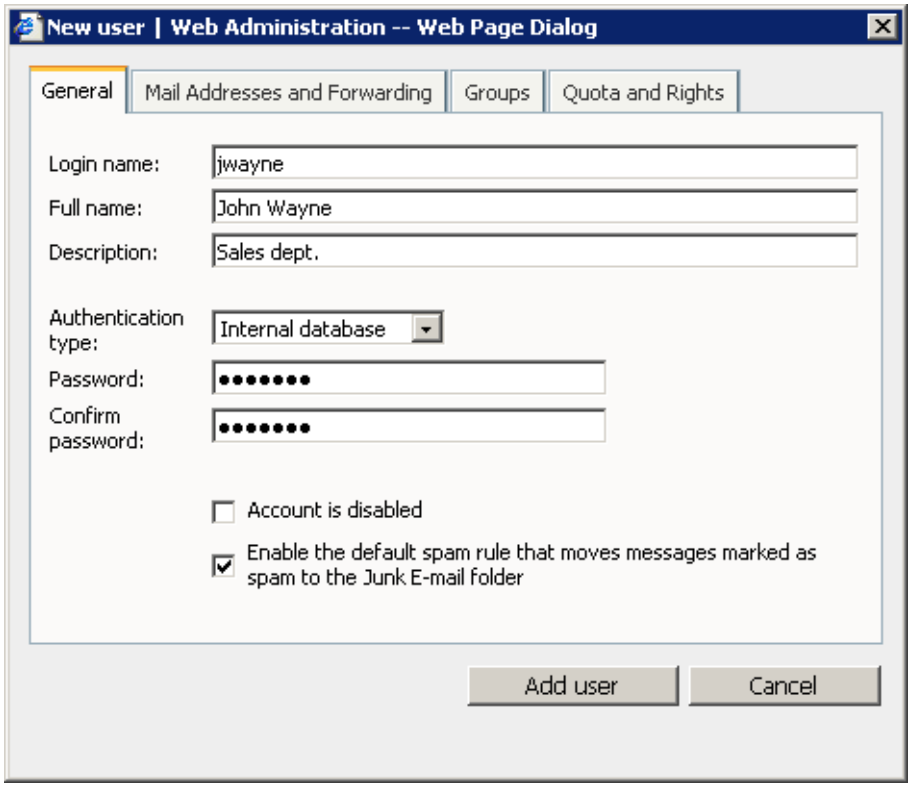

Figure 31.9 User administration — the General tab

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.

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

Authentication
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 filter ...
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.

Mail Addresses and Forwarding

List of additional email addresses
Multiple email addresses can be added to the list for a user mailbox. The primary user address (cannot be deleted) consists of the username and domain where the account is located (see figure 31.10). 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 31.9.

Forwarding settings
The *Mail Addresses and Forwarding* tab allows forwarding of messages to other email addresses. Click *Add* to add an address to which messages from this folder will be forwarded.

To enable forwarding of messages to listed addresses while keeping these messages in the mailbox, enable the *Deliver messages to both mailbox and forwarding addresses* option (otherwise, forwarded messages will not be saved in the mailbox).

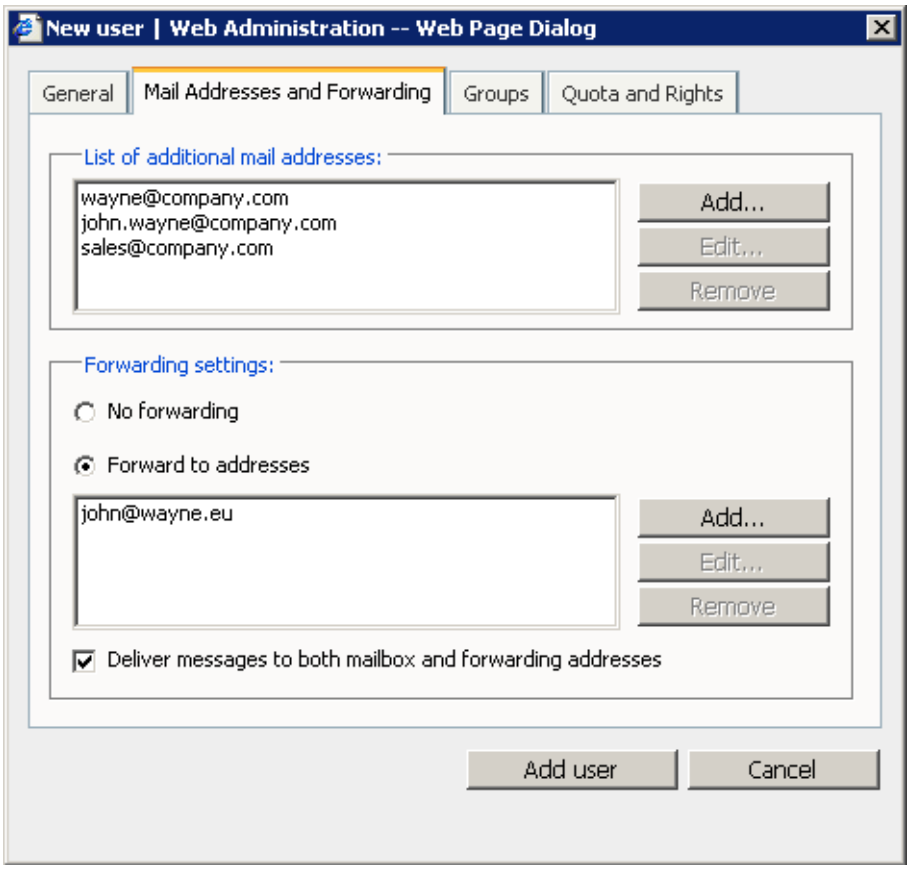

Figure 31.10 User administration — the Mail Addresses and Forwarding tab

User groups

On the *Groups* tab, you can use the *Add* and *Remove selection* buttons to add or remove groups of which the user is a member. First, create the desired group in *Groups* section (see chapter 31.8). 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.

Quota and Rights

You can specify restrictions and rights 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.

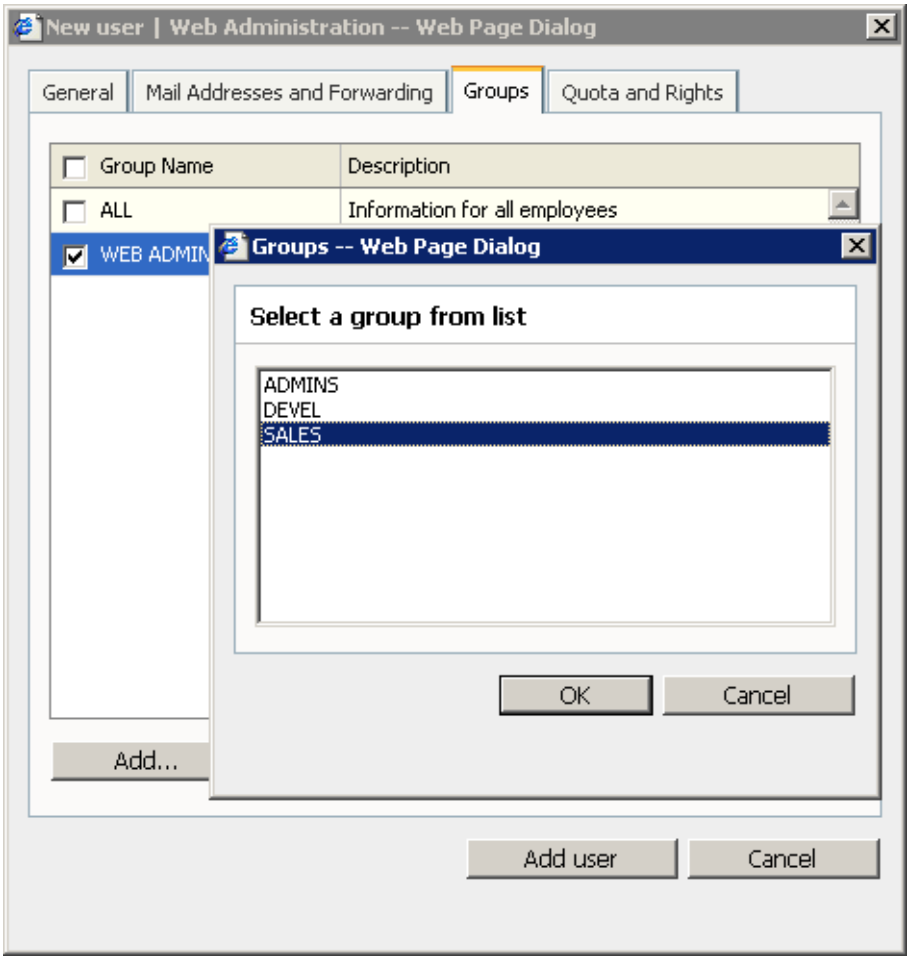

Figure 31.11 User administration — the Groups tab

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*).

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.

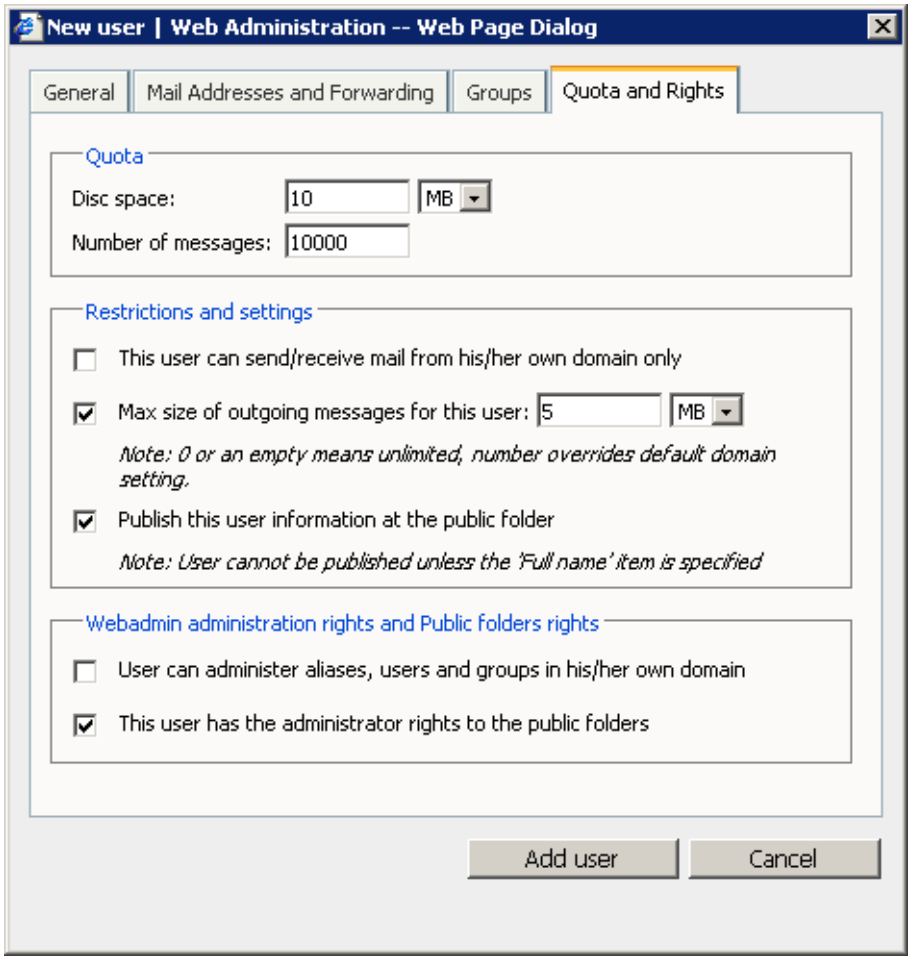

Figure 31.12 User administration — the Quota and Rights tab

Restrictions and 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.

Max size of outgoing messages

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.

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 and Public folder rights

This user has the administrator rights...
A special access right to *KMS 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.

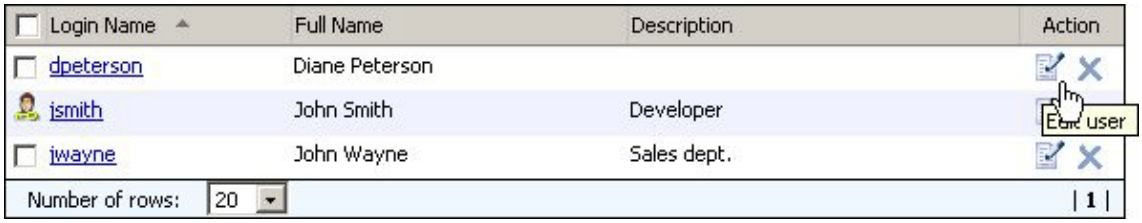

Figure 31.13 User account editing

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.

Move user's message folder to an account of another user...
This option is useful especially when another user needs to work with messages, events and tasks from this folder.

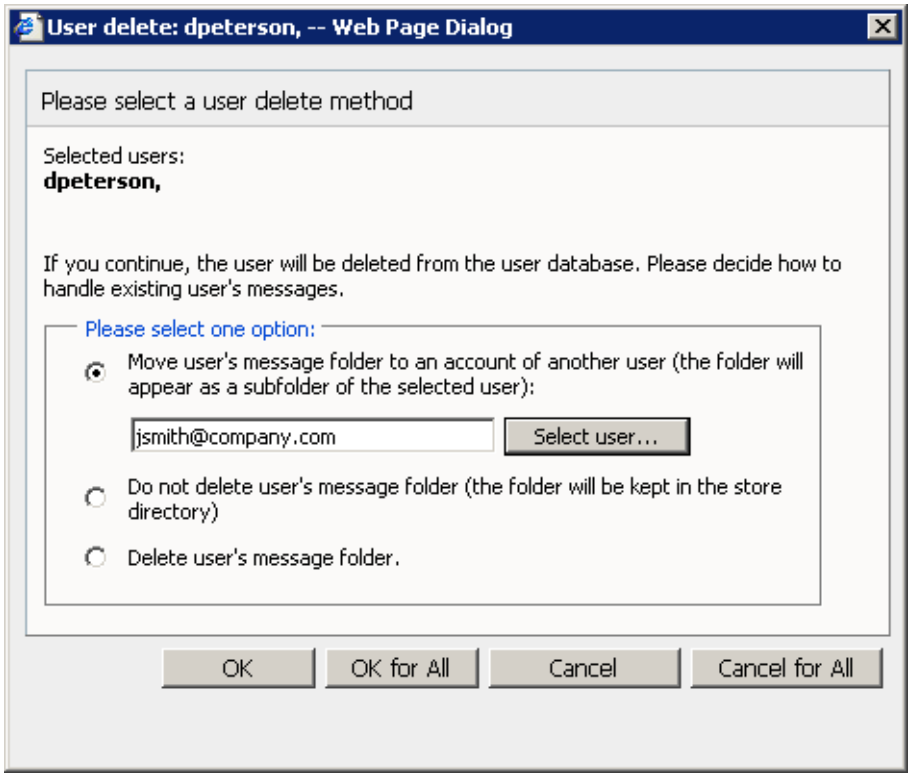

Figure 31.14 Remove user dialog

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 recorded in the *Warning* log in *Kerio MailServer*.

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 *KMS Web Administration*. However, the data of such accounts cannot be edited. It is, however, possible to avoid this problem by using the *Show only users from internal database (hide users from directory service)* option to hide all mapped users.

31.8 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 31.9) — 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:

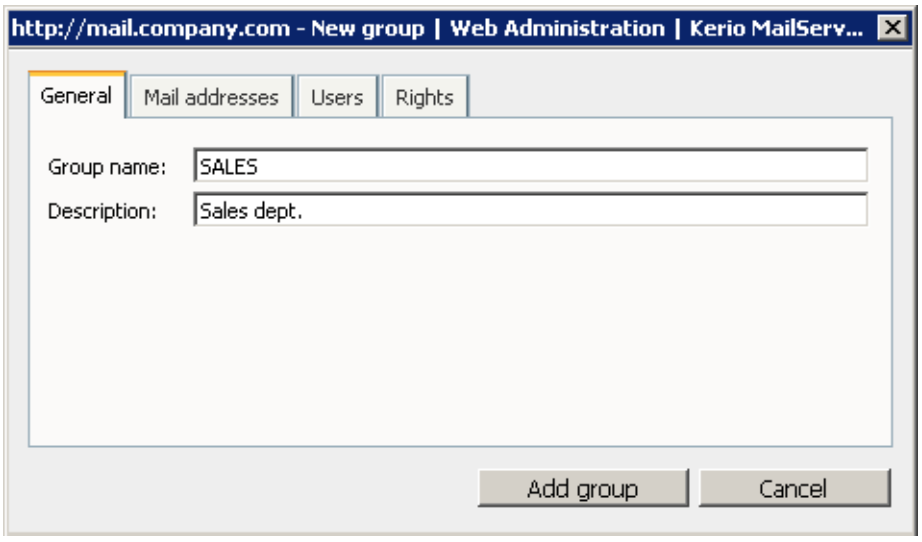

Figure 31.15 Group management — the General tab

Group name
Unique name of the group.

Description
Description of the group; may be left blank.

Mail Addresses

On this tab it is possible to define 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 31.16). Assign these addresses to the three salesmen in the *Users* tab (see picture 31.17).

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).

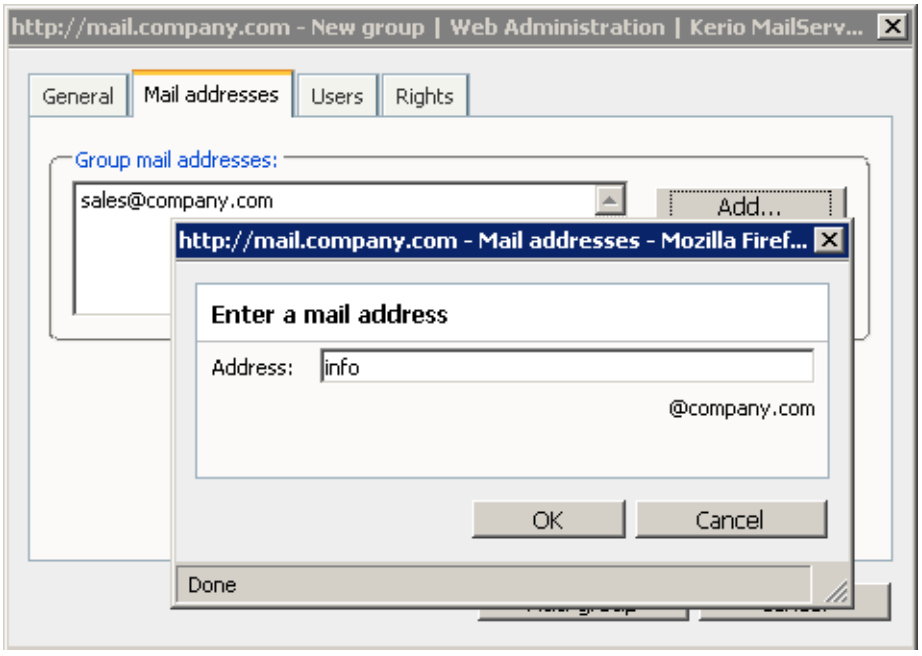

Figure 31.16 Group administration — the Mail Addresses tab

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.

Users

Using the *Add* and *Remove selection* buttons you can add or remove users to/from the 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 31.7).

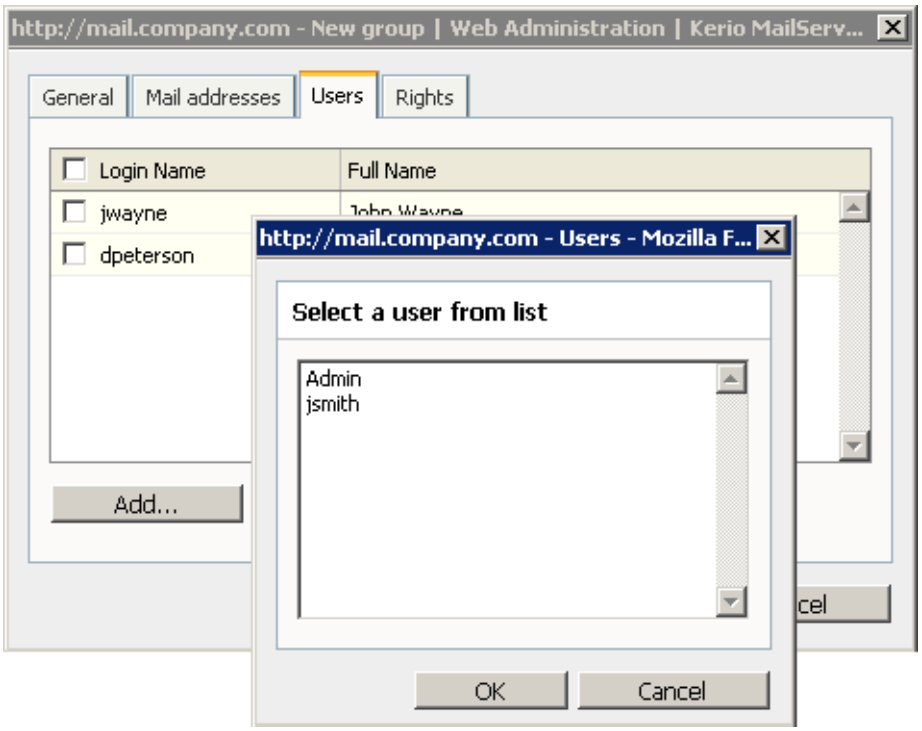

Figure 31.17 Group management — the Users tab

Rights

The *Rights* tab allows administrators setting of the following rights:

Users 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.

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.

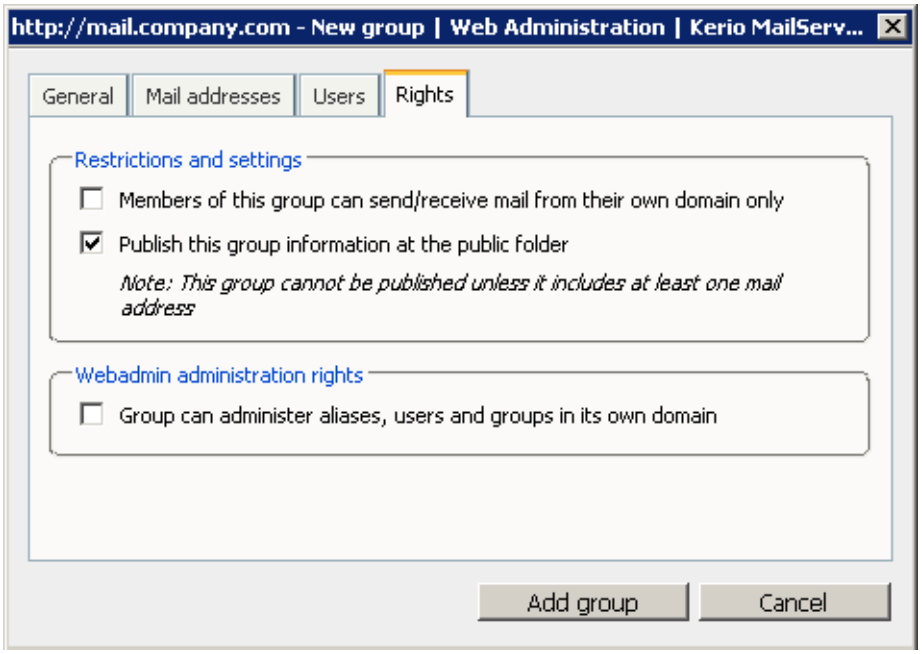

Figure 31.18 Group management — the Rights tab

Group can administer...
: A special group access right to *KMS Web Administration*. This setting is independent on the access rights settings for *Kerio Administration Console*.

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.

Remove group

The *Remove* 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 *KMS Web Administration*. However, the data of such groups cannot be edited. It is, however, possible to avoid this problem by using the *Show only groups from internal database (hide groups from directory service)* option to hide all mapped groups.

31.9 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).

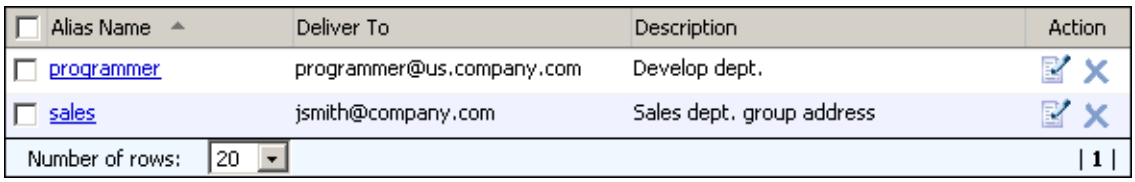

Figure 31.19 Aliases

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 31.20). 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 31.7), or group definition (see chapter 31.8).

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.

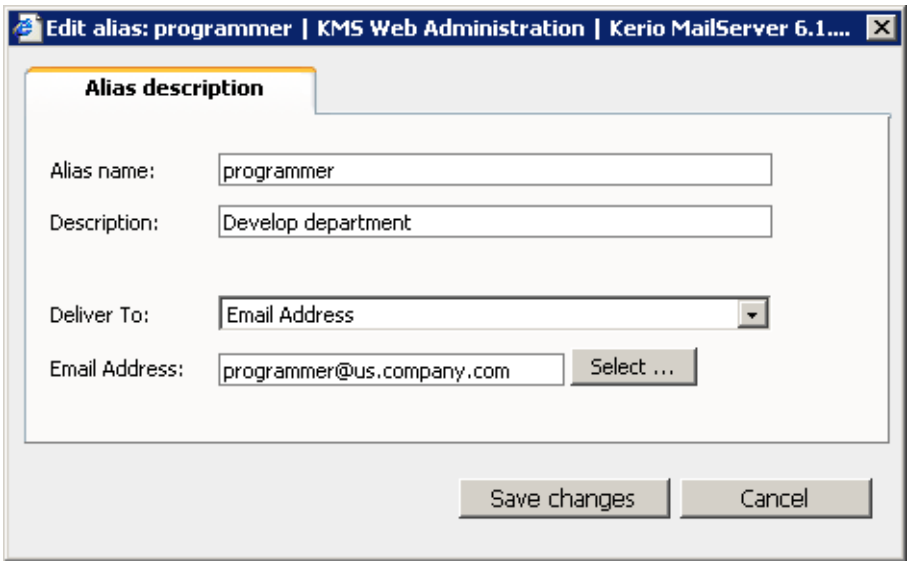

Figure 31.20 Alias creation dialog

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:

- *Email Address* — any (user or group) email address. Click *Select* to select a user or a group from the list.
  Note: If no email address is specified for the group, it will be set automatically, following this pattern:

  `group_name@domain`

- *Public Folder* — public folder name in the following format: `#public/Folder`.

Click the *Delete* button 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 32

Kerio Outlook Connector

Kerio Outlook Connector is a special module for *MS Outlook* extending cooperation between *Kerio MailServer* and *MS Outlook*. This module helps keep data which must be available to users saved on the server. This data include email folders, calendars, tasks, contacts, notes as well as public folders.

Along with *Kerio MailServer 6.5.0*, *Kerio Technologies* released besides the standard *Kerio Outlook Connector* also the new *Kerio Outlook Connector (Offline Edition)*. *Kerio Outlook Connector (Offline Edition)* brings many advantages lacked in *Kerio Outlook Connector*. As suggested by the name of the module, the main advantage of *Kerio Outlook Connector (Offline Edition)* is working offline in *MS Outlook*, most useful probably for notebook users. Other advantages are searching through message bodies and so called grouping. For more information on *Kerio Outlook Connector*, see section 32.1.

It is recommended to use the standard version of *Kerio Outlook Connector* especially if you use *MS Outlook 2000* since *Kerio Outlook Connector (Offline Edition)* requires *MS Outlook XP* and higher. For more information on *Kerio Outlook Connector*, see section 32.2.

32.1 Kerio Outlook Connector (Offline Edition)

Kerio Outlook Connector (Offline Edition) provides the following features:

- Email, events, notes, contacts and tasks are stored in *Kerio MailServer*. Therefore, they are available via the Internet from anywhere. You can connect either by *MS Outlook*, by *Kerio WebMail* or via another email client.
- *MS Outlook* can be switched to offline mode. This implies that you can manage your email items also from home or on your business trips. This means that your email can be managed even there where the Internet connection is too slow or there is no connection at all. After reconnection to the Internet (switching to online mode), *Kerio Outlook Connector (Offline Edition)* synchronizes all changes with the mailserver and sends mail from *Outbox*. The description indicates that this feature will be used mainly by notebook users. For email management anywhere, simply open the *MS Outlook* and start working.
- *Kerio Outlook Connector (Offline Edition)* supports folder management. In *MS Outlook*, it is possible to create hierarchized folder trees of any depth. Folder sharing, viewing of shared folders and other features are also supported.

- In calendars, meeting scheduling and, in task folders, assigning of tasks to other persons are supported.
- *Kerio Outlook Connector* allows setting of rules for incoming email. These rules are stored at the server, so they are applied globally — i.e. mail will be sorted in the same way in *Kerio WebMail* and other email clients.
- *Kerio Outlook Connector* provides a proprietary antispam strategy.
- *Kerio Outlook Connector* allows searching in message bodies.
- *Kerio Outlook Connector* provides support for message grouping.

Note: The chapter describes settings in *MS Outlook 2007*. It can, therefore, slightly differ on older versions of *MS Outlook*.

For correct functioning of the module, the *HTTP(S)* service must be running in *Kerio MailServer* — this protocol is used for any traffic from and to *Kerio MailServer*.

Kerio Outlook Connector is available in the following language versions:

- English
- Czech
- Chinese
- French
- Dutch
- Croatian
- Italian
- Japanese
- Hungarian
- German
- Polish
- Portuguese
- Russian
- Slovak
- Spanish
- Swedish

Language of the *Kerio Outlook Connector* is set automatically in accordance with the language version set in *MS Outlook*. If a language set *MS Outlook* is not available in the *Kerio Outlook Connector*, English is used automatically.

MS Outlook options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*. This file is available at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

32.1.1 Installation

Kerio Outlook Connector can be installed at the following operating systems:

- Windows XP
- Windows Vista (32 and 64 bits) with the recent Service Pack installed

Installation of the *Kerio Outlook Connector* can be run with the following versions of *MS Outlook*:

- MS Outlook XP + version Service Pack 3 (the version of *Outlook XP* must have this format: `10.0.6515.xyz`).
- MS Outlook 2003 + version Service Pack 2 (if the service pack version is not installed, *Kerio Outlook Connector* installation cannot be started).
- MS Outlook 2007 + version Service Pack 1

Kerio Outlook Connector (Offline Edition) requires Internet Explorer 6.0 or higher.

Warning: Kerio Outlook Connector (Offline edition) communicates with the server via the MAPI based on HTTP(S) protocol. Therefore, it is necessary to run HTTP(S) service on the server and map the corresponding port(s) on the firewall protecting the server.

Installation wizard is used for the *Kerio Outlook Connector* installation. Once the installation is completed, it is necessary to set a profile and an email account explicitly.

Warning:

- *MS Outlook* must be installed on the computer prior to the *Kerio Outlook Connector (Offline Edition)* installation, otherwise the application will not function properly.
- When the upgrade or downgrade of *MS Outlook* is performed, *Kerio Outlook Connector* must be reinstalled manually.

Installation on computers where Kerio Outlook Connector has been installed

In the majority of cases, upgrade from *Kerio Outlook Connector* to *Kerio Outlook Connector (Offline Edition)* is smooth. At the beginning of the installation, a convertor is started which converts all *Kerio Outlook Connector* profiles of the particular user to profiles for *Kerio Outlook Connector (Offline Edition)*. If the station is connected to the Internet, *Kerio Outlook Connector (Offline Edition)* local database is created automatically and updated..

Special cases:

One workstation is shared by multiple users

If a workstation is used by multiple users, install the program once and then run the conventor (*Start* → *Programs* → *Kerio* → *Outlook Profile Conversion Utility*) for each user.

Kerio Outlook Connector is installed without connection to Kerio MailServer

In such cases profiles are converted, but they must be finished upon connecting to the server:

1. In the profiles dialog (*Start* → *Settings* → *Control Panel* → *Mail* → *View Profiles*), select the Kerio profile and click on *Properties*.
2. In the wizard, click on *User Accounts*.
3. On the following page, double-click on the Kerio account and confirm settings by the *OK* button. Konversion to *Kerio Outlook Connector (Offline Edition)* profile is then finished automatically.

This procedure must be taken for each profile with Kerio account.

Profile and Email account settings

The user profile is a file where personal information in *MS Outlook* is stored. In *MS Outlook*, any number of user profiles can be created. Using of multiple user profiles is essential especially 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. In other cases, one profile for one or more email accounts is sufficient.

Settings for a new profile can be configured in the *Start* → *Settings* → *Control Panel* → *Mail* menu:

1. In the *Email Settings* dialog, select the Profiles button.

2. Click on the *Add* button to create a new profile and enter its name. Any name can be used.

3. This opens the email account wizard, where a new account can be created. In the dialog, simply enable the *Manually configure server settings or additional server types* option.

4. In the *Choose e-mail service* dialog, select the Other option and enable *Kerio MailServer (KOC Offline Edition)* (see figure 32.1). Click on *Next*.

5. On the *Accounts* tab set basic parameters for connection to the mailserver (see figure 32.2):

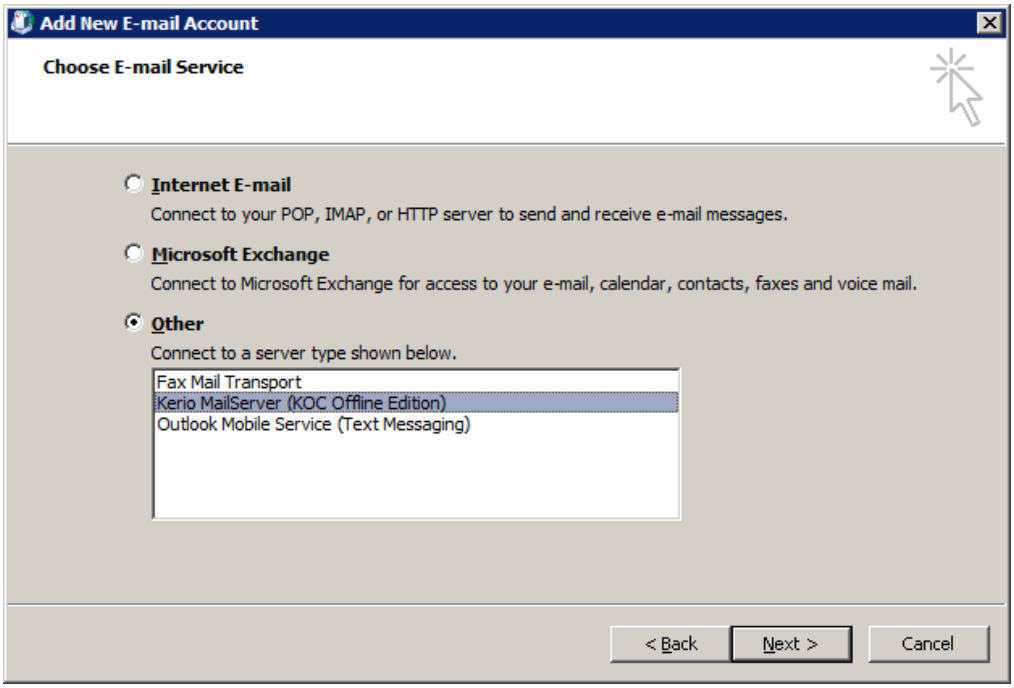

Figure 32.1 New account settings — e-mail service selection

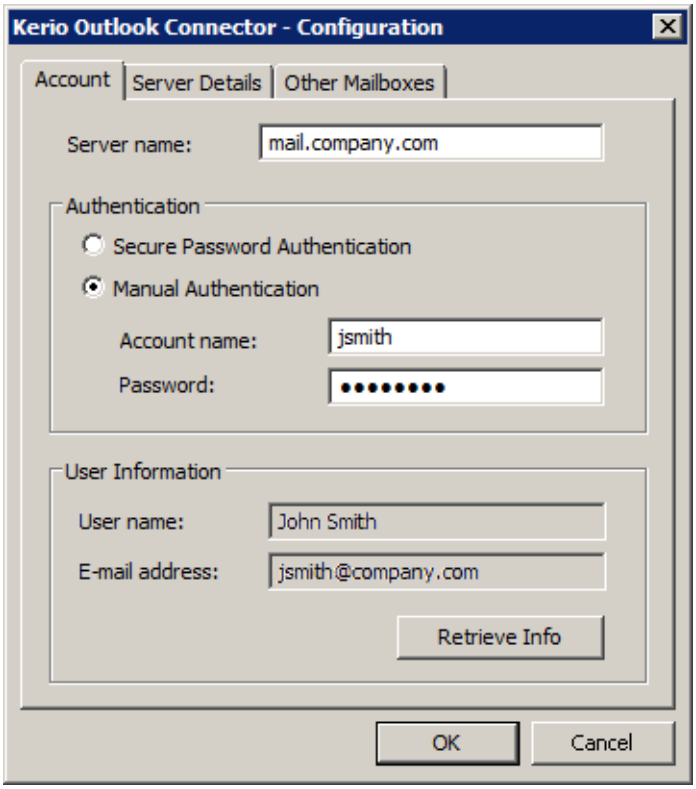

Figure 32.2 New account settings

Server Name

DNS name or IP address of the MailServer.

Secure Password Authentication

This option allows using the NTLM authentication. When checked, users are not required to set usernames and passwords — the authentication against the *Active Directory* domain will be used instead authentication through username and password.

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.

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`).

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.

6. Settings on the *Server Details* tab depend on security policy set on the server. By default, any traffic between *Kerio MailServer* and *MS Outlook* is secured by SSL. It is highly recommended to not change these settings.

   Warning: SSL-secured traffic requires installation of an SSL certificate issued by a trustworthy certification authority.

Automatic updates

Upgrades of *Kerio Outlook Connector* are performed automatically. If a new version of *Kerio Outlook Connector* is available, the module is updated immediately upon the startup of *MS Outlook*.

Warning: When the update is completed, *MS Outlook* is restarted automatically.

The update process and the restart takes up to two minutes.

The automatic update includes check of versions of *Kerio MailServer* and the *Kerio Outlook Connector*. If versions of the server and the client do not match, the user is informed that a different version of *Kerio MailServer* is installed on the server and that the client should be updated. Upon confirmation, the version is upgraded/updated immediately (or downgraded).

Note: If the server and client differ only in their build numbers (numbers in the notification are the same), the client will work even if the update is rejected. If, however, version numbers are different (for example `6.5.0` versus `6.5.1`), *Kerio Outlook Connector* cannot be started unless updated.

32.1.2 The Online/Offline mode

Kerio Outlook Connector (Offline Edition) supports both modes, online and offline. Online mode is the standard *MS Outlook*mode which requires connection to the Internet. Offline mode allows running of *MS Outlook* and working there without connection to the Internet. This requires all email, events, tasks, etc. being stored in the local message store on the client station. Upon connection to the Internet, it is possible to synchronized changes with the corresponding account in *Kerio MailServer*.

The offline mode is helpful especially for users with notebooks who make frequent business trips and need their email accounts even when they are not currently connected

to the Internet. Upon switching to online mode, all new messages, events and tasks are synchronized with the server's store automatically.

By default, the online mode is set in *MS Outlook*. To switch to the offline mode, click on *Work offline* in the *File* menu available on the main toolbar.

If you close*MS Outlook* in the offline mode, it will be opened in offline mode next time it is started. If you want to change this, disable the offline mode manually in the *File* menu.

Kerio Outlook Connector (Offline Edition) informs of switching between online and offline modes and about current synchronization progress and status by a special icon in the systray's notification area (*σεε φιγθρε* 32.3). The icon informs about the following situations:

Figure 32.3 Synchronization status

- Synchronization in progress — arrows are displayed at the icon.
- *MS Outlook* is running in the offline mode — grey down-arrow is displayed at the icon.
- *MS Outlook* lost connection to the server — red cross is displayed over the icon.

If the synchronization is not running and *MS Outlook* is running in the online mode, the icon is hidden.

Synchronization

Any folder saved in *Kerio MailServer* can be synchronized in any of these two modes:

- Full synchronization of the folder.
- Synchronization of message header and body in plain text.

In default mode, synchronization of *Kerio MailServer* and the *Kerio Outlook Connector* works as follows:

- Inbox — whole messages are synchronized.
- Other email folders — only message headers and body in plain text are synchronized.
- Events — whole events are synchronized.
- Contacts — whole contacts are synchronized.
- Tasks — whole tasks are synchronized.
- Notes — whole notes are synchronized.

Default synchronization mode can be changed (adjusted) in properties of individual folders:

1. Right-click the selected folder and choose *Properties* from the pop-up menu.

2. In the *Properties* window switch to the *Folder Synchronization* tab (see figure 32.4).

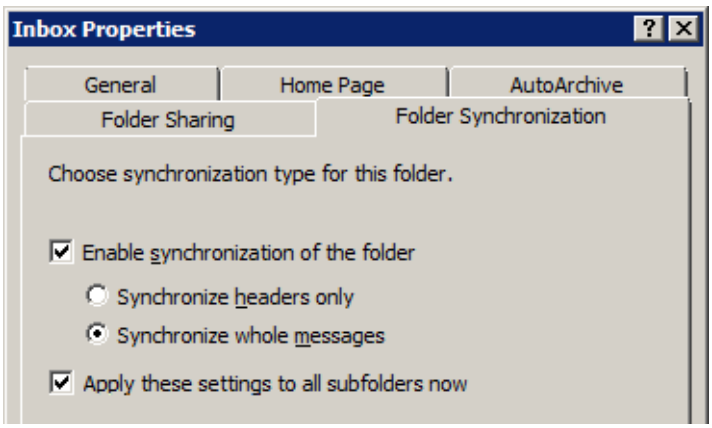

Figure 32.4 Folder synchronization settings

Warning: If you do not wish to synchronize the folder at all, disable the *Enable synchronization of the folder* option. However, any items already included in the folder will be kept synchronized.

Conflicts

Conflicts are situations where a message, event or another item is changed separately both on the server and in *Kerio Outlook Connector* in the interval between synchronizations (synchronization is started in defined periods). In such cases, the server is not capable of recognizing which change is the wanted (later) one.

If a conflict occurs during synchronization, the winning item (the one selected to overwrite the other) is saved to a corresponding delivery folder. The beaten item is saved in a special folder called *Conflicts*. This folder is available only in *MS Outlook*. This implies that it is not available in *Kerio WebMail* or another email client.

Both items can be easily compared to select the correct one. If the server have primarily selected the wrong version (the older one), it is possible to move it from the *Conflicts* folder to the correct directory manually and simply remove the other version.

Each conflict is announced by a special message sent to *MS Outlook*. Its subject is *Message in conflict!*. Conflict information includes name of the message, event, contact or another item in conflict and its location in mailbox (folder). Local version of the item is

moved to the *Conflicts* folder. If this version is up-to-date, exchange it with the version in the particular folder.

32.2 Kerio Outlook Connector

Kerio Outlook Connector provides the following features:

- Email, events, notes, contacts and tasks are stored in *Kerio MailServer*. Therefore, they are available via the Internet from anywhere. You can connect either by *MS Outlook*, by *Kerio WebMail* or via another email client.
- *Kerio Outlook Connector* supports folder management. In *MS Outlook*, it is possible to create hierarchized folder trees of any depth. Folder sharing, viewing of shared folders and other features are also supported.
- In calendars, meeting scheduling and, in task folders, assigning of tasks to other persons are supported.
- *Kerio Outlook Connector* allows setting of rules for incoming email. These rules are stored at the server, so they are applied globally — i.e. mail will be sorted in the same way in *Kerio WebMail* and other email clients.
- *Kerio Outlook Connector* provides a proprietary antispam strategy.

Kerio Outlook Connector also includes *Help* which can be triggered from the *MS Outlook's* toolbar (*Help* → *Kerio Outlook Connector Help*).

Kerio MailServer, *MS Outlook* and *Kerio Outlook Connector* communicate via *Microsoft's* open MAPI interface. 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 (*MS Outlook* and *Kerio MailServer* in this case). MAPI is used especially for writing of various modules for *MS Outlook*.

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.

Warning: In addition to the services listed above, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

Installation of the *Kerio Outlook Connector* can be run under Windows 2000 Professional (version Service Pack 4), XP (version Service Pack 1 or Service Pack 2) and Windows Vista (Home, Business, Enterprise or Ultimate editions).

The Windows OS must include Internet Explorer 6.0 or higher.

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 *Outlook XP* must have this format: `10.0.6515.xyz`).
- MS Outlook 2003 + version Service Pack 2 (if the service pack version is not installed, *Kerio Outlook Connector* installation cannot be started).
- MS Outlook 2007 + version Service Pack 1

Notes:

- All settings relate to *Windows XP* and *MS Outlook 2003*. If you use a different version of *MS Outlook 2000*, the settings may differ (see *Kerio MailServer, User's Guide*).
- *Kerio Outlook Connector* provides support for digital signatures. The function and settings for digital signatures are described in standard *MS Outlook* help.

Kerio Outlook Connector options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

TIP: If you need to work with your email also offline, replace the standard *Kerio Outlook Connector* by the *Kerio Outlook Connector (Offline Edition)* (see chapter 32.1).

Installation of the *Kerio Outlook Connector* can be run either independently or along with *Kerio MailServer Migration*.

Kerio Outlook Connector is available in the following language versions:

- English
- Czech
- Chinese
- French
- Dutch
- Croatian
- Italian
- Japanese
- Hungarian
- German
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Language of the *Kerio Outlook Connector* is set automatically in accordance with the language version set in *MS Outlook*. If a language set *MS Outlook* is not available in the *Kerio Outlook Connector*, English is used automatically.

32.2.1 Installation and configuration without the migration tool

Manual installation of the *Kerio Outlook Connector* for *Kerio MailServer* is performed by the installation wizard. Once the installation is completed, it is necessary to set a profile and an email account explicitly.

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 manually.

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:

1. In the just opened *Mail Setup — Outlook* dialog, click on *Show Profiles* (see figure 32.5).

2. The *Mail* dialog is opened (see figure 32.6) where profiles and user accounts may be administered.

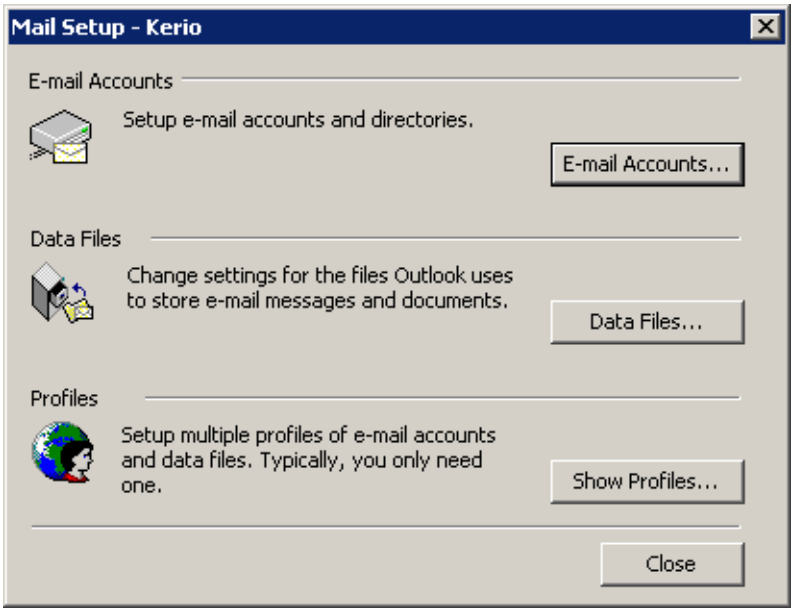

Figure 32.5 Profile setup

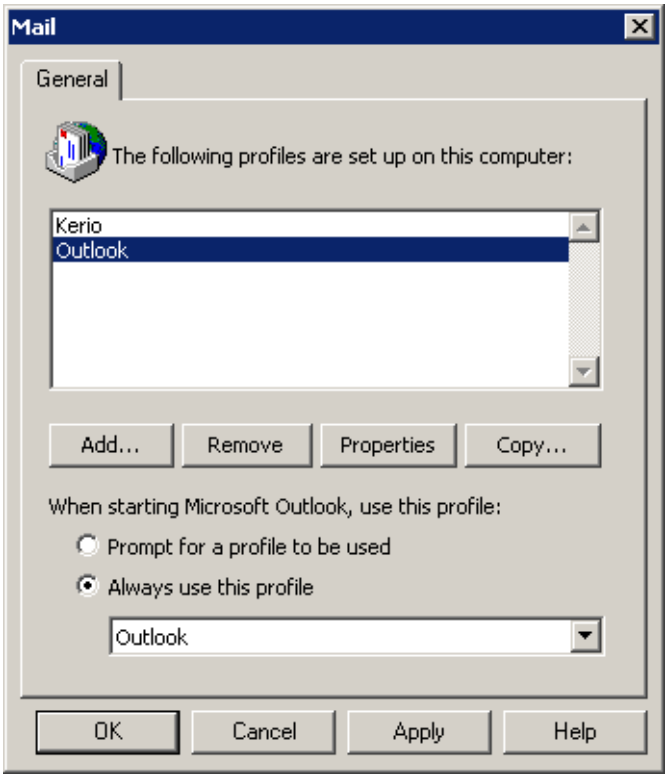

Figure 32.6 Creation of a profile

3. Click on *Add*. A dialog box is opened with a blank entry for specification of the new

profile's name. Any string is allowed as the name. At figure 32.7, the name entered is `Kerio`. Click *OK* to confirm settings and save the profile.

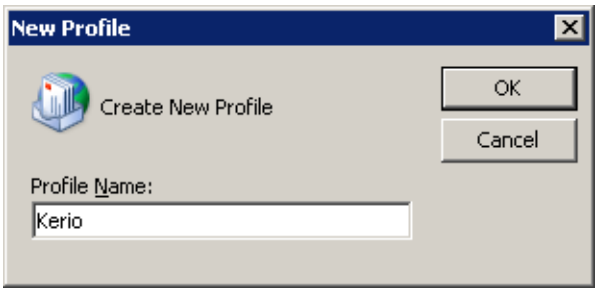

Figure 32.7 New profile

4. The new profile is empty (i.e. no email account is created in it). Therefore, the wizard where a new account can be created is started automatically once a new profile is created.

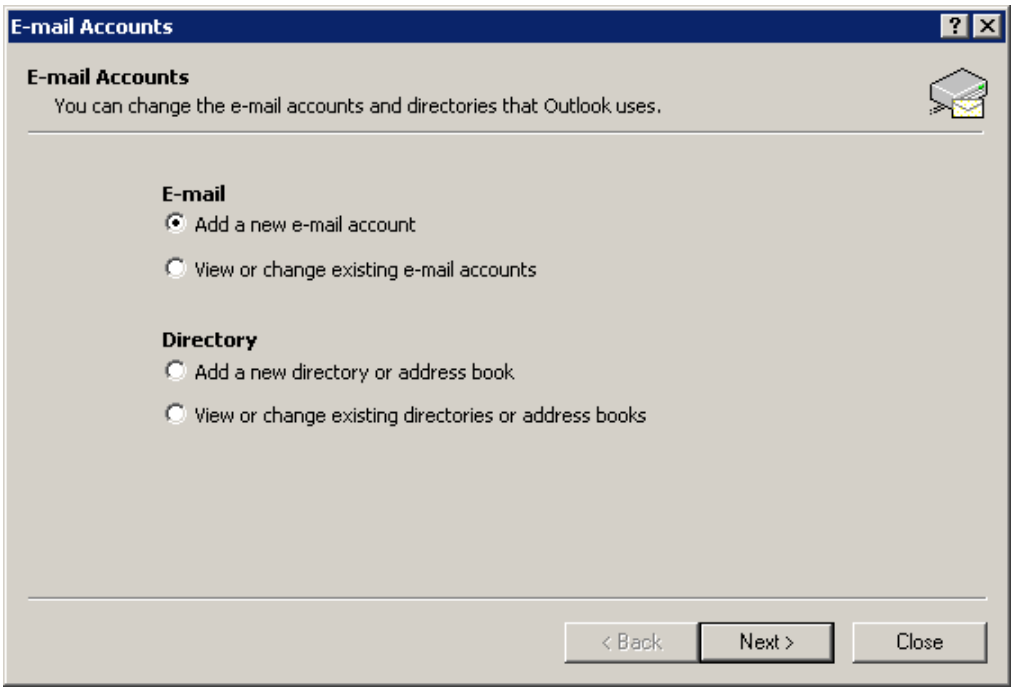

Figure 32.8 Account settings — creation of new account

Email accounts or an address book can be added or changed in the first dialog of the wizard. Once you create an account, select — *Add a new email account* (see figure 32.8).

5. In dialog two, select the *Additional server types* option (see figure 32.9) and click on *Next*.

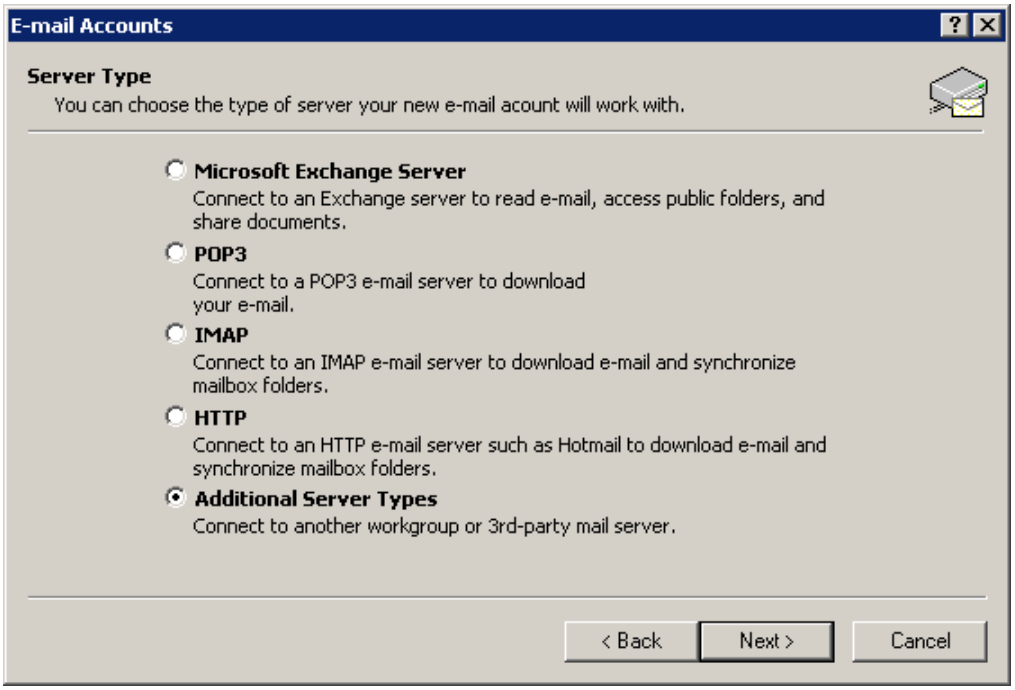

Figure 32.9 Account settings — server type selection

6. In the next dialog, server type can be selected (see figure 32.10). Select the *Kerio MailServer* option (it is often the only option offered here).

7. 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:

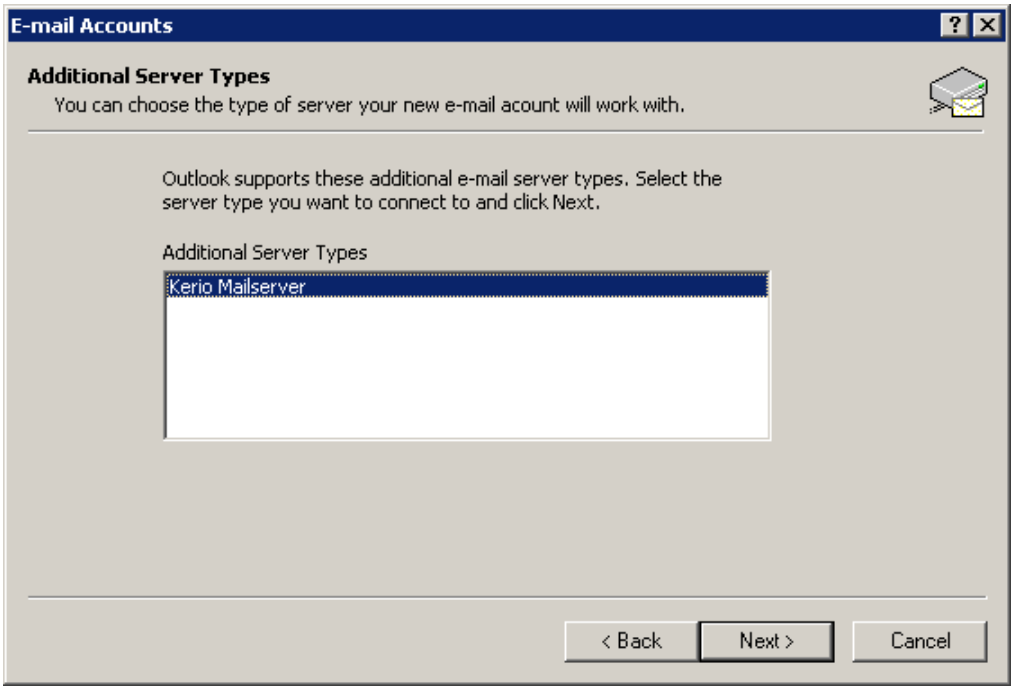

Figure 32.10 Account settings — Kerio MailServer selection

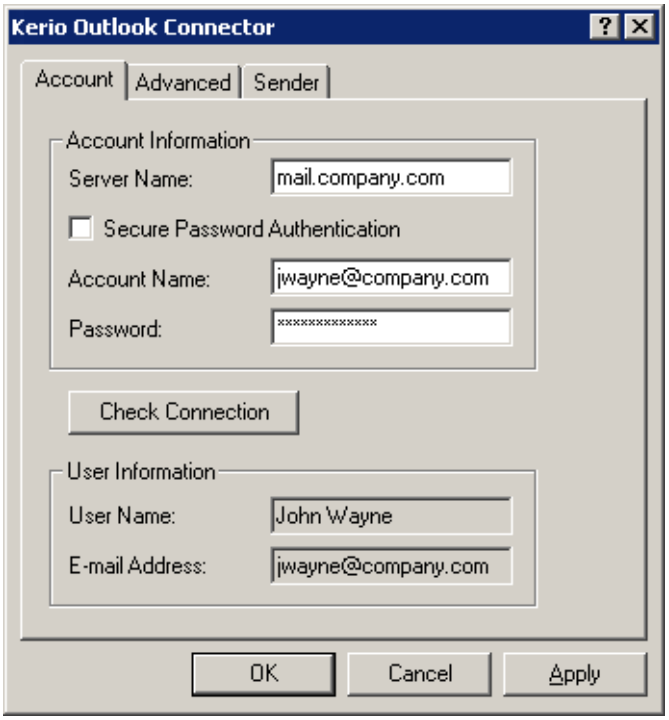

Figure 32.11 Account settings — connection settings

Server Name
DNS name or IP address of the MailServer.

Secure Password Authentication
This option allows using the NTLM authentication. When checked, users are not required to set usernames and passwords — the authentication against the *Active Directory* domain will be used instead authentication through username and password.
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.

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`).

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.

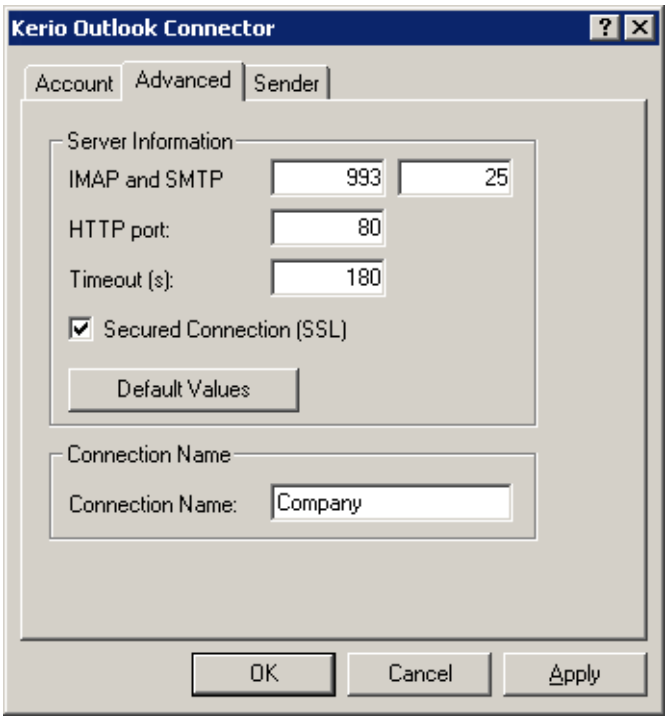

Figure 32.12 Account settings — ports

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*.

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.

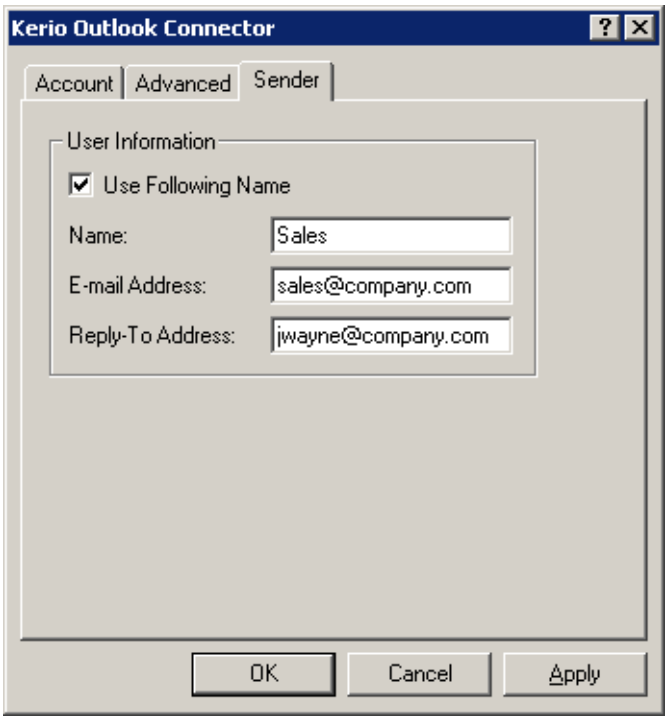

Figure 32.13 Account settings — sender information settings

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 MS Outlook 2000 is used, changes performed on the Sender tab will take effect after a restart of the application.

8. Click *OK* to confirm and save the settings and to close the wizard. The profile created can be found in the list provided on the *Mail* page. Now, two options of profile modes are available (see figure 32.6):

- *Always use this profile* — this option sets the new profile as default. Then, the profile including the new account is opened automatically upon each startup of *MS Outlook*.
- *Prompt for a profile to be used* — if this option is used, a menu is opened providing a list of all profiles (see figure 32.14). Upon each startup of *MS Outlook*, one of these profiles can be selected.

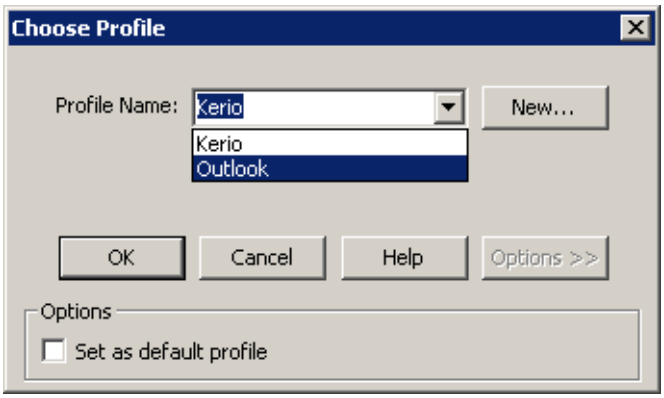

Figure 32.14 Choose Profile

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* and *Outlook Address Book* items during configuration. In higher versions of *MS Outlook*, *Outlook Address Book* is added automatically.

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.

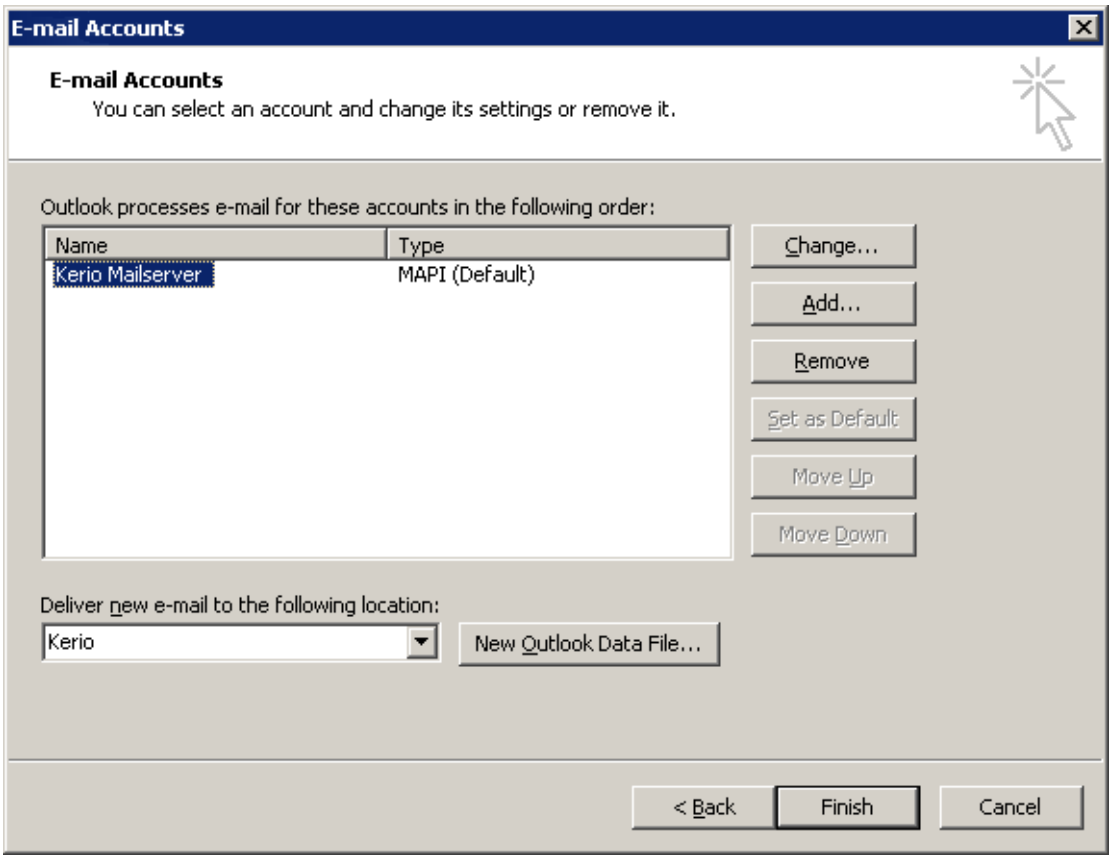

Figure 32.15 Data file settings

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).

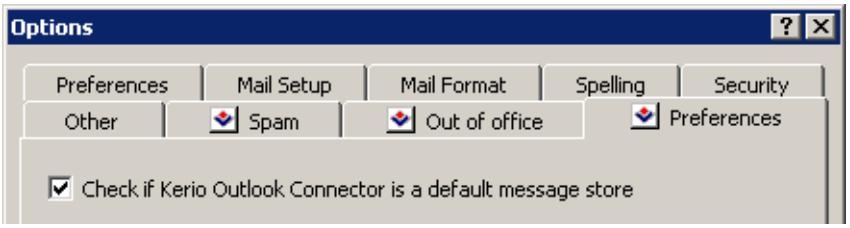

Figure 32.16 The store checking option

32.2.2 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 by using a special migration tool, the *Kerio MailServer Migration* application. 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 32.17 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.

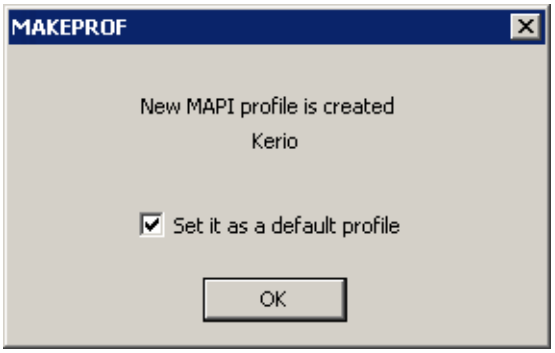

Figure 32.18 Successful profile creation information

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.

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*.

32.2.3 Upgrade of the Kerio Outlook Connector

Upgrades of *Kerio Outlook Connector* are performed automatically. If a new version of *Kerio Outlook Connector* is available, the module is updated immediately upon the startup of *MS Outlook*.

Warning: When the update is completed, *MS Outlook* is restarted automatically.

The update process and the restart takes up to two minutes.

The automatic update includes check of versions of *Kerio MailServer* and the *Kerio Outlook Connector*. If versions of the server and the client do not match, the user is informed that a different version of *Kerio MailServer* is installed on the server and that the client should be updated (see figure 15.23). Upon confirmation by the YES button, the version is upgraded/updated immediately (or downgraded).

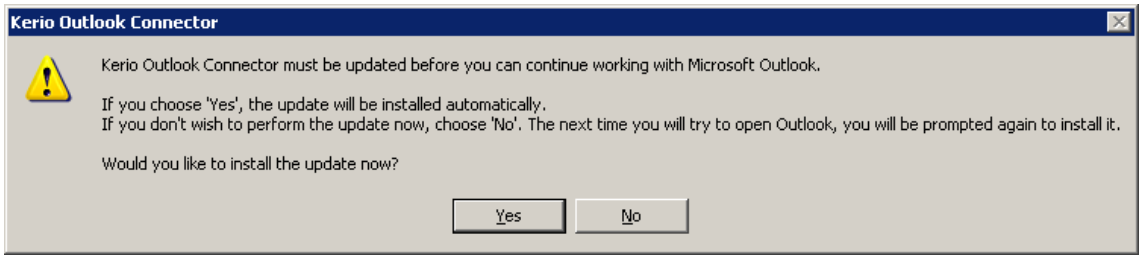

Figure 32.19 Version collision notification

Note: If the server and client differ only in their build numbers (numbers in the notification are the same), the client will work even if the update is rejected. If, however, version numbers are different (for example `6.4.0` versus `6.4.1`), *Kerio Outlook Connector* cannot be started unless updated.

Chapter 33

Kerio Synchronization Plug-in

Kerio Synchronization Plug-in is an extension to *MS Outlook* enabling basic groupware features (Calendars, Contacts and Notes) in private folders. The *Kerio Synchronization Plug-in* was designed for users that travel frequently and need to have access to email, calendar, and contacts locally. Besides that, the 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.

Note: It is also possible to work offline in *MS Outlook* by using the *Kerio Outlook Connector (Offline edition)* (for details, see section 32.1).

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.

Kerio Synchronization Plug-in also includes *Help* which can be triggered from the *MS Outlook's* toolbar. This help can also be found in *Start* → *Programs* → *Kerio* → *Synchronization Plug-in*.

Warning: Kerio MailServer supports synchronization by the SyncML protocol only for the client extension of *Kerio Synchronization Plug-in*.

Installation of the *Kerio Synchronization Plug-in* can be run under Windows 2000 Professional (version Service Pack 4), XP (version Service Pack 1 or Service Pack 2) and Windows Vista (Home, Business, Enterprise or Ultimate editions).

The Windows OS must include Internet Explorer 6.0 or higher.

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.
- *LDAP(S)* — useful where users want to search using the LDAP service (for details, see chapter 19).

Warning: In addition to the services listed above, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

Kerio Synchronization Plug-in can be installed on the following versions of *MS Outlook*:

- MS Outlook 2000 + version Service Pack 3
- MS Outlook XP + version Service Pack 3
- MS Outlook 2003 + version Service Pack 2 (at least version Service Pack 1 is required for installation)
- MS Outlook 2007 + 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 in *MS Outlook's* private folders. These items folders can be combined only with standard IMAP or POP3 accounts. It is not possible to use it for synchronization of MAPI accounts.

Kerio Synchronization Plug-in options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*, available for download at *Kerio Technologies* website (`http://www.kerio.com/kms-manual`).

If any problem regarding synchronization occurs, go to the *Debug* log and enable the *Sync ML Synchronization* option (for instructions how to do this, refer to chapter 22.8). The log including synchronization information can help you detect and solve possible problems.

Kerio Synchronization Plug-in is available in the following language versions:

- English
- Czech
- Chinese
- French
- Dutch
- Croatian
- Italian
- Japanese
- Hungarian
- German
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Language of the *Kerio Synchronization Plug-in* is set automatically in accordance with the language version set in *MS Outlook*. If a language set *MS Outlook* is not available in

the *Kerio Synchronization Plug-in*, English is used automatically.

33.1 Installation

Kerio Synchronization Plug-in is installed only once. Updates are performed automatically (see below).

Standard wizard is used for the installation. For successful installation, follow these instructions:

1. If *MS Outlook* is running, close it.
2. Install *Kerio Synchronization Plug-in*.
3. In *MS Outlook*, create a new profile (for detailed instructions, refer to chapter 32.2.1).
4. A particular POP3 or IMAP account is set withing creation of the profile.
5. Start *MS Outlook* and follow instructions provided in the *Kerio Synchronization Plug-in* user guide to set synchronization.

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 manually.

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 15.6).

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

```
Kerio\MailServer\webmail\download
```

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.

Note: Kerio Synchronization Plug-in is updated immediately upon startup of *MS Outlook* (before the profile selection). Therefore, *Kerio Synchronization Plug-in* is updated even if you want to work in a profile which is not used by *Kerio Synchronization Plug-in*.

Chapter 34

Support for iCalendar

The support for *iCalendar* in *Kerio MailServer* enables various applications which can handle the format (such as *MS Outlook 2007*, *Apple iCal*, *Mozilla Calendar*, *Lotus Notes* and *Ximian Evolution*) to publish and subscribe to calendars via *Kerio MailServer*.

By default, *Kerio MailServer* supports calendars in *MS Outlook 2007*, *Windows Calendar* on Windows Vista and *Apple iCal* on Apple Mac OS X.

34.1 Web calendars in MS Outlook 2007

MS Outlook 2007 allows sharing of calendars via the Internet. Calendars are available through subscription and publishing:

- *Calendar subscription* — calendar subscription downloads the particular calendar from a web server to a local store.
- *Calendar publishing* — calendar publishing is uploading of a calendar to a web store.

For manipulation with calendars, *MS Outlook 2007* uses iCalendar (iCal), a standard format for exchange of calendar data.

Kerio MailServer supports the iCal format and it is, therefore, possible to subscribe calendars stored on *Kerio MailServer* in *MS Outlook* as well as to publish calendars at *Kerio MailServer's* accounts. In addition to subscription to their own calendars, users can also subscribe to calendars shared by other users.

Warning: In *MS Outlook*, subscribed calendars are available only in the read-only mode. Published calendars are available on the server for reading only (this implies that it is not edit published calendars when accessed by *Kerio WebMail*, for example).

After authentication, the traffic is performed by the HTTP protocol. Therefore, the service must be running in *Kerio MailServer*. In addition to this, it is also necessary to map the corresponding port on the firewall protecting the server. Otherwise, the service will not be available from the Internet (for details, see section 2.3).

Subscription and publishing of calendars may be useful especially to view calendars of users who do not have an account in *Kerio MailServer* or to publish calendar in the Internet.

MS Outlook options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*. This file is available at the *Kerio Technologies* website at http://www.kerio.com/kms-manual.

34.2 Windows Calendar

Windows Calendar is a *Microsoft Corporation's* application used for calendar management on *Windows Vista*. This application enables to view events of multiple calendars in a single schedule and thus quickly identify conflicts in the time schedule. Calendars may be either stored on the disk or it is possible to subscribe for calendars stored at the web server. It is also possible to publish calendars on the web server.

Kerio MailServer supports publishing of calendars in user email accounts on the server and subscription of calendars stored in the mailbox from the *Windows Calendar*. In addition to subscription to their own calendars, users can also subscribe to calendars shared by other users.

Note: In *Windows Calendar*, subscribed calendars are available only in the read-only mode. Published calendars are available on the server for reading only (this implies that it is not edit published calendars when accessed by *Kerio WebMail*, for example).

Subscription traffic is performed by the HTTP or the HTTPS protocol. Publishing of calendars is performed via HTTPS only. This implies that it is necessary that the service is running in *Kerio MailServer* and a valid *Kerio MailServer's* SSL certificate must be installed on the *Windows Calendar* host. In addition to this, it is also necessary to map the corresponding port on the firewall protecting the server. Otherwise, the service will not be available from the Internet (for details, see section 2.3).

The *Windows Calendar* application supports *iCalendar* which is a standard format used for exchange of calendar data. The *iCalendar* built in *Kerio MailServer* enables *Kerio MailServer* to support cooperation with *Windows Calendar*.

Note: If calendars published as subfolders of the main calendar called *Calendar*, all events will also be displayed in the *Free/Busy* calendar.

Windows Calendar options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*. This file can be downloaded at the *Kerio Technologies* website at http://www.kerio.com/kms-manual.

34.3 Apple iCal

Developed by *Apple Computer*, *Apple iCal* is an application allowing management of calendars on *Mac OS X*. The application enables to manage events of multiple calendars in a single schedule and thus quickly identify conflicts in the time schedule.

Calendars may be either stored on the disk or, with read rights, it is possible to subscribe for calendars stored at the web server. It is also possible to publish calendars on the web server.

Kerio MailServer supports publishing of calendars in user email accounts on the server and subscription of calendars stored in the mailbox from the *Apple iCal*. In addition to subscription to their own calendars, users can also subscribe to calendars shared by other users.

Warning: In *Apple iCal*, subscribed calendars are available only in the read-only mode. Published calendars are available on the server for reading only (this implies that it is not edit published calendars when accessed by *Kerio WebMail*, for example).

Note: Since *Apple iCal* for Mac OS X Tiger, it is possible to synchronize locally stored calendars with calendars on *Kerio MailServer*. The *Kerio Sync Connector* (see chapter 40) is required for this purpose.

Subscription and publishing of calendars are performed by HTTP (in this case, it is not possible to use HTTPS). Therefore, the HTTP service must be running in *Kerio MailServer*. In addition to this, it is also necessary to map the corresponding port on the firewall protecting the server. Otherwise, the service will not be available from the Internet (for details, see section 2.3).

As suggested by the name, the *iCalendar* (also known as *iCal*) format is applied to calendar management. *iCal* is a standard format used for exchange of calendar data. The *iCalendar* built in *Kerio MailServer* enables *Kerio MailServer* to support cooperation with *Apple iCal*.

Note: If calendars published as subfolders of the main calendar called *Calendar*, all events will also be displayed in the *Free/Busy* calendar.

Apple iCal options and settings are addressed in the *Kerio MailServer, User's Guide* document. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

Chapter 35

CalDAV support

Since 6.5.0, *Kerio MailServer* supports CalDAV which is an extension for the WebDAV interface designed for exchange of calendar data. For details on this protocol, see http://www.caldav.org/. CalDAV standard is defined in RFC 4791.

CalDAV is an HTTP-based protocol. Therefore, the HTTP(S) service is required in *Kerio MailServer* for its support.

The protocol can be used for synchronization of calendars, scheduling of meetings with assistance of the Free/Busy server and delegating of calendars to other *Kerio MailServer* users.

35.1 Apple iCal

The client officially supported by CalDAV is *Apple iCal* which is a special application for calendar management on Mac OS X. *Apple iCal* supports CalDAV since Mac OS X 10.5 Leopard. Support of *Kerio MailServer* currently allows:

- synchronization of calendars,
- synchronization of To Do with the Task folder,
- scheduling of meetings,
- subscription of delegated calendars,
- providing Free/Busy information of *Kerio MailServer* users.

Warning: Starting of CalDAV synchronization in *Apple iCal* automatically disables calendar synchronization via *Kerio Sync Connector*. Synchronization of contacts, if defined, is not interrupted.

35.2 Settings

To enable the client connection to *Kerio MailServer*, it is necessary to set correct URL address for the connection.

Apple iCal

`http(s)://<servername>/caldav`

for example:

`http(s)://mail.company.com/caldav`

Other clients (such as Mozilla Sunbird)

`http(s)://<servername>/calendars/<domain>/<user>/<calendarname>`

for example:

`http(s://mail.company.com/calendars/company.com/jsmith/Calendar`

Chapter 36

Support for ActiveSync

Support for the *ActiveSync* protocol allows users to synchronize their email, calendars, contacts and tasks with mobile devices with *Microsoft Windows Mobile*, *Palm OS* and *Symbian* operating systems (for updated list of supported mobile devices, see section 36.2). The *ActiveSync* protocol is based on HTTP(S). For network connections, it uses WiFi, GPRS, UMTS and other technologies.

Kerio MailServer includes direct support for the protocol and therefore there is no need to install any supportive utility if the device also supports *ActiveSync*. If the device does not support the protocol, it is necessary to install an application which allows the synchronization on the device. Description of configuration of all particular devices is included both in the device's user's guide as well as in the *Kerio MailServer, User's Guide* manual (`http://www.kerio.com/kms-manual`). In chapter `Synchronization over ActiveSync`, simple and clear instructions on synchronization settings for all supported devices are provided.

And also, no settings in *Kerio MailServer* are required for the support. The only requirement is that the HTTP(S) service must be running on the default port (i.e. port 80 for HTTP and port 443 for the SSL-secured version). On most of supported mobile devices, ports cannot be changed to non-standard ports.

Warning: In addition to running of services on the server, it is also necessary to map corresponding ports for HTTP and HTTPS on the firewall protecting the server. Otherwise, the service will not be available from the Internet (for details, see section 2.3).

36.1 Synchronization methods

For synchronization of *Kerio MailServer* data with mobile devices, two methods can be applied:

1. Direct synchronization with the server.

2. Synchronization by using a desktop application installed on the workstation.

Note: The methods can usually also be combined.

Direct synchronization with Kerio MailServer

This synchronization method as well as its options and usage is addressed in chapter *Support for ActiveSync*.

This synchronization method does not require connection of the device to a desktop computer. The technology allows to connect over HTTP(S) *ActiveSync* protocol directly to the mailserver and synchronize mailbox folders with folders on the mobile device. On devices with an Internet connection, users can synchronize their data any time and, on newer devices, it is also possible to perform online synchronizations by using the *DirectPush* technology.

This synchronization method allows synchronization of the following folder types:

- mail folders,
- contacts (except Palm Treo 650),
- calendar,
- tasks — tasks synchronization is available only on devices with *Windows Mobile 5.0* and later.

Note: Appliance of the *ActiveSync* protocol in *Kerio MailServer* allows also synchronization of public and shared email folders (this rule applies only to devices with *Windows Mobile* operating systems).

The following parameters must be set for the direct synchronization with the server:

- The HTTP(S) service must be running in *Kerio MailServer*. For connections to the server from the Internet, it is necessary to enable an appropriate port (usually only for the HTTPS service) at the firewall behind which *Kerio MailServer* is running.
- It is necessary that network connection is set properly on the device.
- For connections via the HTTPS protocol (recommended for security reasons), it is necessary to have installed a trustworthy certificate (see chapter 36.4).
- The configuration of the device must allow connection to *Kerio MailServer*. The configuration requirements depend on device:

  Windows Mobile

  In Windows Mobile systems, it is necessary to set the *ActiveSync* application so that it can connect to the server. The configuration may vary in different versions of Windows Mobile. On the device, open the *ActiveSync* application, find the *Add Server Source* item in the *Menu* (Windows Mobile 2005) or open the *Server* tab from the *Tools* menu (Windows Mobile 2003) and enter the *Kerio MailServer's* Internet name, user name and password for connection to the mailbox. These settings are described in detail in *Kerio MailServer, User's Guide* (`http://www.kerio.com/kms-manual`). The linked page also includes simple instructions for configuration of the *ActiveSync* application (for all supported versions of Windows Mobile).

Palm Treo 650, 680 and 700p

On *Palm Treo 650*, synchronization with mailserver via *ActiveSync* is set in the *Versa Mail* mail client. In the account's configuration, it is necessary to set the *Mail Service* option to *Exchange ActiveSync* and enter *Kerio MailServer's* Internet name as well as login name and password for connection to the mailbox.

These settings are described in detail in *Kerio MailServer, User's Guide* (http://www.kerio.com/kms-manual).

Nokia E-series

Nokia Eseries mobile devices support the *ActiveSync* protocol if the *Email For Exchange* application (developed by *Nokia*) is installed on the device. Installation and settings are described in detail in *Kerio MailServer, User's Guide* (http://www.kerio.com/kms-manual).

Mobile devices with RoadSync

The *DataViz's* RoadSync application allows synchronization of email, calendars and contacts over the *ActiveSync* protocol. The application and the mobile device's settings are focused at http://www.dataviz.com/.

Synchronization by the ActiveSync desktop application

This synchronization method is performed out of *Kerio MailServer* and its description can be found in *ActiveSync* user's guides and in device manuals.

Warning: Settings described here apply only to *Windows Mobile*.

For successful data synchronization by using the *ActiveSync* desktop application, the following conditions must be met:

- The mobile device must include any version of the *ActiveSync* application (all supported versions of *Windows Mobile* operating systems include the application).
- *MS Outlook* is required on the user's desktop computer. It is necessary that an account connected to *Kerio MailServer* is created in *MS Outlook* (it is recommended to use a Kerio account extended with *Kerio Outlook Connector* since this allows also synchronization of *Notes* folders).
- The *ActiveSync* desktop application installed on the user's desktop computer is required.

Synchronization with the server via desktop applications is performed in a way that *MS Outlook* can access the data on the server (thanks to the connected and authenticated email account). MS Outlook is synchronized along with the *ActiveSync* desktop application while the desktop application can be synchronized with the device upon a connection. The process also works the other way round. After a successful connection, new data is synchronized via the *ActiveSync* desktop application with *MS Outlook*. This client applies the data in *Kerio MailServer* folders.

One of the advantages of synchronization via *MS Outlook* and the desktop application is the possibility to synchronize all folder types stored at the server (including tasks and notes in any device versions).

36.2 Supported versions of ActiveSync and mobile devices

Kerio MailServer supports the following versions of the *ActiveSync* protocol:

- ActiveSync 1.0 (Windows Mobile 2002, Palm OS — Palm Treo 650)
- ActiveSync 2.0 (Window Mobile 2003, Palm OS — Palm Treo 680, 700p)
- ActiveSync 2.1 (Windows Mobile 2003 SE)
- ActiveSync 2.5 (Windows Mobile 5.0, Windows Mobile 5.0 AKU2)

Note: In this case, the number of the *ActiveSync* version refers to the protocol version, not to the desktop application.

Kerio MailServer supports several mobile devices. Table 36.1 provides a list of supported devices running on *Windows Mobile*.

Version	Running on	Release date:
Windows Mobile 2002 (Pocket PC 3.0)	Windows CE 3.0	January 2002
Windows Mobile 2003 (Pocket PC 4.2)	Windows CE 4.20	June 2003
Windows Mobile 2003 Second Edition (SE)	Windows CE 4.21	March 2004
Windows Mobile 5.0	Windows CE 5.0	May 2005
Windows Mobile 5.0 AKU2	Windows CE 5.1	February 2006
Windows Mobile 6.0	Windows CE 5.2	February 2007

Table 36.1 List of supported devices running on MS Windows Mobile

Note: Kerio MailServer supports both *Windows Mobile.* for Pocket PC and the edition for Smartphone devices (mobile devices without touchscreens).

Overview of supported devices is provided in table 36.2.

Detailed information on individual features of the device and its configuration are provided in guides to particular devices. Configuration of *ActiveSync* in the device which allows connection of the device to *Kerio MailServer* and successful data synchronization is addressed in chapter `Synchronization over ActiveSync` in *Kerio MailServer, User's Guide* (`http://www.kerio.com/kms-manual`).

Different system versions allow different cooperation options. Older versions of *Windows Mobile* do not support all *Kerio MailServer* features. Features available on individual supported operating systems and their versions are shown in table 36.3.

The following features are not supported by *Kerio MailServer*:

Device type	Operating system
Palm Treo 650, 680 and 700p	Palm OS
Palm Treo 700w and 750v	Windows Mobile 5.0 AKU2
Nokia Eseries[a]	Symbian OS 9.1
Nokia N73 and N95[b]	Symbian S60 3rd edition
Sony Ericsson M600, P990i[c]	Symbian UIQ

[a] Nokia Eseries devices are supported if the external application Mail for Exchange 1.3.0 or higher is installed.

[b] Both Nokia Nseries devices are supported if the external application Mail for Exchange 1.6.1 or higher is installed.

[c] Sony Ericsson M600 and P990i are supported if the external application Exchange ActiveSync 2.10 or higher is installed.

Table 36.2 List of the other supported devices

Device type	Email	Calendar	Contacts	Tasks	Direct Push	Global Address Lookup	Kerio Smart Wipe
WM 2002	YES	YES	YES				YES
WM 2003 and WM 2003 SE	YES	YES	YES				YES
WM 5.0	YES	YES	YES	YES			YES
WM 5.0 AKU2	YES	YES	YES	YES	YES	YES	YES
WM 6.0	YES	YES	YES	YES	YES	YES	YES
Palm Treo 700w and 750v	YES	YES	YES	YES	YES	YES	YES
Palm Treo 650	YES	YES			YES[a]	YES[a]	YES
Palm Treo 680 and 700p	YES	YES	YES		YES[b]	YES[b]	YES
Nokia Eseries[c]	YES	YES	YES		YES	YES	YES
Nokia N73 and N95[d]	YES	YES	YES		YES	YES	YES
Sony Ericsson M600 and P990i[e]	YES	YES	YES		YES	YES	YES

[a] Requires upgrade for VersaMail 3.5 and installation of the Exchange ActiveSync Update for Treo 650 smartphone. For details, see http://software.palm.com/.

[b] Requires installation of EAS SP 2 update (http://www.palm.com/us/support/downloads/treo/easupdate.html).

[c] Nokia Eseries devices are supported if the external application Mail for Exchange 1.3.0 or higher is installed.

[d] Both Nokia Nseries devices are supported if the external application Mail for Exchange 1.6.1 or higher is installed.

[e] Sony Ericsson M600 and P990i are supported if the external application Exchange ActiveSync 2.10 or higher is installed.

Table 36.3 Supported features

- Setting of security policy from the server (Enforce Security Policy)
- SMS-based Always Up-To-Date (AUTD)

36.3 RoadSync

Kerio MailServer supports the *RoadSync 2.0* application developed by *DataViz*. *RoadSync* enables synchronization between *Kerio MailServer* and mobile devices. The synchronization is performed by the *ActiveSync* protocol.

RoadSync supports synchronization of the following folder types:

- Email,
- Calendar,
- Contacts,

The *RoadSync* application can be installed on the following mobile devices:

- Symbian UIQ,
- Symbian S80,
- Symbian S60 3rd Edition,
- Palm OS (synchronization is available for email only),
- Java MIDP 2.0 (synchronization is available for email only),

For details on *RoadSync* and supported devices, see the *DataViz* website at `http://www.dataviz.com/`.

36.4 SSL encryption

For the traffic, ActiveSync uses the HTTP or the HTTPS protocol.

Warning: For security reasons, it is recommended to synchronize only by the HTTPS protocol, since *ActiveSync* uses only unencrypted user login data for authentication at the server.

For description on encryption of services running in *Kerio MailServer*, see chapter 10. This method requires a valid SSL certificate installed on the device.

The following conditions must be met to make certificates valid:

- The certificate must be issued by a trustworthy certification authority. Trustworthy means that the mobile device needs to know the server's root certificate. *Windows Mobile* includes root certificates of several certification authorities. List of these authorities can be found at the Microsoft Corporation website.
- Date of the certificate must be valid and correct date and time must be set in the device.
- The certificate must include a valid name of the email domain for which *Kerio MailServer* is used.

Valid certificates for encrypted traffic can be either certificates issued by trustworthy certification authorities (these certificates can be quite expensive, however, they avoid possible installation difficulties) or a certificate issued by an internal certification authority or a so-called self-signed certificate generated in *Kerio MailServer* (for details, see chapter 10).

In case of certificates issued by a trusted certification authority, no settings or installations are required. In cases of internal certificates or self-signed certificates, the root certificate must be installed on the device.

Windows Mobile requires certificate encoded in the DER X.509 format. The `.cer` extension is required. The simpliest method to get and install a certificate is to download it to the device by a browser.

Kerio MailServer's self-signed certificate in the required format is available at `http://server_name/server.cer`

On devices with *Windows Mobile 2002*, traffic can be performed only by HTTPS. The unencrypted version of the protocol is not supported. It is also necessary that *Kerio MailServer* authenticates with a certificate authorized by a trustworthy certification authority. This can be either a certificate authorized by a supported commercial certification authority (certificates issued by VeriSign, CyberTrust, Thawte and Entrust are supported) or a root certificate of the authority which issued the certificate for *Kerio MailServer* can be installed on the device (for details, see section *Allowing installation of a root certificate in WM 2002*).

Warning: It is not possible to install the *Kerio MailServer's* self-signed certificate on *Windows Mobile 2002*. It is only possible to use root certificates authorized by at least one internal authority.

Since *Windows Mobile 2003*, *ActiveSync* configuration includes an option to enable/disable SSL encryption. However, it is strongly recommended to use the SSL encryption since only the basic authentication method is used for user authentication within the synchronization (no encryption is used for the login data transfers so the data can be easily misused).

Since *Windows Mobile 2003*, installation of the self-signed certificate on mobile devices is very simple. The instructions can be found in section *Installation of the Kerio MailServer's self-signed root certificate*.

Warning: Security rules in Smartphone devices with *Windows Mobile 2005* forbid installation of new root certificates. In such cases, it is necessary to enable installation of root certificates in the device registry first (the instructions are provided below).

Installation of the Kerio MailServer's self-signed certificate

The *Kerio MailServer's* self-signed certificate can be installed as described below:

1. To install the certificate on *Windows Mobile 2002* or on *Windows Mobile 5.0 Smartphone Edition*, follow the instructions provided in sections *Allowing installation of a root certificate in WM 2002* and *Allowing installation of a root certificate in WM 5.0 Smartphone Edition*. In other cases, start the installation by step 2.

2. On the mobile device, run a web browser.

3. In the URl textfield, enter the server's address following the pattern

   `http://server_name/server.cer`

   (e.g. `http://mail.company.com/server.cer`)

   or

   `https://server_name/server.cer`

(e.g. `https://mail.company.com/server.cer`)

4. A dialog is displayed asking whether the certificate should be downloaded to the device. Click *OK* to confirm the action.

5. Next, you'll be asked whether the certificate should be installed and used. Again, click on the *OK* button.

Now, the certificate is installed.

Allowing installation of a root certificate in WM 2002

To add a root certificate issued by a certification authority which is not supported by the device, follow these instructions:

1. Download the application from the `AddRootCert` link [409KB] and unpack it.

2. Copy the `addrootcert.exe` file to the device.

3. Copy the server's certificate to the device (the certificate must be encoded in DER X.509 format and the `.cer` extension is required).

4. In the device, click on the `addrootcert.exe` file and run it.

5. Use the application to install the certificate.

6. Restart the device.

Allowing installation of a root certificate in WM 5.0 Smartphone Edition

The security policy of Smartphone devices with *Windows Mobile 5.0* or *Windows Mobile 5.0 AKU2* forbids installation of root certificates issued by other than trusted certification authorities.

To allow installation of root certificates issued by authorities not supported by the particular device (an internal certificate or the *Kerio MailServer's* self-signed certificate), it is necessary to install a mobile device registry editor on the mobile device and use this editor to allow installation of untrustworthy root certificates. For this purpose you can use for example the `regeditSTG.zip` (24.01 KB) application which is available for free at `http://www.htceurope.com/`.

In this editor, follow these instructions:

1. Download the `regeditSTG.zip` application from the web page provided above and unpack it.

2. Move the editor to the mobile phone (e.g. by using the *MS ActiveSync* desktop application).

Warning: It is necessary that the file is saved in the phone, not on the memory card.

3. On the telephone, click on the file and run it.

4. Run `regeditSTG.exe` and find `HKLM\Security\Policies\Policies`.

5. Change the following registry items:
   - 00001001 overwrite the 2 with 1
   - 00001005 overwrite the 16 with 40
   - 00001017 overwrite the 128 with 144

6. Now, it is possible to download the certificate from the server and install it as described in section 36.4.

   Warning: So called "hard reset" removes the registry changes (it is necessary to repeat the settings if needed).

SSL encryption in Sony Ericsson devices

If the *Kerio MailServer's* self-signed certificate is installed, the device does not require confirmation for each synchronization with the server:

```
[Security Information       ?]
The certificate could not be
verified.
Select 'Certificate details' to get
more information about the
certificate.
Do you want to accept the
certificate and proceed?
[ Yes ]  [  No  ]  [ Details ]
```

Therefore, it is recommended to install a certificate signed by a trustworthy certification authority.

36.5 Remote deletion of the device data (Wipe)

The wipe feature allows the *Kerio MailServer* administrator to remove content of synchronized folders or even of the whole mobile device (so called hard reset) by a single click. This feature may be helpful when the device gets lost or stolen. This makes the data stored on the devices more secure. In addition to data clear-out, this action also disables further connections of the device to *Kerio MailServer* by disallowing connection of the device to the server by the original user login data.

Since the device types and operating systems are different, it depends on these conditions whether it is possible to reset the device completely or only to clear out synchronized folders. Remote hard restart is supported only by *Windows Mobile 5.0 AKU2*. Since older versions of *Windows Mobile* do not support this feature, only data synchronized by *ActiveSync* can be removed remotely.

Note: It is not possible to use this feature to perform remote memory cards wipes. However, memory cards usually store also email attachments. *ActiveSync* supports wipe-out of any synchronized data, including the attachments. This means that the wipe removes all data on the device as well as any attachments, including those which are stored on the memory card.

To perform remote wipe-out, go to the *Domain Settings* → *User Accounts* section of the administration console:

1. Select the user whose data will be removed from the device.
2. Right-click to open the pop-up menu and select *Status* → *Mobile Devices*.
3. This opens a dialog where mobile devices of the particular user can be administered (see figure 36.1).

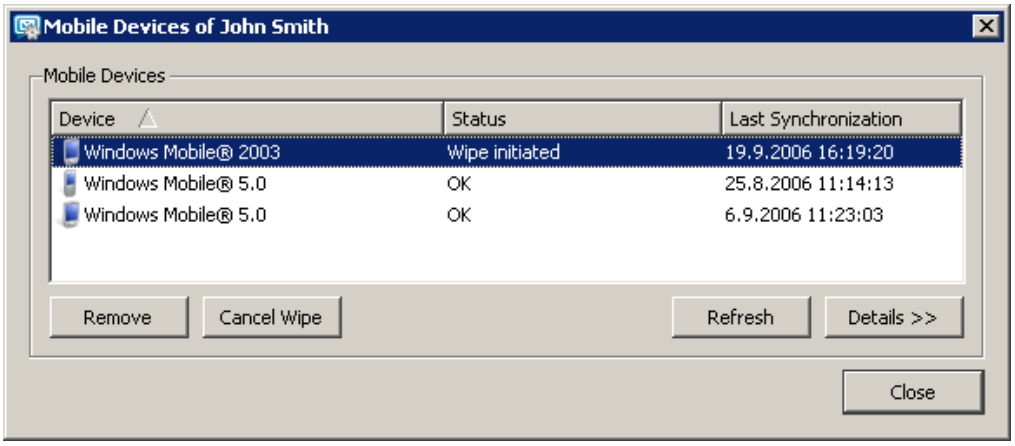

Figure 36.1 Administration of mobile devices

4. Select the device where the data should be wiped out and click on *Wipe*.

Warning: The wipe-out process will be completed upon the next connection of the device to *Kerio MailServer*. Users who have lost their devices should be informed that they should not run the synchronization if they find it and they should contact the administrators and ask them to cancel the wipe-out before the device is used again. The wipe action process can be cancelled by the *Cancel Wipe* button which appears when the *Wipe* button is used.

Details of the wipe process are recorded in the *Security* log (the *Security* log is addressed in section 22.4).

User confirmation of the wipe action

On Windows Mobile operating systems, user confirmation of the synchronizations security policy is required for wipe actions. In other words, it is necessary that the user agrees that the administrator performs the wipe action. Therefore, a dialog (see figure 36.2) appears which must be confirmed by the user during the first data synchronization between the device and *Kerio MailServer* (usually immediately when login data for *ActiveSync* is set in *Kerio MailServer*). if not confirmed, it is not possible to complete the synchronization process.

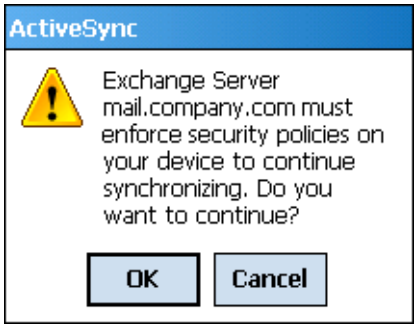

Figure 36.2 Wipe confirmation

This measure is applied for security reasons.

36.6 Removing a device from the administration of mobile devices

As the time goes on, users often buy new devices. Their older types are still connected to *Kerio MailServer*. Although these items do not cause any collisions or other problems, it is recommended to remove unused devices to keep the server well-organized.

Unused mobile devices can be removed as follows:

1. In *Domain Settings* → *User Accounts*, select a user whose devices are not used any longer.
2. Right-click on the account to open a pop-up context menu and select *Mobile Devices*.
3. This opens a dialog where mobile devices of the user can be administered (see figure 36.1).
4. Select the device where the data should be wiped out and click on *Remove*.

36.7 Synchronization logs

The entire synchronization process can be monitored and logged by using special tools. These tools can be found both in the *Kerio MailServer's* administration console and in the mobile device. This section provides description and settings instructions for these tools:

Synchronization logging in Kerio MailServer

Kerio Administration Console includes a special option in the *Debug* log (for details on the *Debug* log and its options, see section 22.8). The traffic log can be started as described below:

1. In the *Kerio MailServer's* administration console, go to the *Logs* → *Debug* section.
2. Right-click on the log window to open the pop-up menu.
3. Click on *Messages*.
4. In the *Logging Messages* dialog box, select *ActiveSync Synchronization*.

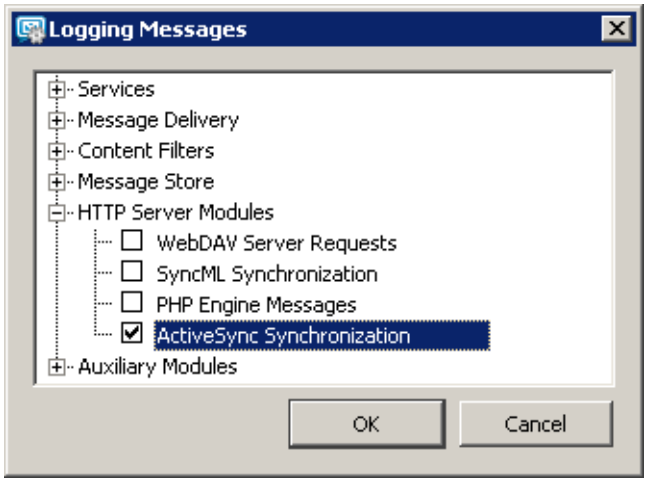

Figure 36.3 The Debug log settings

5. Click *OK* to confirm settings.

Once the log is set, run the synchronization of the device and the server to make the log.

If needed, synchronization log can also be saved, as follows:

1. Logs can be saved in a file in the *Logs* → *Debug* section.
2. Right-click on the created log and choose *Save log* from the pop-up menu.
3. In the *Save Log* dialog, select a path where the file will be saved, choose a file format (TXT or HTML) and confirm the dialog (see figure 36.4).

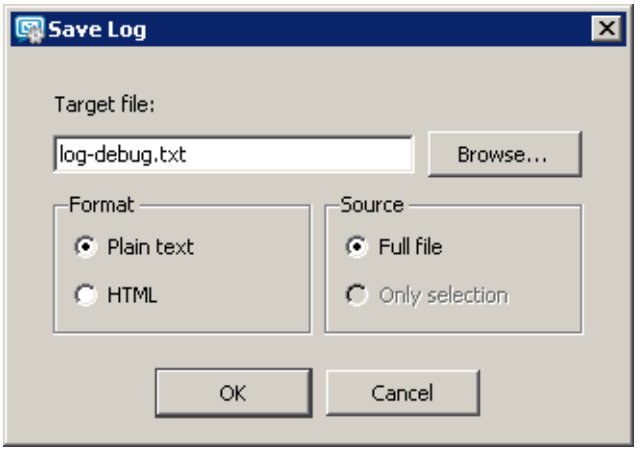

Figure 36.4 Saving a log

Logging synchronization on mobile devices

On *Windows Mobile*, the *ActiveSync* application includes special logs for each synchronization performed that can be helpful when solving traffic issues. Logs can be enabled/disabled in the *Advanced* section of the *ActiveSync* application.

Windows Mobile stores logs in `\Windows\Activesync`. Each synchronization process is saved in a stand-alone file whereas the three most recent logs are kept in the directory mentioned above. Names of the log files are:

`Exchange Server0.txt`

`Exchange Server1.txt`

`Exchange Server2.txt`

These logs may be helpful especially when solving issues in cooperation with the *Kerio Technologies* technical support.

36.8 Troubleshooting

Problems with synchronization of a single folder on Windows Mobile

Problem description

User's attempts to synchronize a subscribed folder fail.

Solution

In *ActiveSync* configuration, perform these settings:

1. In *ActiveSync* configuration, remove the folder from the list of synchronized folders.

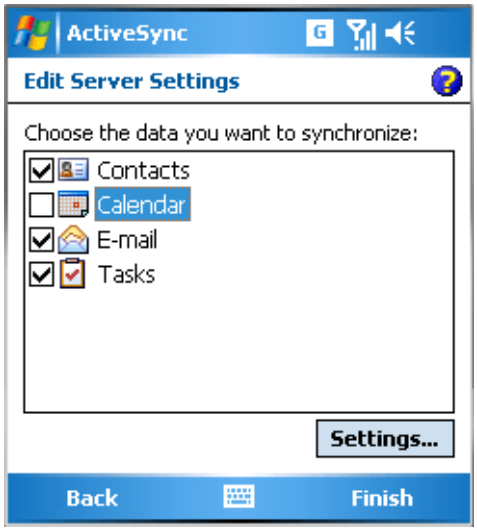

Figure 36.5 Removing a damaged folder from the list of synchronized folders

2. Use so called "soft reset" to reboot the device.
3. Synchronize the device with the server (without the damaged folder).
4. If the synchronization has been completed successfully, add the folder to the list and repeat the synchronization.
5. If even now the synchronization is not successful, please contact *Kerio Technologies* technical support.

Problems with synchronization of all folders on Windows Mobile

Problem description

User's synchronization of folders subscribed for synchronization fail.

Solution

In *ActiveSync* configuration, perform these settings:

1. In *ActiveSync* configuration, remove (uncheck) all folders from the list of synchronized folders (see figure 36.6) and save settings.
2. Use so called "soft reset" to reboot the device.
3. Add the removed folders to the list again and repeat the synchronization.
4. If even now the synchronization is not successful, please contact *Kerio Technologies* technical support.

Note: Besides this method, it is also possible to remove the entire account in *ActiveSync* and configure it again upon the next restart of the devices. Synchronized data will be removed from the device. When a new account is created this data is usually correct.

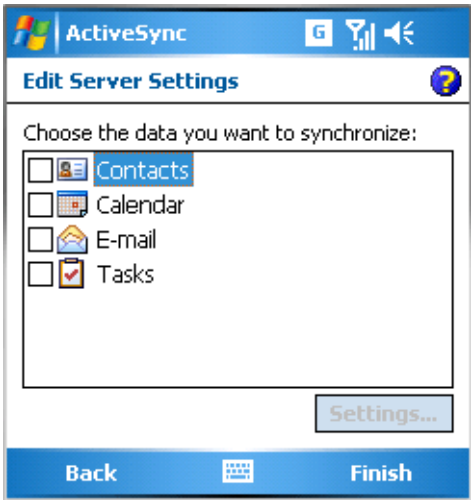

Figure 36.6 Removing all folders from the list of synchronized folders

Connection of the device to the server fails

Various solutions can be applied. Above all, it is necessary to check if the following conditions are met:

- It is necessary that Internet connection is set properly on the device so that the device can connect to *Kerio MailServer*.
- In *ActiveSync* configuration, check that the appropriate login data is used.
- in *Kerio MailServer*, the HTTP(S) service must be enabled on standard ports (most devices do not support setting of non-standard ports for traffic).
- If the device uses for communication an SSL-secured protocol, it is necessary to check whether a valid SSL certificate is used (see section 36.4).
- If the user connects to the server from the Internet, it is necessary to check that standard ports of the HTTP(S) protocol are enabled at the firewall.

Chapter 37

Support for BlackBerry via NotifyLink.

The *NotifyLink* service provided by *Notify Technology Corporation* enables cooperation of mobile devices and diverse servers. *Kerio MailServer* uses this service to synchronize data between *BlackBerry* devices and the *Kerio MailServer's* data store.

Traffic between the *NotifyLink* server and *Kerio MailServer* is performed via the WebDAV interface and the IMAP protocol. Therefore, services HTTP(S), IMAP(S) and the LDAP for contact search must be running in *Kerio MailServer*. No additional settings are needed in *Kerio MailServer*.

Warning: In addition to configuration of the services on the server, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

Synchronization of *BlackBerry* over *NotifyLink* allows to synchronize the following folders:

- Email — all personal folders and subfolders are synchronized.
- Calendar — only the main personal calendar is synchronized.
- Contacts — any folders selected in the configuration can be synchronized.
- Tasks — only the main task folder is included in the synchronization.

NotifyLink is a commercial service (paid) and it can be subscribed at `http://www.notifycorp.com/` where the configuration manual as well as other information can be also found.

Chapter 38

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 16.1).

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.

Warning: In addition to configuration of the services on the server, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

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 sp2 — 11.3.3 for Mac OS X
- *MS Entourage 2008*

MS Entourage must be installed on one of the following versions of Mac OS X:

- Mac OS X 10.3.9 Panther
- Mac OS X 10.4 Tiger
- Mac OS X 10.5 Leopard

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.

If any problem occurs regarding communication of *Kerio MailServer* and an Exchange account in *MS Entourage*, enable the *WebDAV Server Requests* option in the *Debug* log (to see where and how to enable the option, refer to chapter 22.8). The corresponding log may help when solving any related problems.

Options and settings at the client side are addressed in a special document, the *Kerio MailServer, User's Guide*. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

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 along with the 2008 version 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 38.1.

Character	MS Entourage X	MS Entourage 2004	MS Entourage 2008
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	YES	YES
Support for calendar and contact folders in a single account	NO	YES	YES
Support for Out-of-office	NO	NO	YES

Table 38.1 Supported features

Chapter 39

Apple Address Book Support

Kerio MailServer supports standard Mac OS X *Apple Address Book*. This support includes the option of searching for contacts in the *Kerio MailServer's* LDAP database and, since Mac OS X 10.3, also of bi-directional synchronization of contacts with *Kerio MailServer's* user accounts . Support for individual options on individual Mac OS X versions is shown in table 39.1.

Kerio MailServer supports *Apple Address Book* for the following versions:

- *Apple Address Book pro Mac OS X 10.2 Jaguar*
- *Apple Address Book pro Mac OS X 10.3 Panther*
- *Apple Address Book pro Mac OS X 10.4 Tiger*
- *Apple Address Book pro Mac OS X 10.5 Leopard*

OS version	Searching in the Kerio MailServer's LDAP database	Synchronization of contacts over Apple iSync	Synchronization over the Kerio Sync Connector
Mac OS X 10.2	YES	NO	NO
Mac OS X 10.3	YES	YES	NO
Mac OS X 10.4	YES	YES	YES
Mac OS X 10.5	YES	YES	YES

Table 39.1 Support for Apple Address Book on individual Mac OS X versions

To enable traffic between *Kerio MailServer* and *Apple Address Book*, the following services must be running in *Kerio MailServer* (enabled in the administration console):

- LDAP(S) — this service is required for searching in the *Kerio MailServer's* LDAP database.
- HTTP(S) — this service is required for synchronization of contacts.

Warning: In addition to configuration of the services on the server, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

Apple Address Book and *Kerio Sync Connector* settings are described in *Kerio MailServer, User's Guide*. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

Chapter 40

Kerio Sync Connector for Mac

Kerio Sync Connector is a special application which enables bi-directional data synchronization between *Kerio MailServer* and the *Apple iCal* or the *Apple Address Book* application:

- *Apple iCal — Kerio Sync Connector* allows bi-directional synchronization of locally stored events and To Do items.
- *Apple Address Book — Kerio Sync Connector* enables bi-directional synchronization of locally stored contacts.
  Note: Kerio Sync Connector does not support synchronization of distribution lists.

The main benefit of *Kerio Sync Connector* is that the synchronization for both applications can be set at a single point. Moreover, *Apple iCal* data is synchronized in both directions for the selected local calendar(s) which use the *Kerio MailServer's* data store.

For data synchronization, *Kerio Sync Connector* uses the WebDAV protocol. Therefore, HTTP and HTTPS services must be running in *Kerio MailServer*.

Warning: In addition to configuration of the services on the server, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

Kerio Sync Connector can be installed on workstations with operating systems Apple Mac OS X 10.4.9 and higher. The installation is performed with the `kerio-ksc-6.5.0-1069.mac.dmg` installation package which is available for free at *Kerio Technologies* website. Follow these installation instructions:

1. Double-click on the installation package to open it.
2. The *Finder* opens the installation package as a disk and offers the *Kerio MailServer Installer* executable installation file.
3. Standard wizard is used for the installation.

Kerio Sync Connector options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

If you use Mac OS X 10.5 Leopard, it is recommended to use rather synchronization via the built-in CalDAV account in *Apple iCal* (for details, see chapter 35) than via *Kerio Sync*

Connector. This implies that after installation of the *Kerio Sync Connector* it is necessary to disable synchronization of calendars and set CalDAV account in *Apple iCal*. These settings will not affect synchronization of contacts in *Apple Address Book*.

Synchronization troubleshooting

Kerio MailServer and *Kerio Sync Connector* provide special tools for possible synchronization troubleshooting, as follows:

Traffic logs

Traffic between *Kerio MailServer* and the *Kerio Sync Connector* can be logged both at *Kerio MailServer* or/and at the *Kerio Sync Connector*:

- *Kerio MailServer*
  1. Open *Kerio Administration Console* → *Logs* → *debug*.
  2. Right-click on the log pane to open a context menu, and select *Messages*.
  3. In the *Logging Messages* box just opened, enable the *WebDAV Server Requests* option (see figure 40.1).

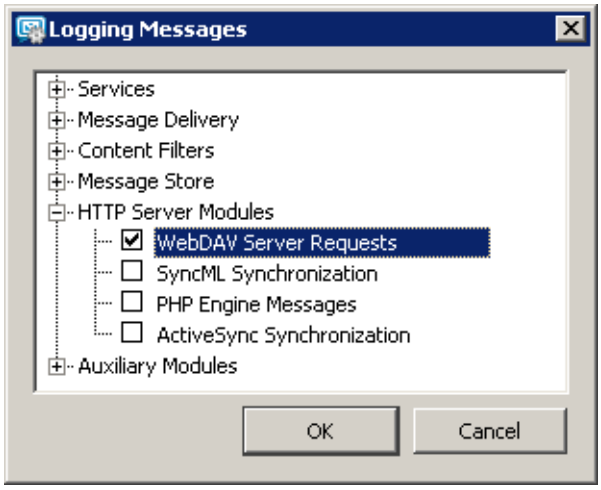

Figure 40.1 Debug log settings

  Once your problems are solved, it is recommended to disable the logging.
- *Kerio Sync Connector*
  1. Go to *System Preferences* → *Kerio Sync Connector* and switch to the *Advanced* tab.
  2. Check the *Enable debug logging* option (see figure 40.2).
     The log can be found in the *Console* application (*Applications* → *Utilities* → *Console*).

Figure 40.2 Log settings in Kerio Sync Connector

Synchronization fixing

The synchronization fix may help where problems with synchronized data occur. The fix will result in generation of a copy of data on the server or in the client. The copy replaces the opposite side's data so that both stores include identical data. The risk is that a part of the data having been saved since the last synchronization may be lost in the fix.

Follow these synchronization fix instructions:

1. Go to *System Preferences* → *Kerio Sync Connector* and switch to the *Advanced* tab.
2. Click on *Repair*.
3. In the dialog box just opened, select if the data on the server beat the data on the client during the synchronization, or vice versa. Click *OK* to initiate the synchronization.

Reporting problems to Kerio Technologies

If the synchronization problem is caused by an error in the application, it is recommended to send the synchronization log to *Kerio Technologies* for further analysis. Any information recorded in the log are used only to solve problems associated with usage of this product. No information including the sender's email address will be misused in any way.

To send the report, follow these instructions:

1. Go to *System Preferences* → *Kerio Sync Connector* and switch to the *Advanced* tab.
2. Click on *Send report*.
3. This opens an email composer window where the log message and the sender's address are attached. Simply send the message, it is not necessary to add any

information.

Chapter 41

Support for Apple Mail

Since version 6.1.2, *Kerio MailServer* supports some groupware features of IMAP and Entourage accounts in *Apple Mail 10.4* and higher. 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.

   If the file is being edited on *Mac OS X* or *Linux* operating systems, login to the system as the root user (a special user with full access rights to the system).

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.

Warning: In addition to configuration of the services on the server, it is also necessary to map corresponding ports on the firewall protecting the server. Otherwise, services will not be available from the Internet (for details, see section 2.3).

Apple Mail options and settings are addressed in a special document, the *Kerio MailServer, User's Guide*. This file can be downloaded at the *Kerio Technologies* website at `http://www.kerio.com/kms-manual`.

Chapter 42

Apple iPhone Support

Since version 6.4.1 *Kerio MailServer* supports *Apple iPhone 1.0*. *Kerio MailServer* supports lots of features:

- Email can be send and received via IMAP, POP3 and SMTP or synchronized with desktop applications (*Apple Mail* and *Outlook Express*) via *Apple iTunes*.
- Contacts and calendar can be synchronized with desktop applications via *Apple iTunes*. Calendar and contacts can be synchronized with applications *Apple iCal*, *Apple Address Book* and *Microsoft Outlook* (XP, 2003 and 2007).
- *Safari* supports both full version of *Kerio WebMail* and *Kerio WebMail Mini*.
  Warning: In full version of *Kerio WebMail*, it is not possible to edit existing contacts, events, tasks and notes.

To enable *Apple iPhone* support in *Kerio MailServer*, installation of iTunes 7.3 or higher on user stations is required. *iTunes* is used for synchronization of desktop clients with *Apple iPhone*.

Synchronization between desktop applications and *Apple iPhone* requires the following operating systems:

- Windows XP Service Pack 2 and later,
- Mac OS X 10.4.10 and later.

As implied, in *Kerio MailServer* it is necessary to run the following services:

- *HTTP(S)* — the service is required for connection to *Kerio WebMail*.
- *POP3(S)* — the service is required for POP3 accounts.
- *IMAP(S)* — the service is required for IMAP accounts.
- *SMTP(S)* — the protocol is used for email sending.

Besides the services listed above, it is necessary to map corresponding ports on the firewall protecting the server to make the services available from the Internet (for details, see section 2.3).

Warning: If traffic between *Kerio MailServer* and mail client is running on port 25, a problem might occur with email sending. Since public WiFi networks often do not support traffic on unencrypted protocols, SMTP on port 25 can be blocked. In such case users cannot send email out of the network. However, SMTPS on port 465 is usually allowed. For this reason, it is recommended to set users' email clients to SMTPS encryption.

42.1 Email

On *Apple iPhone*, email accounts can be set either manually or it is possible to use the automatic configuration:

Automatic configuration

If synchronization is performed via *iTunes*, it is possible to use also automatic synchronization of email folders in *Apple Mail* or in *Outlook Express* on *Windows* (settings of IMAP account).

Manual configuration

Manual configuration requires only standard settings of incoming and outgoing server. *Apple iPhone* offers three types of accounts: IMAP, POP3 and EXCHANGE. Any of them can be used for connection to *Kerio MailServer*.

Configuration details can be found in the chapter referring to *Apple iPhone* in the Kerio MailServer 6, User's Guide.

42.2 Synchronization of events and contacts

Direct synchronization of *Apple iPhone* with *Kerio MailServer* is not supported. Calendars and contacts can be synchronized only over the desktop application *Apple iTunes* version 7.3 and higher:

Calendar

Calendars can be synchronized with the following applications:

- *Apple iCal* — all calendars can be synchronized.
- *MS Outlook* — only the default calendar can be synchronized.
- *Windows Calendar* — *iTunes* do not support this synchronization.

Contacts

Contacts can be synchronized with the following applications:

- *Apple Address Book* — all items of contacts can be synchronized.
- *MS Outlook* — all significant items are synchronized; only one contact folder is synchronized; synchronization of distribution lists is not supported.
- *Windows Contacts* — all contact items are synchronized; distribution lists are synchronized as so called group.

Chapter 43

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/.

43.1 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.

Enterprise House

Vision Park

Histon

Cambridge CB4 9ZR

Tel.: +44 1223 202 130, Fax.: +44 1223 233 055

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.com/.

http://www.kerio.com/

Appendix A

Legal Presumption

Microsoft®, Windows®, Windows NT®, Internet Explorer®, Active Directory®, Outlook®, ActiveSync®, Entourage® and Windows Mobile® are registered trademarks of Microsoft Corporation.

Apple®, iCal®, Mac OS®, Safari™, Tiger™ and Panther® and Open Directory logo™ are registered trademarks or trademarks of Apple Computer, Inc.

Palm®, Treo™ and VersaMail® are trademarks or registered trademarks of Palm, Inc.

Red Hat® and Fedora™ and Fedora™ are registered trademarks or trademarks of Red Hat, Inc.

SUSE® is registered trademark of Novell Inc.

Mozilla® and Firefox® are registered trademarks of Mozilla Foundation.

Linux® is registered trademark of Linus Torvalds.

Kerberos™ is trademark of Massachusetts Institute of Technology (MIT).

McAfee® and Proven Security™ are registered trademarks or trademarks of Network Associates, Inc.

avast!® is registered trademark of ALWIL Software.

Symantec™ is trademark of Symantec Corporation.

eTrust™ is trademark of Computer Associates International, Inc.

ClamAV™ is trademark of Tomasz Kojm.

VisNetic® and VisNetic AntiVirus™ are registered trademarks or trademarks of Deerfield Communications Inc.

Cybertrust® is registered trademark of Cybertrust Holdings, Inc. and/or their filials.

Thawte® is registered trademark of VeriSign, Inc.

Entrust® is registered trademark of Entrust, Inc.

Sophos® is registered trademark of Sophos Plc.

ESET® and NOD32® are registered trademarks of ESET, LLC.

Grisoft® and AVG® are registered trademarks of Grisoft Inc.

NotifyLink® is registered trademark of Notify Technology Corporation.

BlackBerry® is registered trademark of Research In Motion Limited.

RoadSync™ is trademark of DataViz Inc.

Nokia® and Mail for Exchange® are registered trademarks of Nokia Corporation.

Symbian™ is trademark of Symbian Software Limited.

Sony Ericsson® is registered trademark of Sony Ericsson Mobile Communications AB.

SpamAssassin™ is trademark of Apache Software Foundation.

SpamHAUS® is registered trademark of The Spamhaus Project Ltd.

Appendix B

Used open-source libraries

This product contains the following open-source libraries:

Free Type 2

FreeType 2 is a software font engine that is designed to be small, efficient, highly customizable and portable while capable of producing high-quality output.

The FreeType Project is copyright ©1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg.

Heimdal Kerberos

Used by KMS on Linux via libtauth.

Heimdal is an implementation of Kerberos 5, largely written in Sweden. It is freely available under a three clause BSD style license (but note that the tar balls include parts of Eric Young's libdes, which has a different license). Other free implementations include the one from MIT, and Shishi. Also Microsoft Windows and Sun's Java come with implementations of Kerberos.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Copyright ©1995-1997 Eric Young (eay@@mincom.oz.au). All rights reserved.

Copyright ©1990 by the Massachusetts Institute of Technology

Copyright ©1988, 1990, 1993 The Regents of the University of California. All rights reserved.

Copyright ©1992 Simmule Turner and Rich Salz. All rights reserved.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

IBPP

Copyright ©2000-2006 T.I.P. Group S.A. and the IBPP Team

Permission is hereby granted, free of charge, to any person or organization ("You") obtaining a copy of this software and associated documentation files covered by this license (the "Software") to use the Software as part of another work; to modify it for that purpose; to publish or distribute it, modified or not, for that same purpose; to permit persons to whom the other work using the Software is furnished to do so; subject to the following conditions: the above copyright notice and this complete and unmodified permission notice shall be included in all copies or substantial portions of the Software; You will not misrepresent modified versions of the Software as being the original.

The Software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use of other dealings in the Software.
IBPP is an interface for the Firebird database written in C++.
Homepage: http://www.ibpp.org/

libiconv

Copyright ©1999-2003 Free Software Foundation, Inc.
Author: Bruno Haible
Homepage: http://www.gnu.org/software/libiconv/
The *libiconv* library is distributed and licensed as LGPL.
Kerio MailServer includes a customized version of this library. Complete source codes of the customized version of *libiconv* library are available at:

http://download.kerio.com/dwn/kms-iconv.zip

libIDL

LibIDL is a front-end for CORBA 2.2 IDL and Netscape's XPIDL.
Copyright ©1998, 1999 Andrew T. Veliath.

libjpeg

Libjpeg is a library for handling the JPEG (JFIF) image format.
Copyright ©1991-1998, Thomas G. Lane.
This software is the work of Tom Lane, Philip Gladstone, Jim Boucher, Lee Crocker, Julian Minguillon, Luis Ortiz, George Phillips, Davide Rossi, Guido Vollbeding, Ge' Weijers, and other members of the Independent JPEG Group.

libpng

Libpng is the official PNG reference library. It supports almost all PNG features.
Copyright ©2000-2002 Glenn Randers-Pehrson.

libspf

libspf2 implements the Sender Policy Framework, a part of the SPF/SRS protocol pair. libspf2 allows Sendmail, Postfix, Exim, Zmailer and MS Exchange check SPF records. It also verifies the SPF record and checks whether the sender server is authorized to send email from the domain used. This prevents email forgery, commonly used by spammers, scammers and email viruses/worms (for details, see http://www.libspf2.org/).
Copyright ©2005 by Shevekand Wayne Schlitt, all rights reserved.

libtiff

Libtiff is a library for handling the TIFF image format.
Copyright ©1988-1997 Sam Leffler
Copyright ©1991-1997 Silicon Graphics, Inc.

php_mbstring

Copyright ©2001-2004 The PHP Group.
Copyright © 1998,1999,2000,2001 HappySize, Inc. All rights reserved.
Homepage: http://www.php.net/downloads.php
The *php_mbstring.dll* library uses the *libmbfl* library which is distributed and licensed as LGPL.
Kerio MailServer includes a customized version of this library. Complete source codes of the customized version of *php_mbstring* library are available at:

http://download.kerio.com/dwn/kms-mbstring.zip

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 includes software developed by the *OpenSSL Project* for use in the *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/user_name`). Other subdirectories representing individual folders are created in this directory.

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).

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

M

N

O

P

R

S

T

U

W

X