Kerio Connect

Administrator's Guide

Kerio Technologies

Contents

Installing Kerio Connect

Product editions

Standard installation package

Kerio Connect is available as a standard installation package for:

- Windows
- Mac OS X
- Linux RPM
- Linux Debian

VMware Virtual Appliance

Virtual appliance for VMware products.
VMware Virtual Appliance is a software appliance edition pre-installed on a virtual host for VMware. The virtual appliance is distributed as OVF and VMX.
See Kerio Connect VMware Virtual Appliance for detailed information.

Windows

For system requirements go to the product pages.

1. Download the Kerio Connect installation file.
2. Run the installation.

   Kerio Connect must be installed under the user with administration rights to the system.
3. Follow the steps in the installation wizard.
4. Click **Finish** to complete the installation.

   
   The Kerio Connect installation process is logged in a special file (`kerio-connect.setup.log`) located in the folder `%TEMP%`.

   Kerio Connect engine starts (immediately or after restart) and runs as a service.
5. Perform the initial configuration of Kerio Connect.

Mac OS X

For system requirements go to the product pages.

1. Download the Kerio Connect installation file.
2. Run the installation.

   Kerio Connect must be installed under the user with administration rights to the system.
3. Follow the steps in the installation wizard. Kerio Connect is installed in the `/usr/local/kerio/mailserver` folder.
4. Click **Finish** to complete the installation.

   Kerio Connect engine starts upon the computer system startup and runs as a service.
5. Perform the initial configuration of Kerio Connect.

 Do not delete the Kerio Connect installation package. It includes Kerio Connect Uninstaller.

Kerio Connect engine

To run or restart the service, go to **System Preferences** → **Other** → **Kerio Connect Monitor**.

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

- **Stopping Kerio Connect engine:**

  ```
  sudo /usr/local/kerio/mailserver/KerioMailServer stop
  ```
- **Running Kerio Connect engine:**

  ```
  sudo /usr/local/kerio/mailserver/KerioMailServer start
  ```
- **Restarting Kerio Connect engine:**

  ```
  sudo /usr/local/kerio/mailserver/KerioMailServer restart
  ```

Linux — RPM

For system requirements go to the product pages.

1. Download the Kerio Connect installation file.
2. Run the installation.

Kerio Connect must be installed under the user with `root` rights.

For installations, Kerio Connect uses the RPM application. All functions are available except the option of changing the Kerio Connect location.

3. Follow the steps in the installation wizard. Kerio Connect is installed in the `/opt/kerio/mailserver` folder.
4. Click **Finish** to complete the installation.
5. Perform the initial configuration of Kerio Connect.

New installation

Start the installation using this command:

```
# rpm -i <installation_file_name>
```

Example: `# rpm -i kerio-connect-8.0.0-6333.linux.rpm`

If problems with package dependencies occur and you cannot install Kerio Connect, download and install the `compat-libstdc++` package.

We recommend you read the LINUX-README file carefully, immediately after installation (located in the installation directory in the folder `doc`).

Kerio Connect engine

The script that provides automatic startup of the daemon (the Kerio Connect engine) on reboot of the operating system is located in `/etc/init.d` folder.

Use this script to start or stop the daemon manually. Kerio Connect must be run under the user `root`.

- **Stopping Kerio Connect engine:**

  ```
  /etc/init.d/kerio-connect stop
  ```

- **Running Kerio Connect engine:**

  ```
  /etc/init.d/kerio-connect start
  ```

- **Restarting Kerio Connect engine:**

  ```
  /etc/init.d/kerio-connect restart
  ```

If your distribution has `systemd` available, use these commands:

- **Stopping Kerio Connect engine:**

  ```
  systemctl stop kerio-connect.service
  ```

- **Running Kerio Connect engine:**

```
systemctl start kerio-connect.service
```

Linux — DEB

For system requirements go to the product pages.

1. Download the Kerio Connect installation file.
2. Run the installation.

   Kerio Connect must be installed under the user with `root` rights.
3. Follow the steps in the installation wizard. Kerio Connect is installed in the `/opt/kerio/mailserver` folder.
4. Click **Finish** to complete the installation.
5. Perform the initial configuration of Kerio Connect.

New installation

Start the installation using this command:

`# dpkg -i <installation_file_name.deb>`

Example: `# dpkg -i kerio-connect-8.0.0-1270.linux.i386.deb`

If problems with package dependencies occur and you cannot install Kerio Connect, download and install the `compat-libstdc++` package.

We recommend you read the DEBIAN-README file carefully, immediately after installation (located in the installation directory in folder `doc`).

Kerio Connect engine

The script that provides automatic startup of the daemon (Kerio Connect engine) on reboot of the operating system is located in `/etc/init.d` folder.

Use this script to start or stop the daemon manually. Kerio Connect must be run under the user `root`.

- **Stopping Kerio Connect engine:**

  `sudo service kerio-connect stop`
- **Running Kerio Connect engine:**

  `sudo service kerio-connect start`
- **Restarting Kerio Connect engine:**

  `sudo service kerio-connect restart`

When installing on Debian with a graphical user interface, open the installation package with the `gdebi` installer: Right-click the file and click **Open with**.

Performing initial configuration in Kerio Connect

About initial configuration

Before you start using Kerio Connect, you must perform an initial configuration.

The initial configuration sets the basic parameters for Kerio Connect. These include:

- primary domain
- administrator's account
- data store

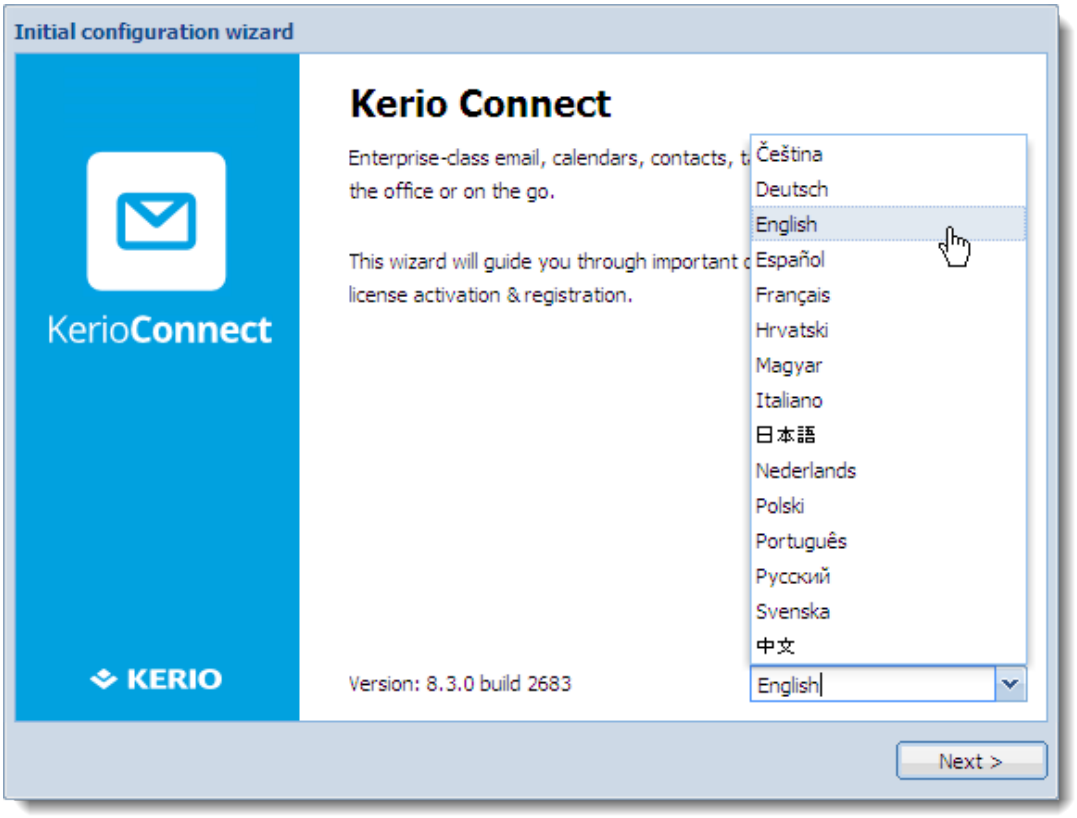
The wizard also creates special files where the server configuration is saved.

Configuring initial parameters

You can change all the settings from the initial configuration wizard later in the administration interface.

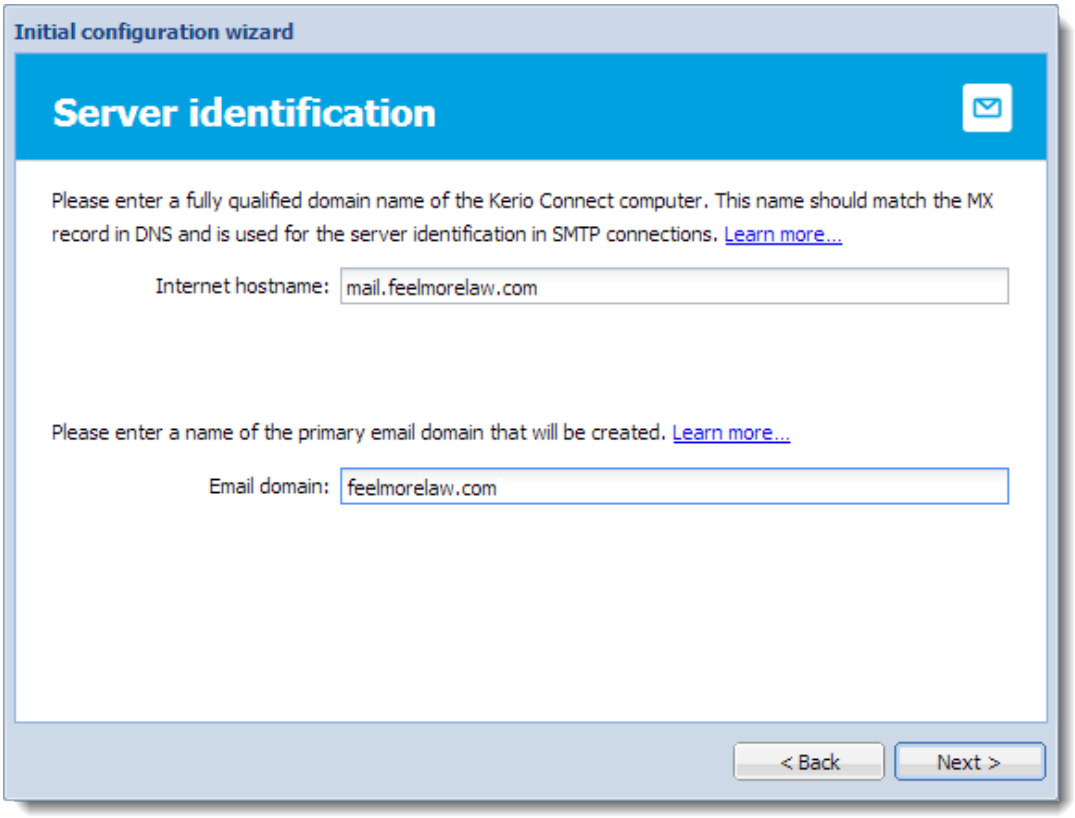
1. Install Kerio Connect.
2. Open the following address in your web browser:

   `https://kerio_connect_server:4040/admin`
3. Select a language for the initial configuration wizard and click **Next**.



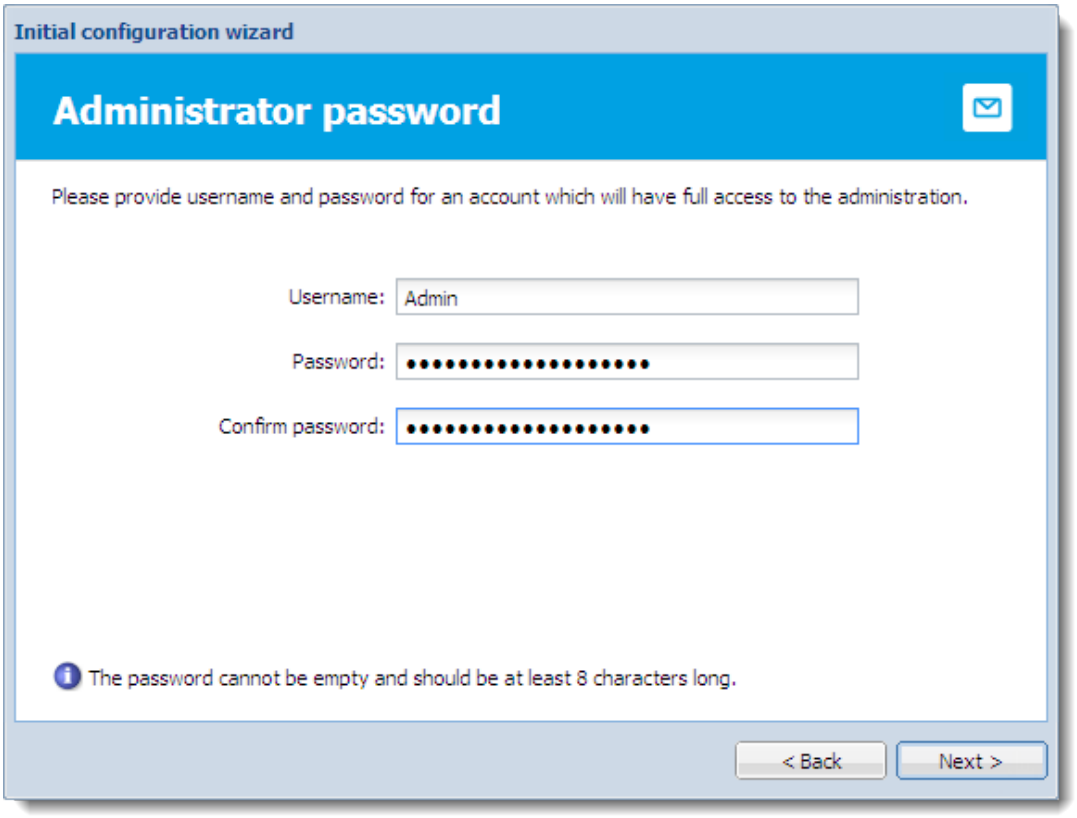
This language will be also set as a default language after the first logon to the administration interface.

4. Type the **Internet hostname** and **Email domain**. Click **Next**.



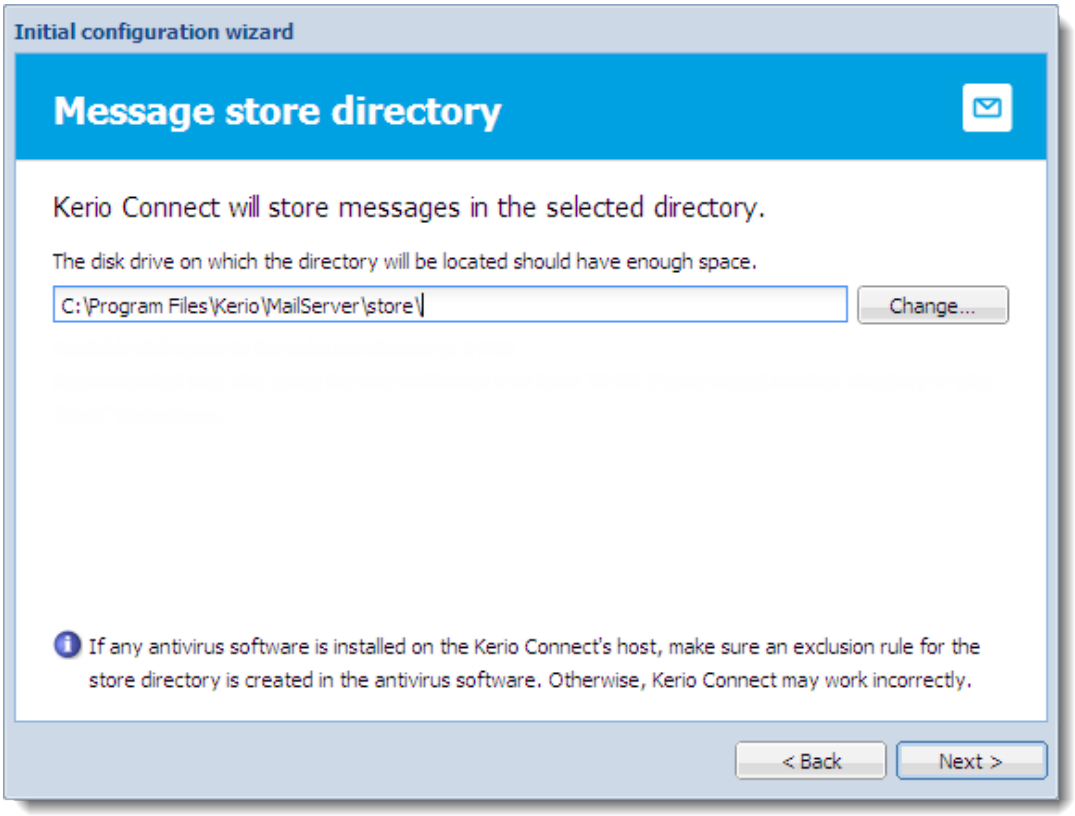
For more information about domains, read the Domains in Kerio Connect article.

5. Set a username and password for an administration account and click **Next**.



This first administration account consumes one license, you can switch to the built-in admin account in the administration interface.
For more information about administrator accounts, read the Setting access rights in Kerio Connect article.

6. Set a directory where the message store will be saved and click **Next**.

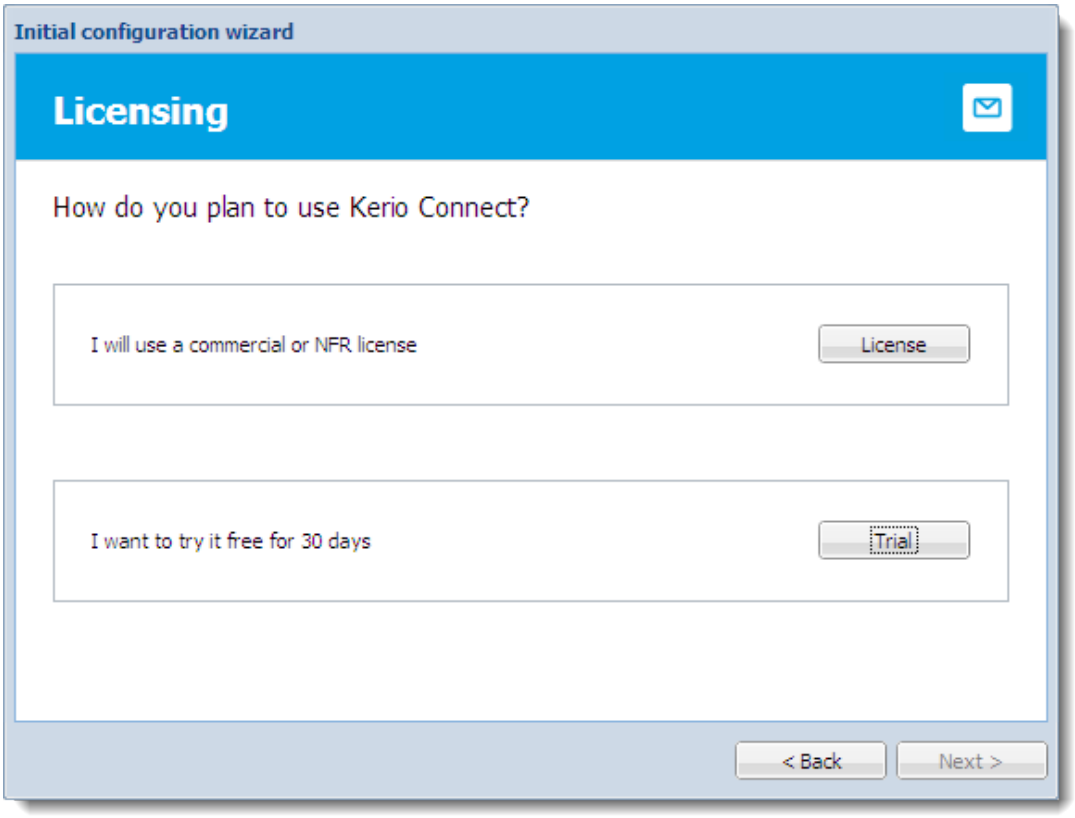


Kerio Connect checks if you have enough free disk space available.

For more information about the message store, read the Configuring data store in Kerio Connect article.

The folder must be on a local disk. If you're using a virtual machine, define the disk as local.

7. Register the product or continue without the registration.



8. Finish the wizard.

When you finish the wizard, log in to Kerio Connect administration using the administrator username and password from the wizard.

Configuration files

During the initial configuration, the following configuration files are created:

users.cfg
: `users.cfg` is an XML file with the UTF-8 coding which includes information about user accounts, groups and aliases.

mailserver.cfg
: `mailserver.cfg` is an XML file with the UTF-8 coding which contains any other parameters of Kerio Connect, such as configuration parameters of domains, back-ups, antispam filter, antivirus.

The default location of the configuration files is:

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

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

Registering Kerio Connect

Why register Kerio Connect?

If you don't register Kerio Connect, it behaves as a *trial version*. The limitations of the trial version are:

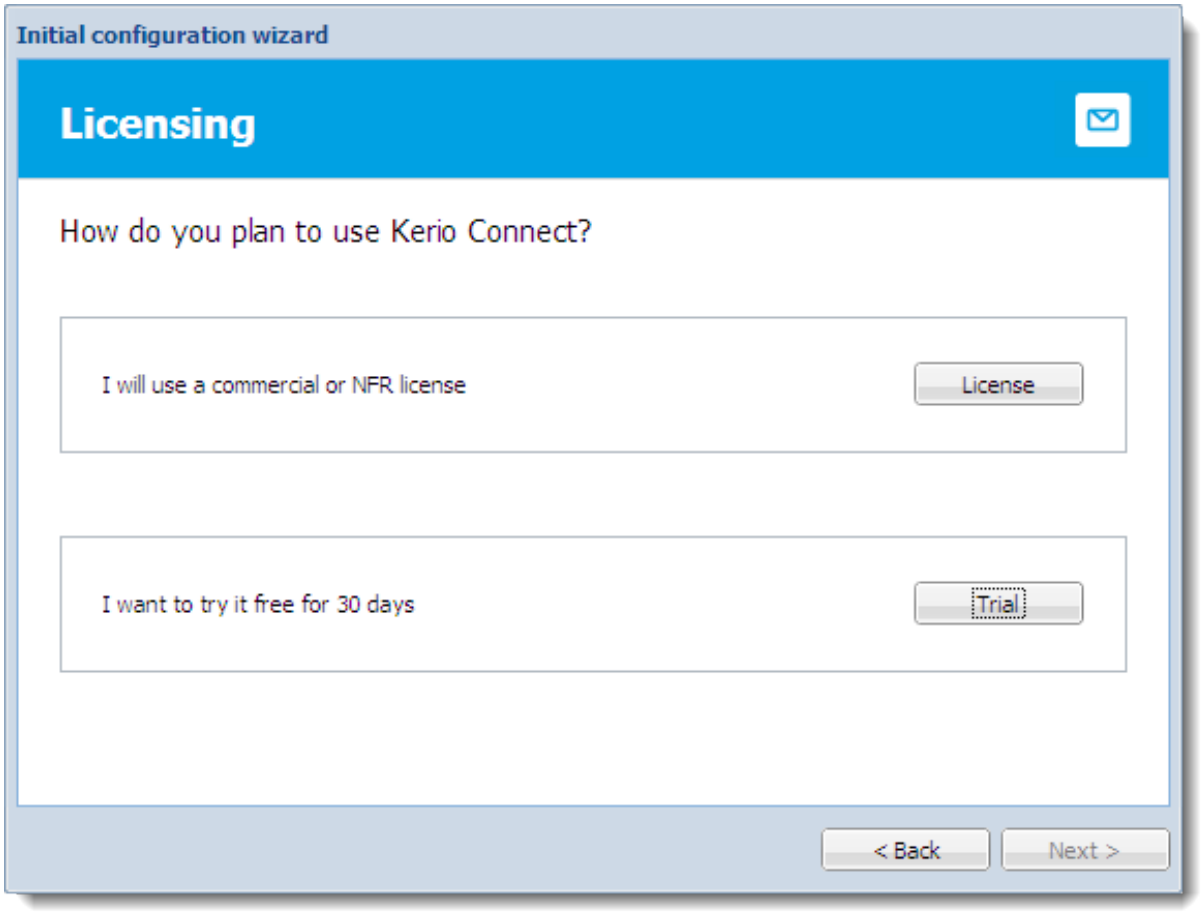
- Thirty days after installation, Kerio Connect Engine will be disabled.
- Sophos antivirus engine cannot be updated for unregistered trial versions.
- Synchronization of mobile devices via Exchange ActiveSync is disabled.
- Greylisting antispam protection is not available.
- Technical support is unavailable.

  If you register a trial version, you will receive technical support during the entire trial period.

You can register Kerio Connect when you run the initial configuration wizard or in the administration interface.

Registering Kerio Connect from the initial configuration wizard

You can register Kerio Connect when you run the initial configuration wizard.

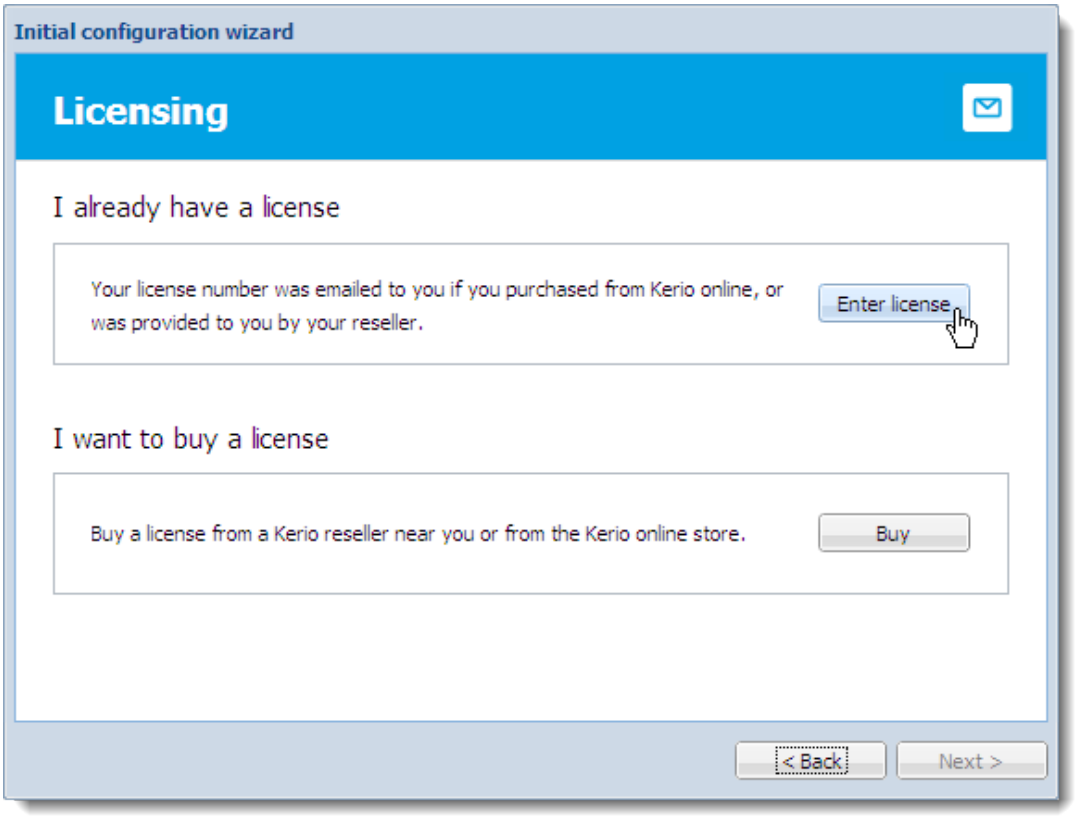


Registering a full version

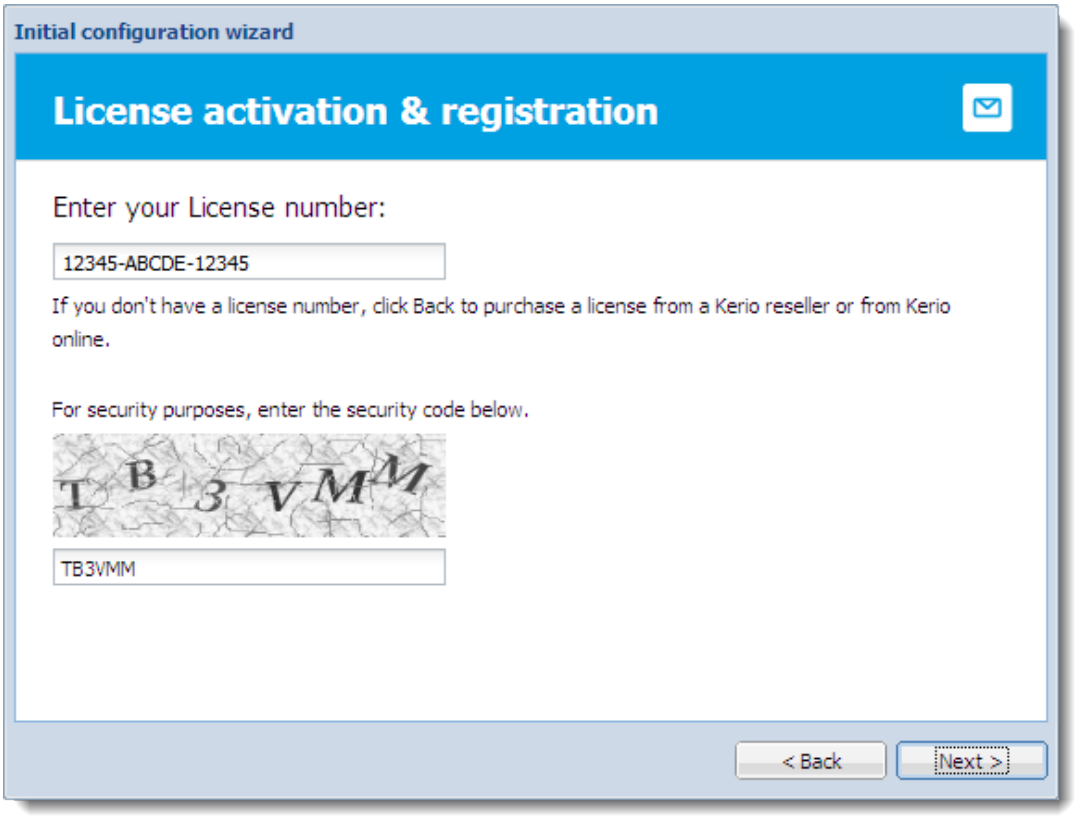
1. On the **Licensing** tab of the configuration wizard, click the **License** button.
2. Prepare to type your license number:

   If you have a license number, click **Enter license**.

   If you don't have a license number, click the **Buy** button.



3. Type your license number and security code, and click **Next.**



4. Decide if you want to grant Kerio Technologies permission to gather usage statistics, and click

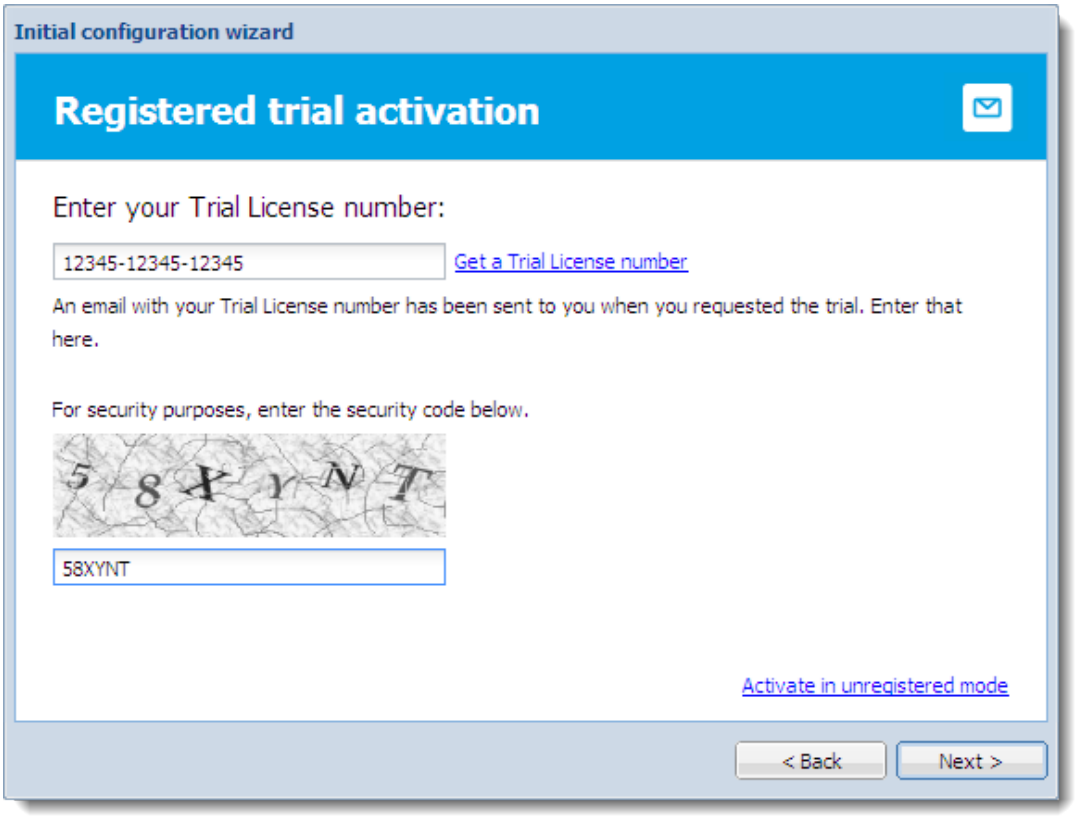
   Next.

5. Click **Finish** to close the wizard.

Registering a trial version

1. On the **Licensing** tab of the initial configuration wizard, click the **Trial** button.
2. Type your trial license number and security code, and click **Next.**

   If you don't have a trial license number, click **Get a Trial License number**.



3. Decide if you want to grant Kerio Technologies permission to gather usage statistics, and click

   Next.

4. Click **Finish** to close the wizard.

Using an unregistered trial version

If you want to use Kerio Connect in the unregistered mode, click the **Activate in unregistered mode** link in the **Registered trial activation** dialog box.

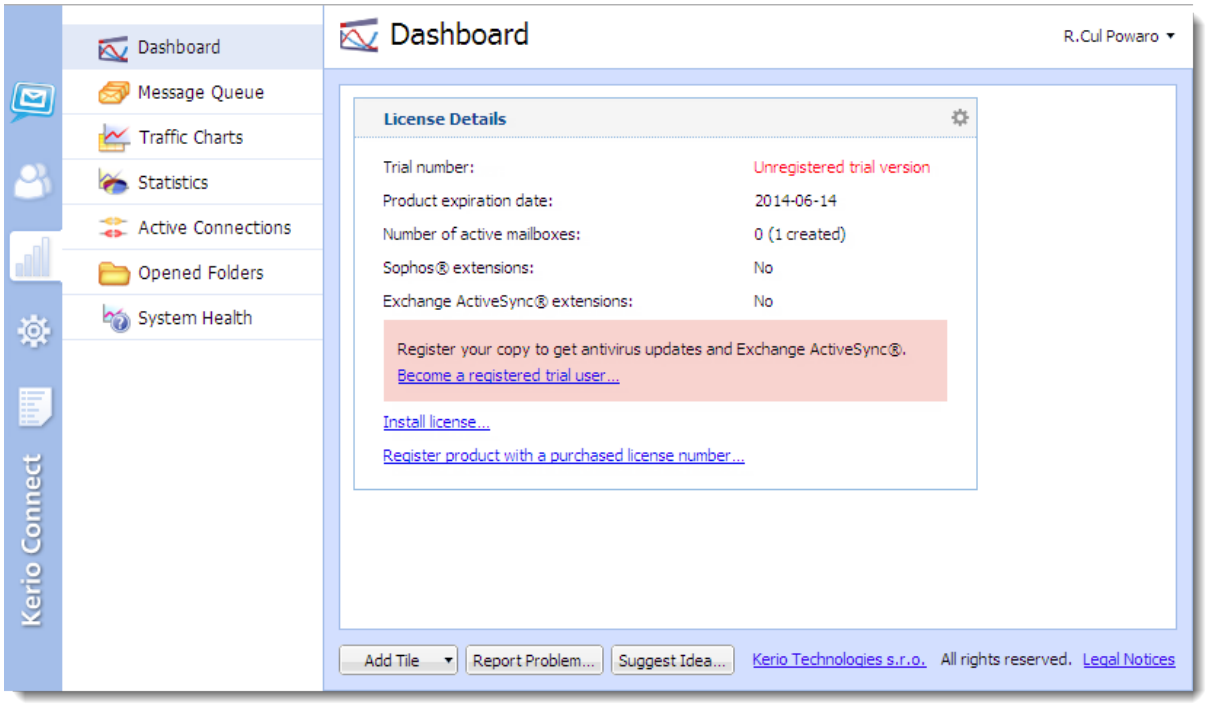
The limitations of the unregistered trial versions are described above, in the Why register? section.

Registering Kerio Connect in the administration interface

You can register Kerio Connect from the **Dashboard** of the administration interface.

During registration, Kerio Connect must contact the Kerio Technologies registration server. Allow outgoing HTTPS traffic for Kerio Connect on port 443 on your firewall.

Registering trial versions



1. Log in to the administration interface and on the **Dashboard** click **Become a registered trial user**.

2. Type your trial license number and security code and click **Next.**

   If you don't have a trial license number, click **Get a Trial License number**.

3. Confirm.

Registering a full version

If you registered a trial version and you have since purchased the full version of Kerio Connect, the license file is automatically imported to your product within 24 hours of your purchase. The trial ID becomes your license number.

If you haven't registered your trial version:

1. In the Kerio Connect **Dashboard**, click **Register product with a purchased license number**.

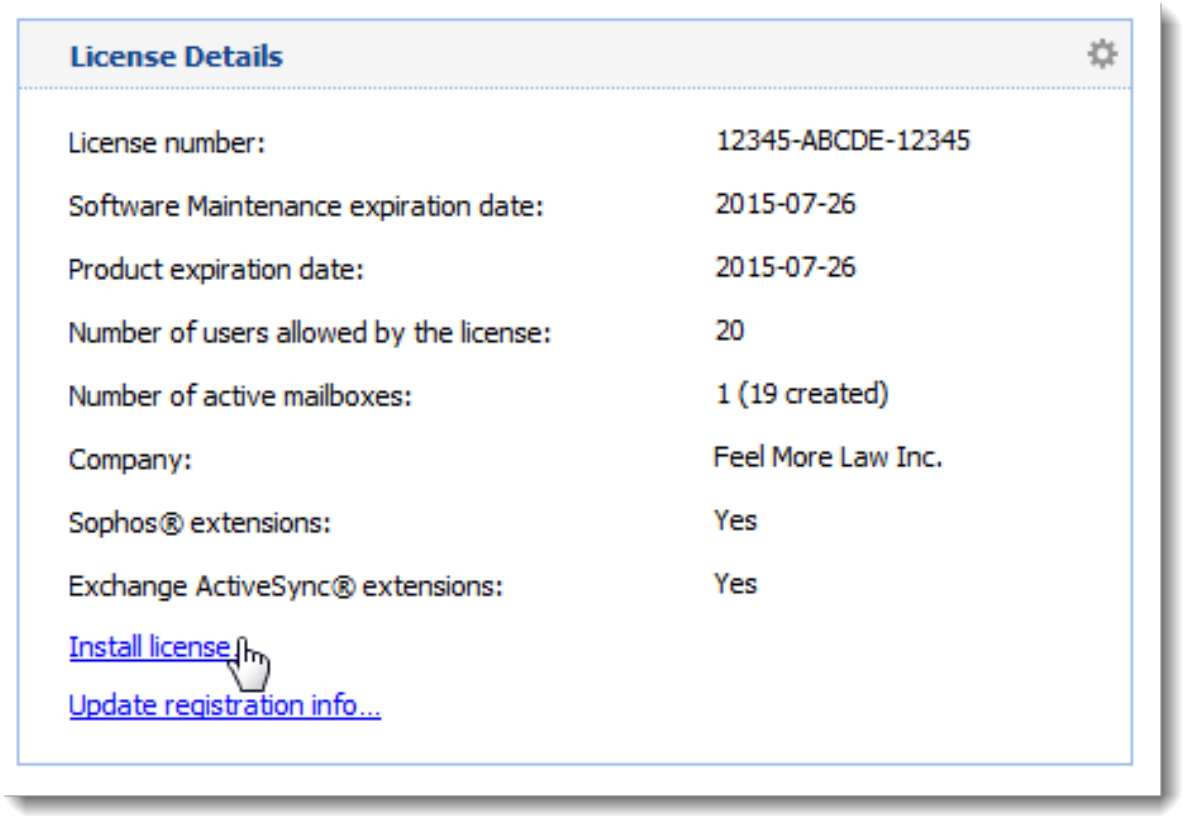
2. Type the information required, including the license number you acquired on purchase.

3. Kerio Connect contacts the registration server, checks the validity of the data you entered, and automatically downloads the license file (digital certificate).

4. Click **Finish** to close the installation wizard.

Installing your license manually

If you have acquired the license file (`*.key`), you can import it to Kerio Connect by clicking **Install license** on the **Dashboard** in the administration interface.



The default location of the license file varies by platform:

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

Licenses in Kerio Connect

Overview

Licenses are counted by number of users.

“Number of users” means the number of mailboxes or accounts that are:

- Created and enabled in Kerio Connect
- Mapped from a directory service

  All users created in this database count as individual licenses.
- Imported from a domain

The following don’t count as licenses:

- Disabled accounts
- Mailing lists
- Resources
- Aliases
- Domains
- Internal administrator account

If you want to increase the number of users allowed by your license, visit the Kerio Connect website.

Users mapped from a directory service

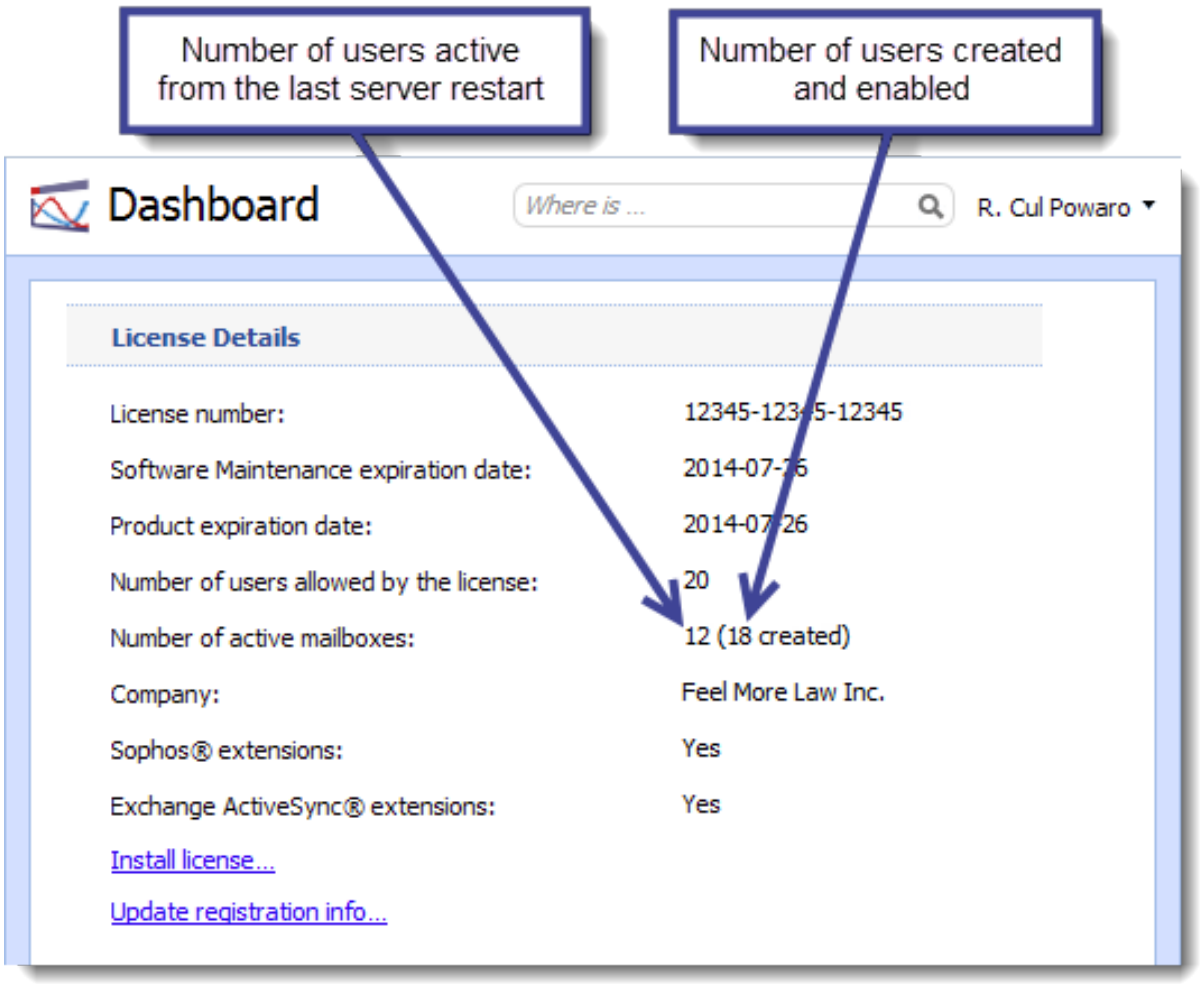
When you map users from a directory service, all users created in the directory service are imported to Kerio Connect. The total number of users in Kerio Connect may thus exceed the number allowed by your license.

Once the number of users who connect to Kerio Connect (i.e. create a mailbox) exceeds the number of users from your license, no other users are allowed to connect to their accounts.

Checking the number of users in your license

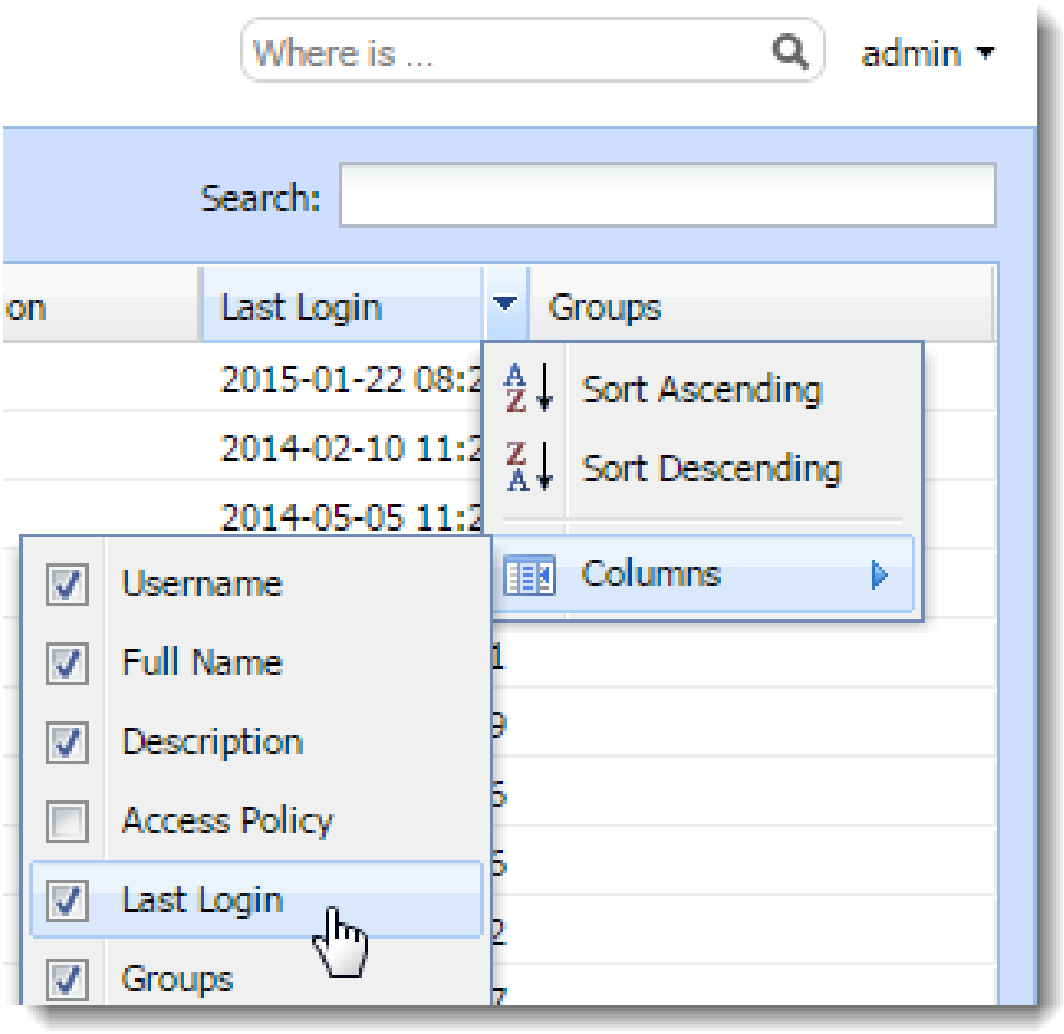
The Kerio Connect Administration interface displays the number of users you have and the number of licenses you purchased.

Go to **Status** → **Dashboard** and view the **License Details** tile.



To free up some user seats in your license, you can remove inactive users from your Kerio Connect:

1. Go to the **Users** section.
2. Click the arrow next to a column name and select **Columns** → **Last Login**.



3. Click the **Last Login** column header to sort users by their last login time.

Now you can remove users who do not use Kerio Connect.

Optional components

Kerio Connect has the following optional components:

- Sophos antivirus
- Exchange ActiveSync add-on

These components are licensed individually. Visit the product pages of Kerio Connect for additional information.

Installing Kerio Connect licenses

For information on registrations and license installations, read Registering Kerio Connect.

Gathering usage statistics

Gathering information

As a part of our commitment to offer the best quality product on the market, Kerio requests your permission to collect anonymous usage statistics addressing the server hardware, software clients and operating systems interacting with our products.

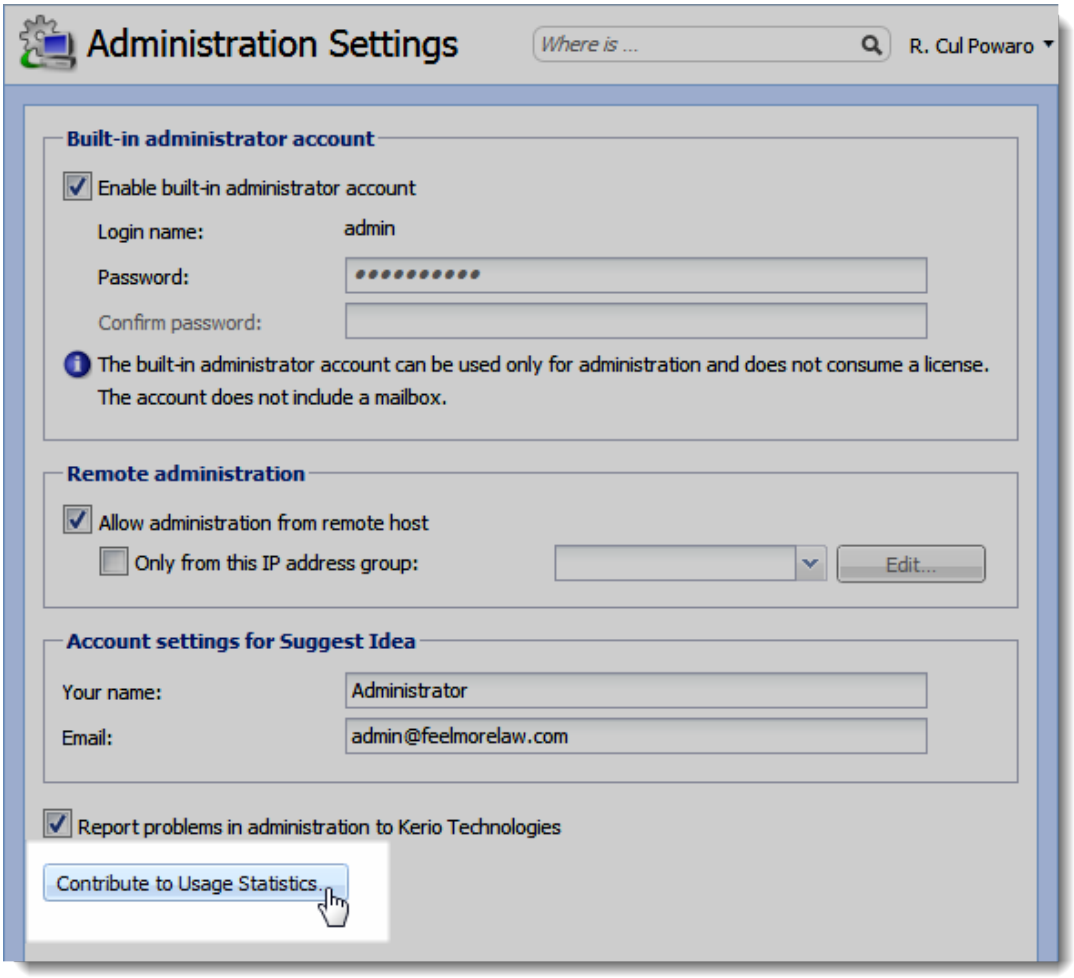
Sending this data does not affect the performance of your Kerio Connect.

Enabling data gathering

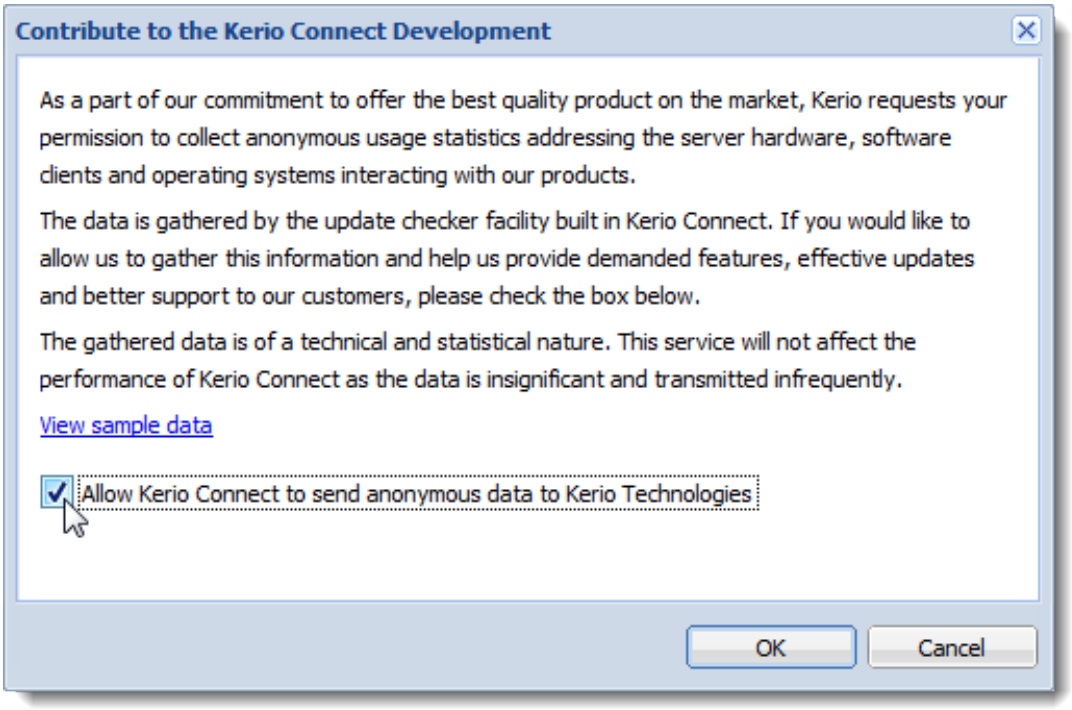
You can allow Kerio to receive anonymous usage statistics during the first activation of Kerio Connect.

To change the settings later, follow these steps:

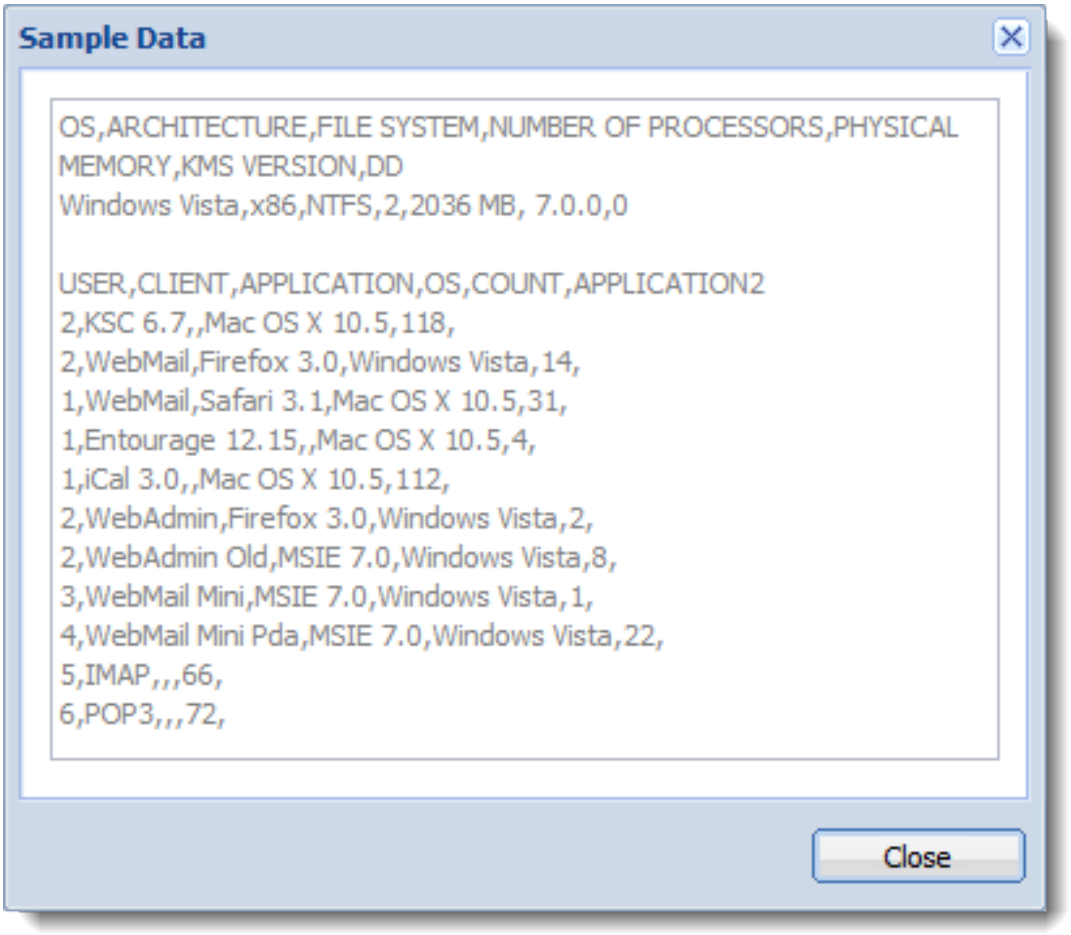
1. Login to the Kerio Connect administration.
2. Go to section **Configuration** → **Administration Settings**.
3. Click the **Contribute to Usage Statistics** button.



4. Check the **Allow Kerio Connect to send anonymous data to Kerio Technologies** option.



5. To view sample data Kerio Connect sends, click the **View sample data** link.


Sample Data
OS,ARCHITECTURE,FILE SYSTEM,NUMBER OF PROCESSORS,PHYSICAL MEMORY,KMS VERSION,DD
Windows Vista,x86,NTFS,2,2036 MB, 7.0.0,0
USER,CLIENT,APPLICATION,OS,COUNT,APPLICATION2
2,KSC 6.7,,Mac OS X 10.5,118,
2,WebMail,Firefox 3.0,Windows Vista,14,
1,WebMail,Safari 3.1,Mac OS X 10.5,31,
1,Entourage 12.15,,Mac OS X 10.5,4,
1,iCal 3.0,,Mac OS X 10.5,112,
2,WebAdmin,Firefox 3.0,Windows Vista,2,
2,WebAdmin Old,MSIE 7.0,Windows Vista,8,
3,WebMail Mini,MSIE 7.0,Windows Vista,1,
4,WebMail Mini Pda,MSIE 7.0,Windows Vista,22,
5,IMAP,,,66,
6,POP3,,,72,
Close

6. Click **OK.**

Upgrading Kerio Connect

Overview

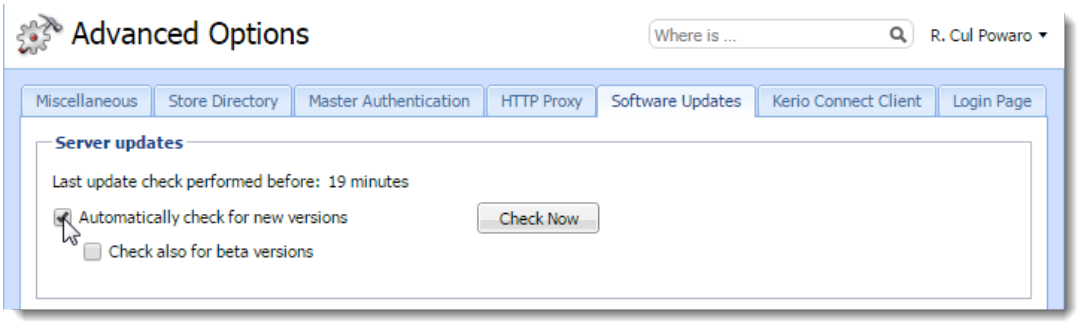
When you purchase Kerio Connect or extend your Software Maintenance, you are eligible to receive new versions of Kerio Connect and its components as soon as they are available.

Checking for updates

Kerio Connect can periodically check for new versions available:

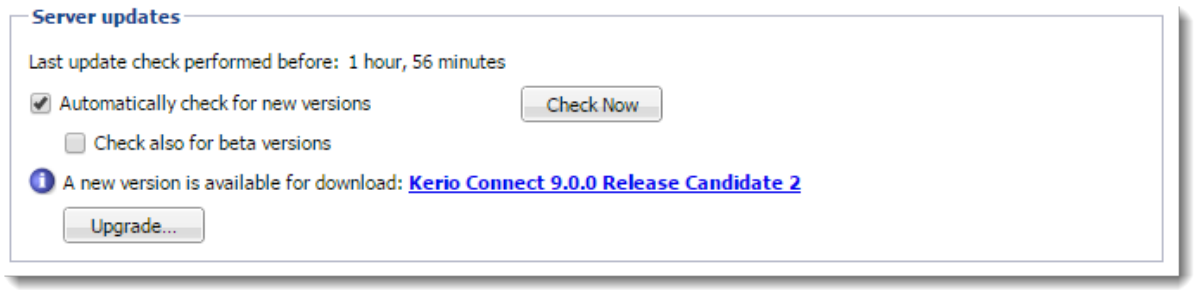
1. Go to the **Configuration** → **Advanced Options** section.
2. Switch to the **Software Updates** tab.
3. Select the **Automatically check for new versions** option.

   If Kerio Connect is used in production, do not enable the **Check also for beta versions** option.



4. To immediately check for new versions, click **Check now**.
5. Click **Apply**.

If a new version is available, Kerio Connect displays a notification in the **Server updates** section.



Configuring HTTP proxy server

If the computer with Kerio Connect installed is behind a firewall, you can use a proxy server to connect to the Internet for updates:

1. Go to the **Configuration** → **Advanced Options** section.
2. Switch to the **HTTP Proxy** tab
3. Select the **Use HTTP proxy for antivirus updates, Kerio update checker and other web services** option.
4. Type the address and port of the proxy server.
5. If the proxy server requires authentication, type the username and password.
6. Click **Apply**.

Upgrading Kerio Connect server

You can upgrade your Kerio Connect:

- Remotely from the administration interface
- Manually on the server

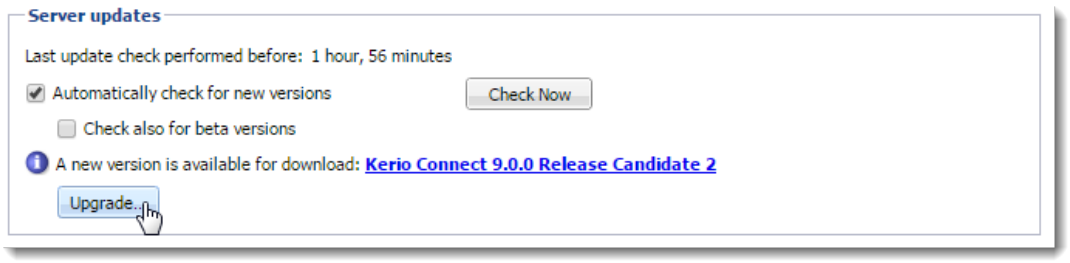
Kerio Connect saves a backup of the configuration files from the previous version in the installation folder in `UpgradeBackups`.

Upgrading the server remotely from the administration interface

New in Kerio Connect 9!

1. In the administration interface, go to the **Configuration** → **Advanced Options** section.

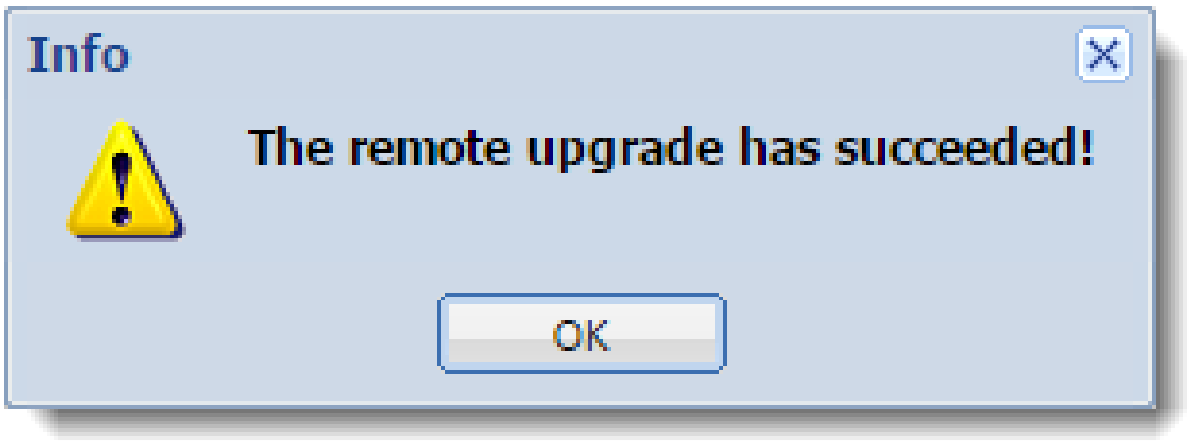
   You can upgrade from any device which can access the Kerio Connect administration interface.
2. Switch to the **Software Updates** tab.
3. Click **Upgrade** in the **Server Updates** section.



4. Click **Yes** to confirm the upgrade.

Kerio Connect starts downloading and upgrading your Kerio Connect server.

After the upgrade is finished, the Kerio Connect Administration login screen appears. Login to the administration interface to verify the remote upgrade finished successfully.



Upgrading Kerio Connect manually

Microsoft Windows

To upgrade Kerio Connect on Microsoft Windows, download and run the installation package.

The program detects the installation directory, stops all running components (Kerio Connect engine and Kerio Connect Monitor) and replaces existing files with new ones automatically.

Mac OS X

To upgrade Kerio Connect on Mac OS X, download and run the installation package.

The program detects the installation directory, stops running components (Kerio Connect engine and Kerio Connect Monitor) and replaces existing files with new ones automatically.

Linux — RPM

To upgrade Kerio Connect on Linux RPM, use this command:

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

Linux — DEB

To upgrade Kerio Connect on Linux Debian, use the same command as for installation:

```
# dpkg -i <installation_file_name.deb>
```

Kerio Connect VMware Virtual Appliance

See the article Kerio Connect VMware Virtual Appliance for information on upgrading the appliance.

Upgrading Kerio Outlook Connector

You can enable automatic updates of Kerio Outlook Connector Offline Edition (KOFF) on client stations.

1. Go to the **Configuration** → **Advanced Options** section.
2. Switch to the **Software Updates** tab.
3. In the **Kerio Outlook Connector (Offline Edition)** section, select the **Install updates automatically** option.

4. Click **Apply**.

Troubleshooting

If any problems occur during the upgrade, consult the Debug log — right-click the Debug log section and select **Messages** → **Update Checker Activity**.

Uninstalling Kerio Connect

How to uninstall Kerio Connect

Windows operating system

Uninstall Kerio Connect through **Control Panel** using the standard uninstall wizard.

 The uninstall wizard offers an option to keep the Kerio Connect data store and configuration files, if you plan to reinstall the program later.

Mac OS X operating system

Uninstall Kerio Connect through the **Kerio Connect Uninstaller**. It is available in the installation package of Kerio Connect (your current version).

 The Uninstaller offers an option to keep the Kerio Connect data store and configuration files, if you plan to reinstall the program later.

Linux operating system — RPM

Uninstall Kerio Connect using this command:

```
# rpm -e kerio-connect
```

 During the uninstallation only files from the original package and unchanged files are deleted. The configuration files, data store, and other changed or added files are kept on your computer. You can delete them manually or use them for future installations.

Linux operating system — DEB

Uninstall Kerio Connect using this command:

```
# apt-get remove kerio-connect
```

 During the uninstallation only files from the original package and unchanged files are deleted. The configuration files, data store, and other changed or added files are kept on your computer. You can delete them manually or use them for future installations.

To uninstall Kerio Connect completely including the configuration files, use this command:

```
# apt-get remove --purge kerio-connect
```

Kerio Connect VMware Virtual Appliance

What is Kerio Connect VMware Virtual Appliance for

A virtual appliance is designed for usage in VMware products. It includes the Debian Linux operating system and Kerio Connect.

For supported VMware product versions, check the product pages.

How to get Kerio Connect VMware Virtual Appliance

Download the Kerio Connect installation package according to your VMware product type:

- For VMware Server, Workstation and Fusion — download the `VMX` distribution package (`*.zip`), unzip and open it.
- For VMware ESX/ESXi — import the virtual appliance from the `OVF` file's URL — e.g.: VMware ESX/ESXi automatically downloads the OVF configuration file and a corresponding disk image (`.vmdk`).

  ```
  http://download.kerio.com/en/dwn/connect/
  kerio-connect-appliance-1.x.x-1270-linux.ovf
  ```

Tasks for shutdown or restart of the virtual machine will be set to default values after the import. These values can be set to "hard" shutdown or "hard" reset. However, this may cause a loss of data on the virtual appliance. Kerio Connect VMware Virtual Appliance supports so called *Soft Power Operations* which allow to shut down or restart hosted operating system properly. Therefore, it is recommended to set shutdown or restart of the hosted operating system as the value.

How to work with Kerio Connect VMware Virtual Appliance

When you run the virtual computer, Kerio Connect interface is displayed.

Upon the first startup, configuration wizard gets started where the following entries can be set:

- Kerio Connect administration account username and password,
- primary domain,

- DNS name of the server,
- data store.

This console provides several actions to be taken:

- change network configuration
- allow SSH connection
- set time zone
- change user `root` password
- restart a disable Kerio Connect Appliance

Figure 1 Console — network configuration

Access to the console is protected by root password. The password is at first set to: `kerio` (change the password in the console as soon as possible — under **Change password**).

Network configuration

The network configuration allows you to:

1. Viewing network adapters — MAC address, name and IP address of the adapter
2. Setting network adapters

- DHCP
- static IP address (if you do not use DHCP, it is necessary to set also DNS)

If you use a DHCP service on your network, the server will be assigned an IP address automatically and will connect to the network. If you do not use or do not wish to use DHCP for Kerio Connect, you have to set the IP address manually.
If the IP address is assigned by the DHCP server, we recommend to reserve an IP address for Kerio Connect so that it will not change.
If you run Kerio Connect VMware Appliance in the local network, check that an IP address has been assigned by the DHCP server. If not, restart the appliance.

Time zone settings

Correct time zone settings are essential for correct identification of message reception time and date, meeting start and end time, etc.

It is necessary to restart the system for your time zone changes to take effect.

How to update Kerio Connect

A terminal is available for product and operating system updates. You can switch it by pressing the standard `Alt+Fx` combination (for example, `Alt+F2`) for running a new console.
Before the first SSH connection to the terminal, it is necessary to enable the latter.

To update Kerio Connect:

1. Download the Debian package (`*.deb`) to your computer.
2. Use SCP/SSH to move it to VMware Appliance.
3. Use the `dpkg` command to upgrade Kerio Connect.

   ```
   # dpkg -i <installation_file_name.deb>
   ```

To update Debian Linux, use the `apt-get` command.

To upgrade the console, go to the Kerio Connect download page and download the **Virtual Appliance Console Upgrade Package**.

Accessing Kerio Connect

What interfaces are available in Kerio Connect

Kerio Connect includes two interfaces:

- for administrators (Kerio Connect administration)
- for users (Kerio Connect Client)

Use officially supported browsers to access the interfaces.

The web interfaces are available in several languages. The default language is the language of your browser.

Kerio Connect Client

What is Kerio Connect Client

Kerio Connect Client is a user interface which allows users to work with:

- email messages
- calendars
- contacts
- notes
- tasks
- integration with other email and calendar clients

How to login

To login to Kerio Connect Client, ask your administrator to give you the URL address of Kerio Connect.

Open your browser and enter the URL in the following format :

`http://kerio.connect.name/`

`http://mail.feelmorelaw.com/`

On the login page, enter your username and password.

If you do belong to the primary domain, enter also the domain name in the username field (e.g. `wsmith@notprimarydomain.com`).

 If you cannot access your account from, for example, your home computer, your company policy may have forbidden the access — ask your administrator.

Kerio Connect administration

How to log in

Only users with corresponding access rights can login to the administration interface.

To login to the Kerio Connect administration, open your browser and enter the DNS name of Kerio Connect:

`kerio.connect.name/admin`

You can access the administration interface only via a secured connection over the HTTPS protocol on port 4040. Your browser will automatically redirect you to:

`https://kerio.connect.name:4040/admin`

 If Kerio Connect is behind firewall, you must allow the HTTPS service on port 4040.

On the login page, enter the username and password of Kerio Connect administrator.

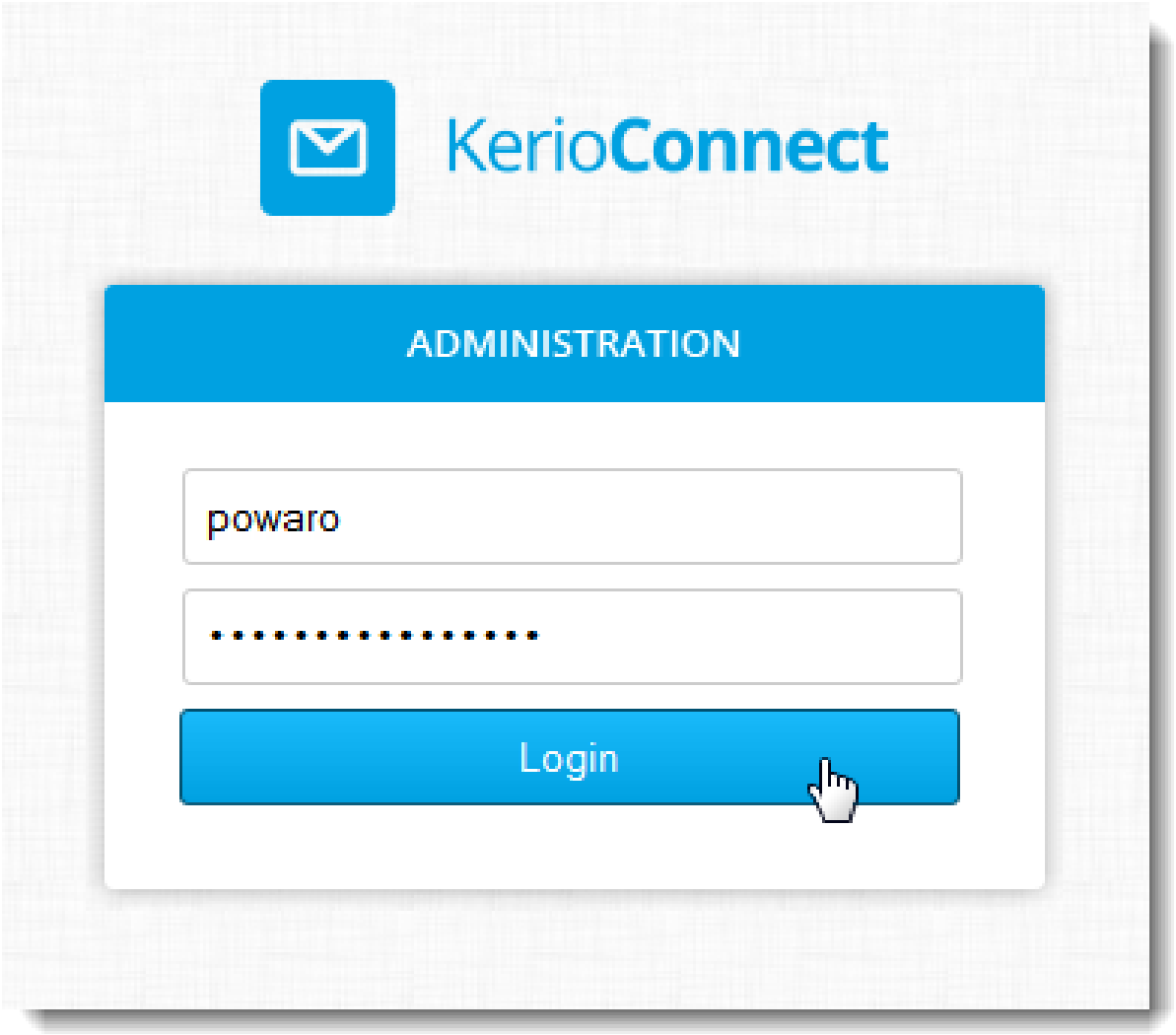


Figure 1 Admin login

If the administrator does not belong to the primary domain, enter also the domain name (e.g. `powaro@feelmorelaw.com`).

Once you login, confirm the security exception — Kerio Connect has issued a self-signed certificate upon installation and since it is not signed by a certification authority, browsers require your confirmation.

First login

If you are logging in the administration interface for the first time, use the username and password of the administrator you created during the installation of Kerio Connect.

How to log out

It is recommended to log out after finishing work in the administration interface. Disconnecting from Kerio Connect increases the security of data stored on the server.

Automatic logout

If any of the interfaces is idle for a pre-defined time, you will be automatically disconnected.

To set the period for automatic logout:

1. In the administration interface, go to section **Configuration** → **Advanced options** → **tab Kerio Connect Client**.
2. In the **Session security** section, set the timeout for
   - **session expiration** — Kerio Connect will end the session after the set timeout without any activity in an interface

     The timeout is reset each time user performs an action.

   - **maximum session duration** — timeout after which users will be logged out even if they actively use an interface
3. As a protection against session hijacking you can force logout after Kerio Connect user changes their IP address.

   Do not use this option, if your ISP changes IP addresses during the connection (e.g. in case of GPRS or WiFi connections).
4. Save the settings.

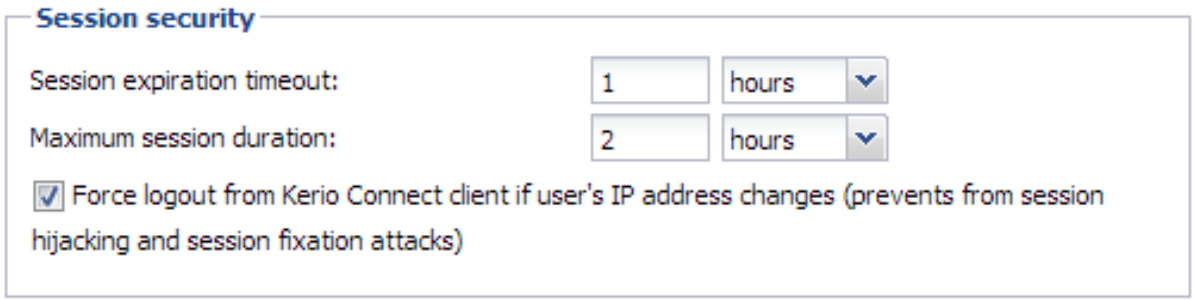


Figure 2 Session security

The session security settings apply to both the administration interface and Kerio Connect Client.

Accessing Kerio Connect administration

Accessing Kerio Connect administration

You can access the Kerio Connect administration only via secured connection (HTTPS) at:

`https://connect_server:4040/admin`

You can use either the IP address or the DNS name of Kerio Connect.

Type in `connect_server/admin` and the browser will automatically redirect you to the secured connection and port 4040.

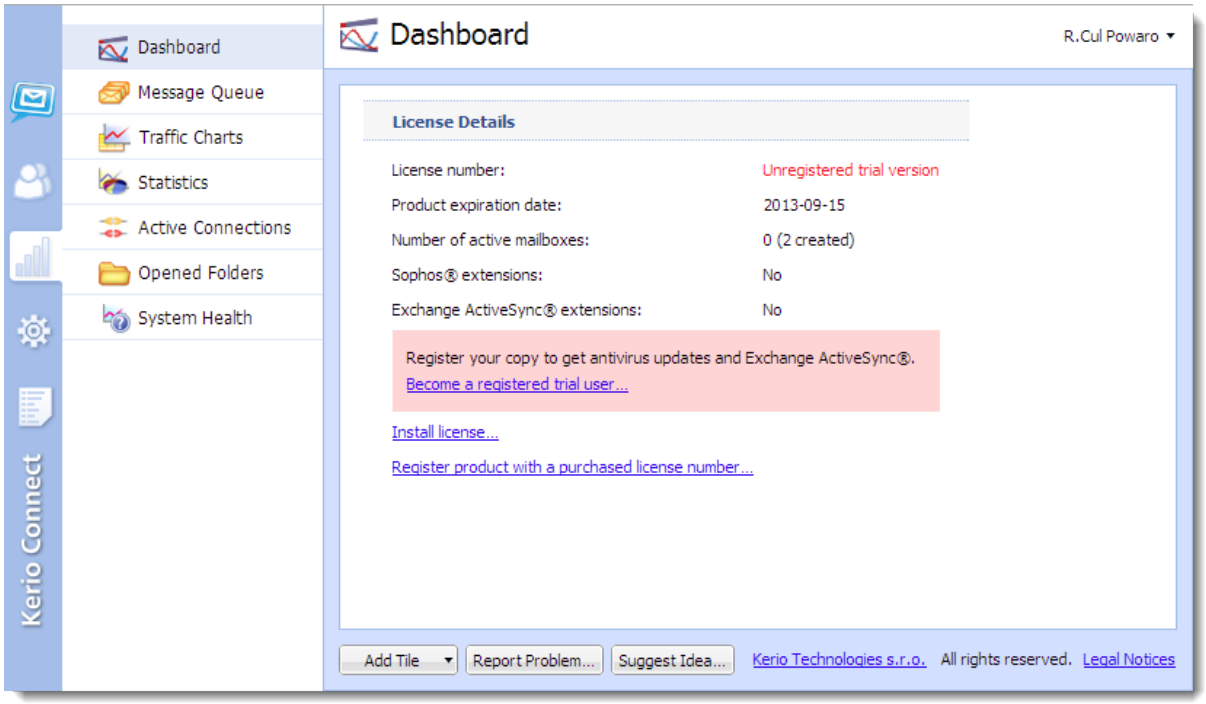


Figure 1 Welcome to Kerio administration

Accessing the administration interface remotely

Administrators can access the administration interface:

From the computer where Kerio Connect is installed
: Default settings of Kerio Connect.

From remote computers

Go to section **Configuration** → **Administration Settings** and check option **Allow administration from remote host**.

You can specify allowed IP addresses group.

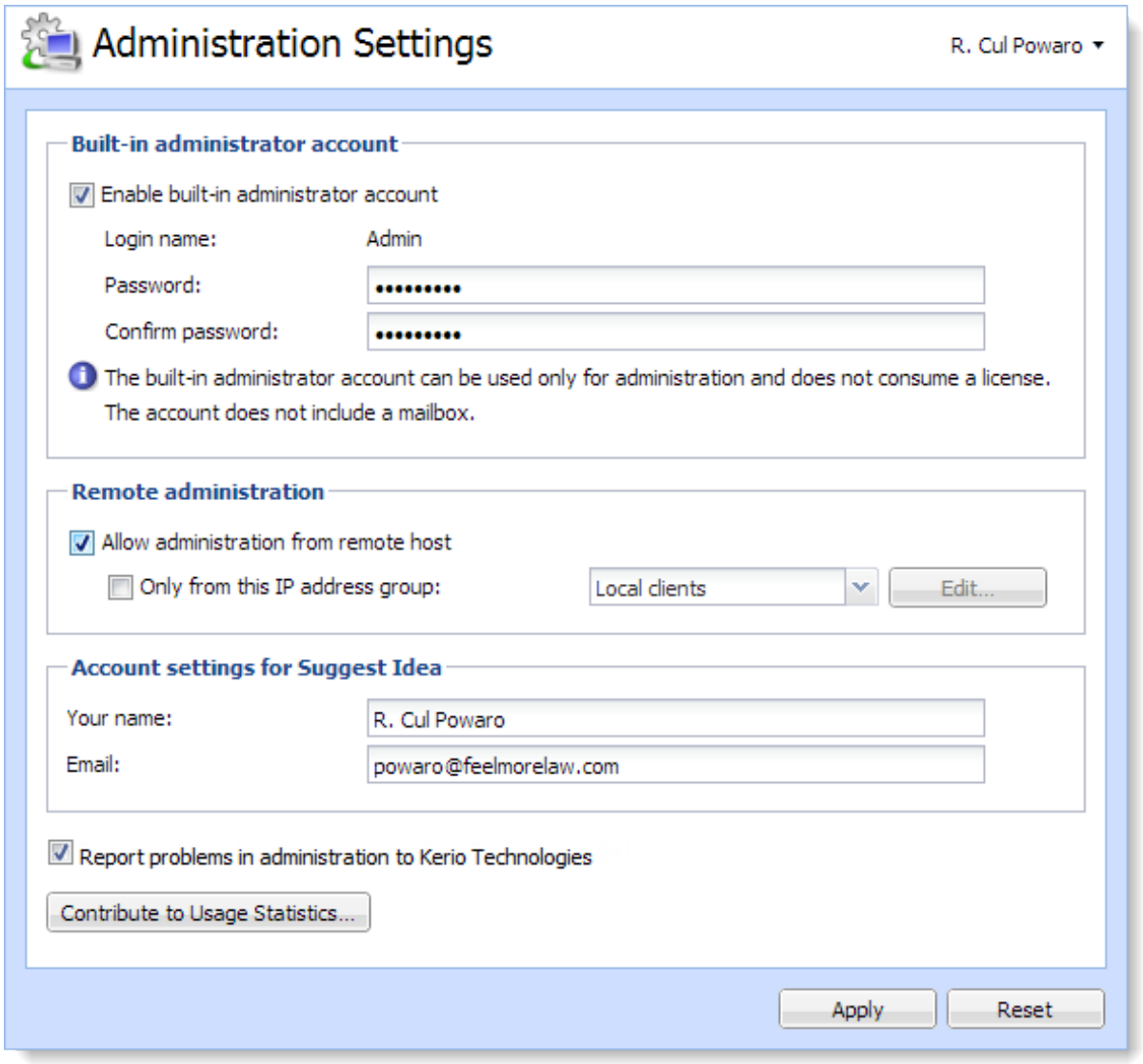


Figure 2 Configuring administration access

Types of administrator accounts

In Kerio Connect, there are two types of administrator accounts:

- built-in administrator
- user with special access rights to the administration

individual users/groups can be assigned these levels of access rights:

- **Whole server read/write** — admin can view and edit the whole administration interface
- **Whole server read only** — admin can view the whole administration interface
- **<domain_name> accounts** — admin can view and edit their own domain settings

Creating administrator accounts

To specify access rights for a user/group:

1. Double click the user/group in section **Accounts** → **Users/Groups**.
2. On tab **Rights**, select the level of access rights.
3. Confirm.

Users can now login to the administration interface.

 In Kerio Connect, users can also manage (be administrators of) public and archive folders.

Enabling built-in administrator account

The built-in administrator account is available solely for accessing the administration interface. Such account:

- has the Whole server read/write access
- has no email address and mailbox
- does not consume a license

To configure the built-in admin:

1. Go to section **Configuration** → **Administration Settings**.
2. Check option **Enable built-in administrator account**.
3. Enter and confirm the password.

   The username is set to `Admin` and cannot be changed.

 If another user (in **Accounts** → **Users**) with username `Admin` exists, from now on this user will be required to use their username including the domain to login to the Kerio Connect administration.
Example: `admin@feelmorelaw.com`

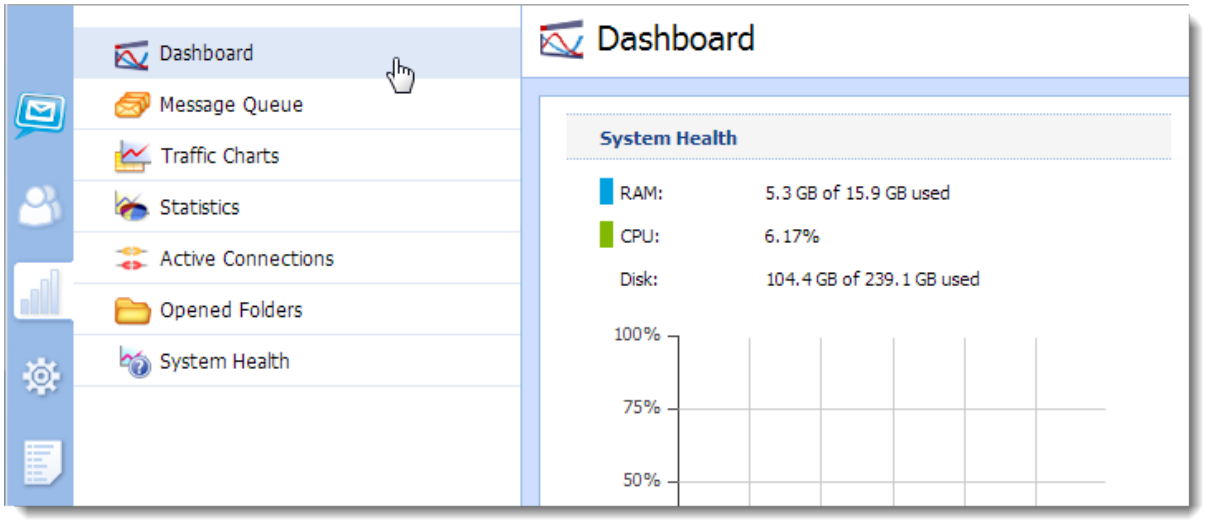
 The same policy as removing other administrator accounts is applied when disabling this account.

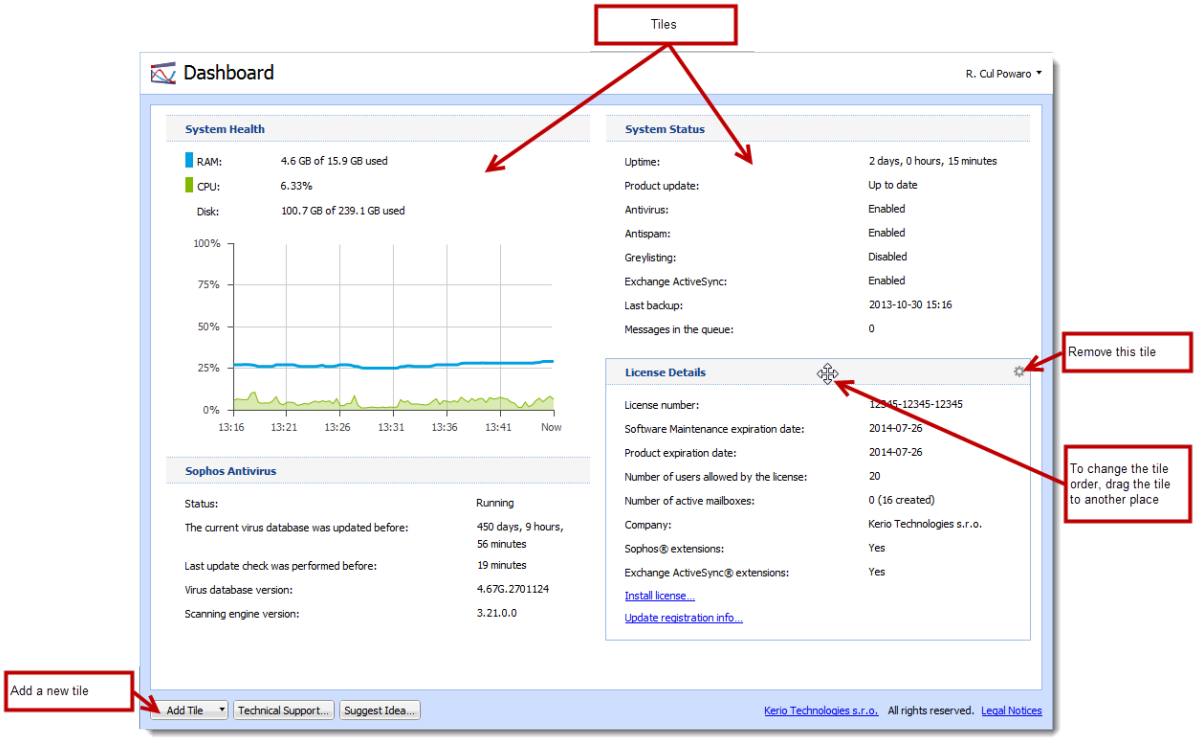
Using Dashboard in Kerio Connect

Dashboard overview

Kerio Connect includes a customizable Dashboard. Dashboard consists of tiles. Each tile displays a different type of information (graphs, statistics, Kerio news etc.)

To display Dashboard, go to **Status** → **Dashboard**.




Tiles
Dashboard
R. Cul Powaro
System Health
RAM: 4.6 GB of 15.9 GB used
CPU: 6.33%
Disk: 100.7 GB of 239.1 GB used
100%
75%
50%
25%
0%
13:16
13:21
13:26
13:31
13:36
13:41
Now
System Status
Uptime: 2 days, 0 hours, 15 minutes
Product update: Up to date
Antivirus: Enabled
Antispam: Enabled
Greylisting: Disabled
Exchange ActiveSync: Enabled
Last backup: 2013-10-30 15:16
Messages in the queue: 0
License Details
License number: 12345-12345-12345
Software Maintenance expiration date: 2014-07-26
Product expiration date: 2014-07-26
Number of users allowed by the license: 20
Number of active mailboxes: 0 (16 created)
Company: Kerio Technologies s.r.o.
Sophos® extensions: Yes
Exchange ActiveSync® extensions: Yes
Install license...
Update registration info...
Sophos Antivirus
Status: Running
The current virus database was updated before: 450 days, 9 hours, 56 minutes
Last update check was performed before: 19 minutes
Virus database version: 4.67G.2701124
Scanning engine version: 3.21.0.0
Add Tile
Technical Support...
Suggest Idea...
Kerio Technologies s.r.o. All rights reserved. Legal Notices
Remove this tile
To change the tile order, drag the tile to another place
Add a new tile

Navigating through the Kerio Connect administration interface

Overview

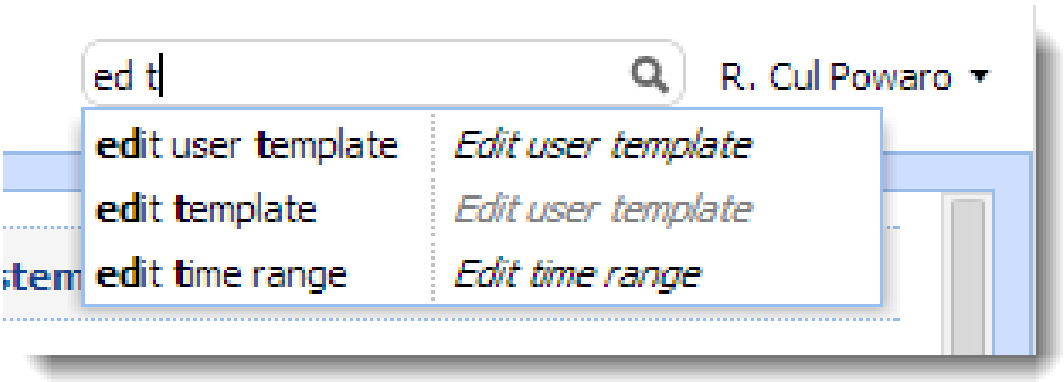
Using keywords, you can easily search for the location of any section or dialog in the Kerio Connect administration interface.

Searching for specific sections in the administration interface

If you need to configure a specific function, the Kerio Connect administration can help you with navigating to a particular section in the interface.

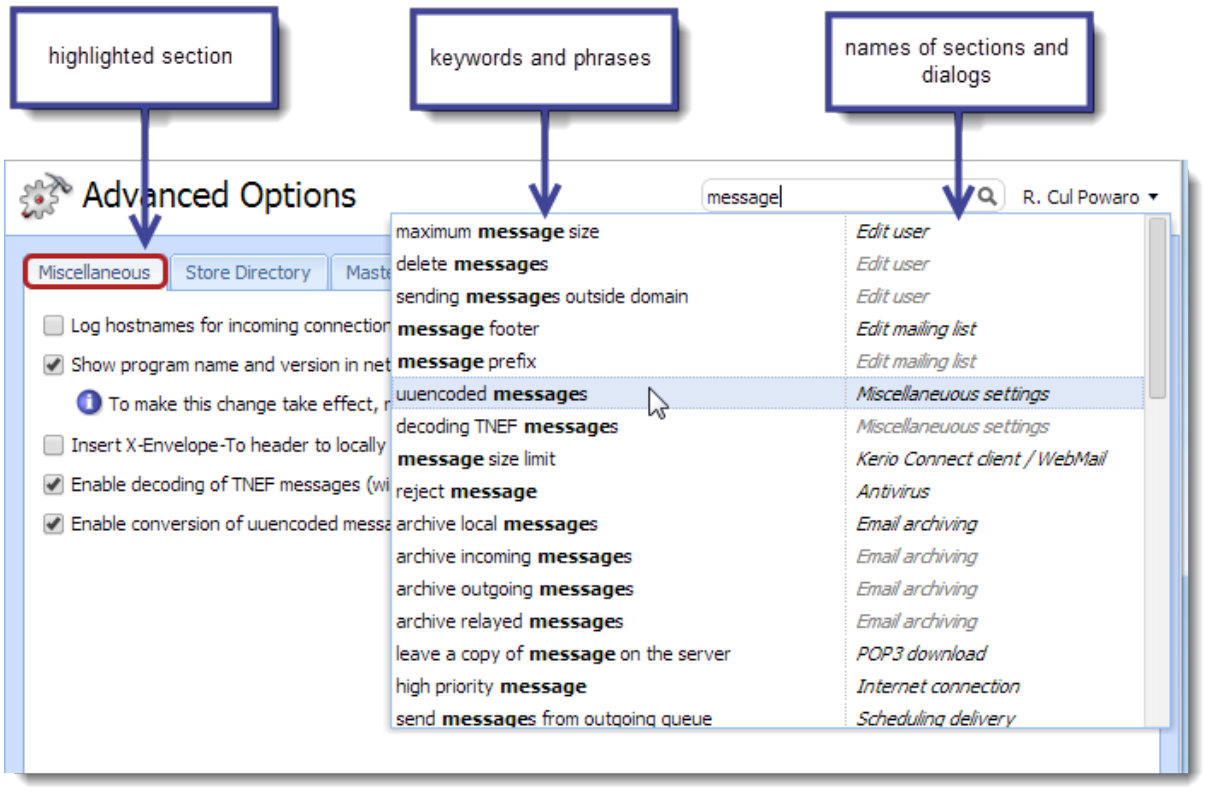
1. Go to the Kerio Connect administration interface.
2. In the top right corner of any page, type what you want to find in the **Where is** box.

   As you type, Kerio Connect offers you a list of keywords and phrases. You can even type just a few letters from multiple words.



3. Select a phrase or use the arrow keys to navigate through the list.

   As you browse through the list, Kerio Connect automatically highlights and switches to the selected section/dialog.



Usernames, domain names or similar items are not included in the search results.

Domains in Kerio Connect

What are domains in Kerio Connect

Email domain is a unique identifier which is used to recognize to which server messages should be delivered. In email address, the domain identifier follows the `@` symbol.

Email domain can differ from the name of the server where Kerio Connect is installed. See the following example:

- domain name — `company.com`
- email domain name — `mail.company.com`
- user email address — `user@company.com`

Kerio Connect may include any number of mail domains. Various parameters can be defined for each domain and its users.

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

Domains are managed in section **Configuration** → **Domain**.

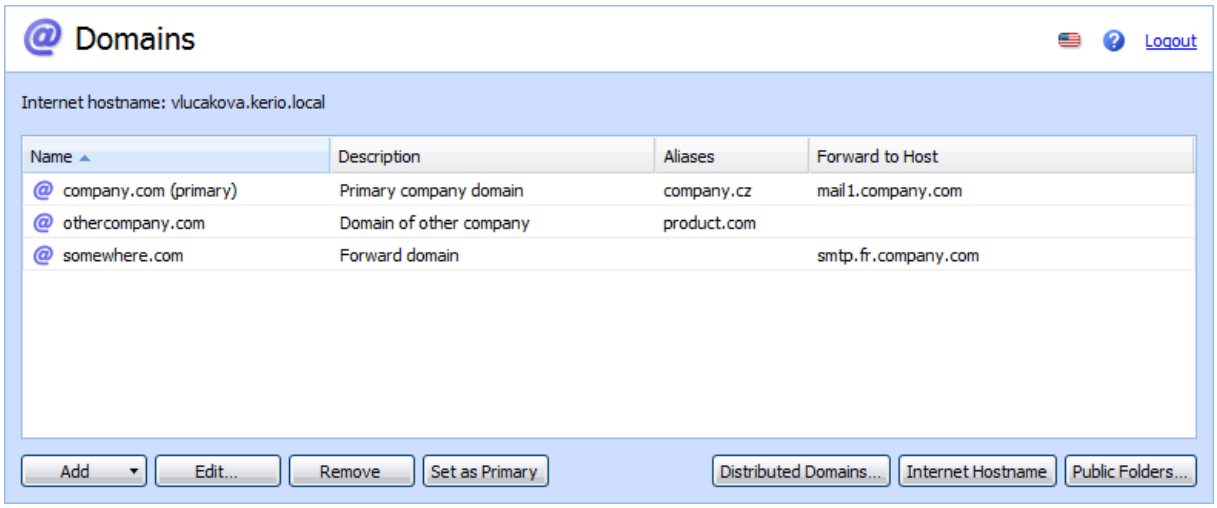


Figure 1 Domains section

Internet hostname

To make email deliverable to mail domains, Kerio Connect requires specification of a DNS name of the host where the server is running. Server names are also used for server identification while establishing the SMTP traffic.

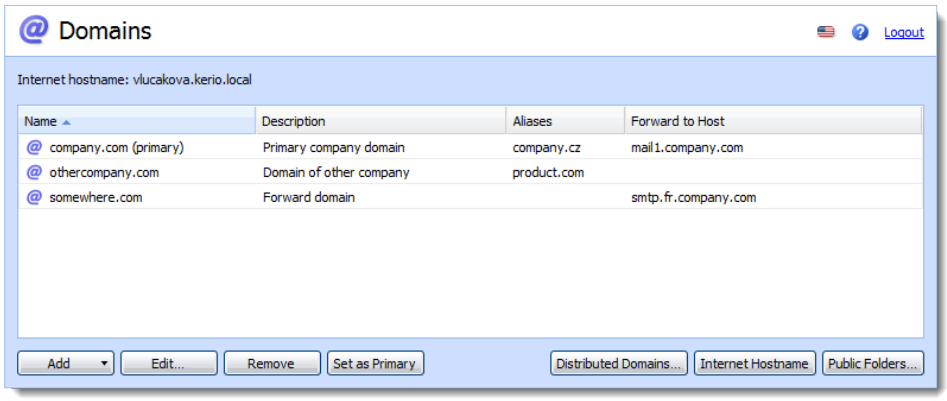
Upon initializing the SMTP communication, the EHLO command is used for retrieving reverse DNS record. The server that communicates with Kerio Connect can perform checks of the reverse DNS record.

If Kerio Connect 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.

To change the internet hostname, click on the **Internet Hostname** button in section **Configuration → Domains**.

Primary domain

One domain in Kerio Connect must be set as **primary**. Users defined in a primary domain do not have to use their full email address for authentication.



By default, the first domains created automatically. When further domains are added, any of the domains can be set as primary (usually the one with the most users).

To change the primary domain, select the domain and click on the **Set as Primary** button in section **Configuration** → **Domains**.

Domains section in Kerio Connect

In the administration interface, domains are managed in section **Configuration** → **Domains**.

Various information (columns) can be displayed in the table. Right-click on any column name and check the items you wish to display as **Columns**.

Adding new domains

To add a new domain to Kerio Connect, consult this article.

Creating domains in Kerio Connect

Adding domains in Kerio Connect

Domains are defined in the Kerio Connect administration interface in section **Configuration** → **Domains**:

1. Click **Add** → **Local Domain**.
2. Type the domain name and description for better reference.
3. Set limit for the maximum number of domain users who can connect to Kerio Connect at a time (recommended for the ISPs).

    The number of users in the **User Count** column in domain list gets red any time the limit is exceeded.

4. Save the settings.

Now the domain is ready. Additional settings are available.

Additional configuration

For each domain, you can also:

- limit the message size and set items clean-out to save space on the server
- connect to directory service and map users
- customize Kerio Connect
- forward emails to another server
- create aliases for the domain

In the **Configuration** → **Domains** section, you can also:

- set new internet hostname
- manage public folders
- create distributed domains

Deleting domains

If you wish to delete domains in Kerio Connect, the domain must not:

- be a primary domain
- contain any users
- have aliases assigned

Connecting Kerio Connect to directory service

Supported directory services in Kerio Connect

Kerio Connect supports the following directory services:

- Microsoft Active Directory
- Apple Open Directory

Why connect to directory services

Mapping accounts from a directory service provides these benefits:

- **Easy account administration** — you can manage user accounts from a single location. This reduces possible errors and simplifies administration.
- **Online cooperation of Kerio Connect and directory service** — Adding, modifying and removing user accounts/groups in the LDAP database is applied to Kerio Connect immediately.
- **Using domain name and password for login** — Users can use the same credentials for Kerio Connect Client login and domain login.

- Mapping is one-way only. Data is synchronized from a directory service to Kerio Connect. Adding new users/groups in Kerio Connect creates local accounts.
- If a directory server is unavailable, it is not possible to access Kerio Connect. Create at least one local administrator account or enable the built-in admin.
- Use ASCII for usernames when creating user accounts in a directory service.

Microsoft Active Directory

To connect Kerio Connect to Microsoft Active Directory, follow these steps:

1. On the Microsoft Active Directory server, install the Kerio Active Directory Extension.
2. In the Kerio Connect administration interface, go to the **Configuration** → **Domains** section.
3. Double-click the domain and go to the **Directory Service** tab.

4. Check the **Map user accounts and groups from a directory service** option and select the type of directory service.

5. Type the DNS name or IP address of the Microsoft Active Directory server.

   If a non-standard port is used for communication of Kerio Connect with Microsoft Active Directory, add the port number to the DNS name/IP address.

6. Type the **Username** and **Password** of a Microsoft Active Directory administrator with full access rights to the administration.

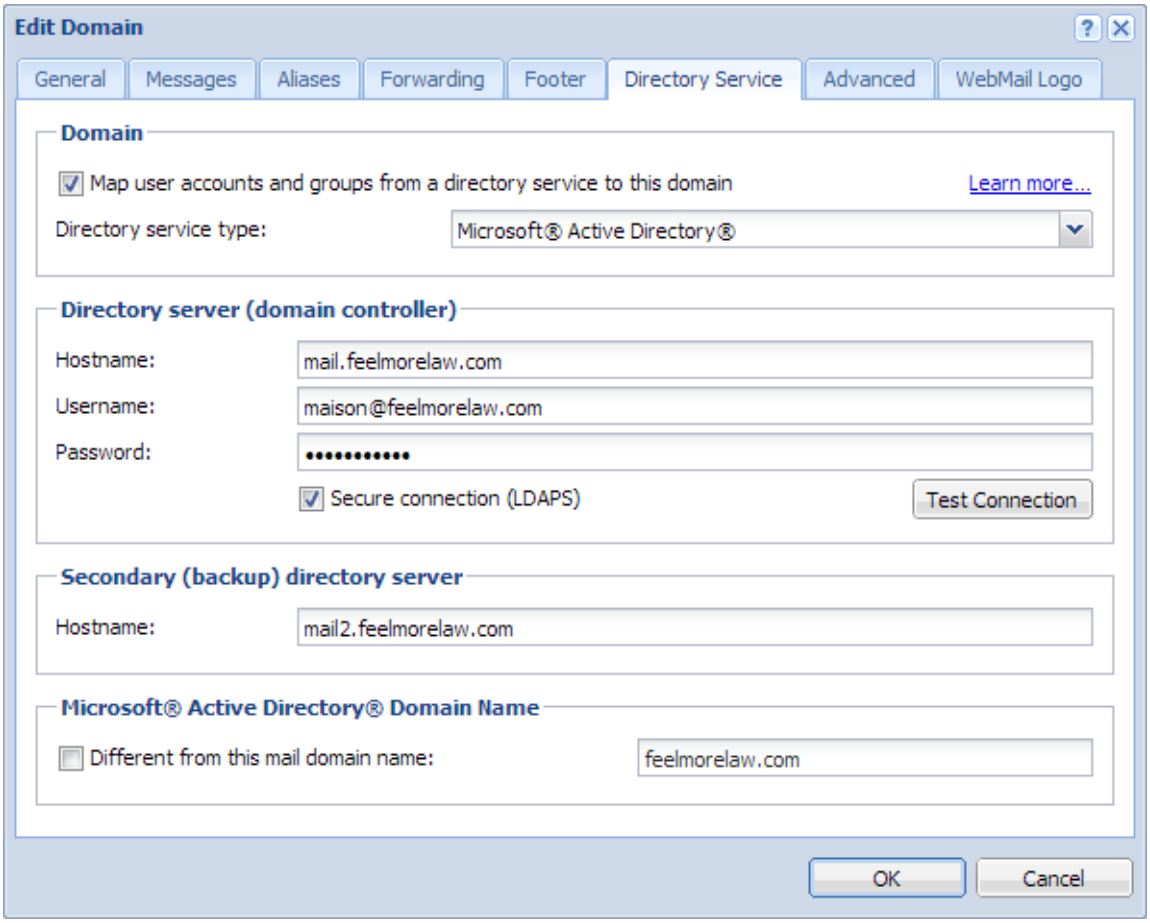
7. **Enable secured connection (LDAPS)** to protect fragile data (e.g. user passwords) sent from Microsoft Active Directory to Kerio Connect and vice versa.

   If you enable LDAPS, the DNS name is required in step 5.

8. Click **Test connection** to verify you entered the correct data.

9. Save the settings.

Now you can map users to Kerio Connect.



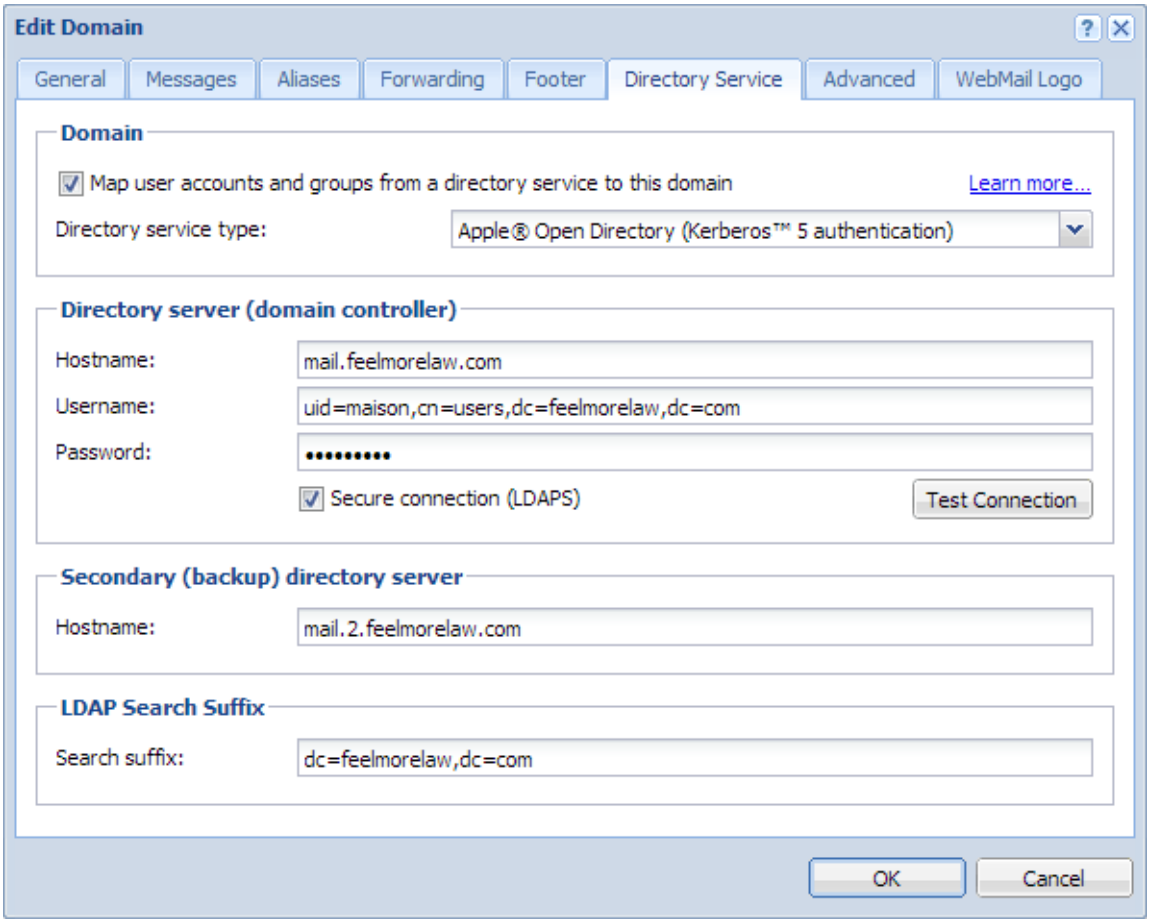
Apple Open Directory

1. On the Apple Open Directory server, install the Kerio Open Directory Extension.
2. In the Kerio Connect administration interface, go to the **Configuration** → **Domains** section.
3. Double-click the domain and go to the **Directory Service** tab.
4. Check the **Map user accounts and groups from a directory service** option and select the type of directory service.
5. Type the DNS name or IP address of the Apple Open Directory server.

   If a non-standard port is used for communication of Kerio Connect with Apple Open Directory, add it to the DNS name/IP address.
6. Type the **Username** and **Password** of an Apple Open Directory administrator with full access rights to the administration.
7. **Enable secured connection (LDAPS)** to protect fragile data (e.g. user passwords) sent from Apple Open Directory to Kerio Connect and vice versa.

   If you enable LDAPS, the DNS names is required in step 5.
8. Click **Test connection** to verify you entered the correct data.
9. Save the settings.

Now you can map users to Kerio Connect.



Mapping users from directory services

For information on activating users, read article Creating user accounts in Kerio Connect.

Migrating user accounts from local database to directory service

For detailed information, read article Migrating user accounts from local database to directory service.

Troubleshooting

All information about directory service can be found in the Debug and Warning logs.

Migrating user accounts from local database to directory service

Overview

You can connect your Kerio Connect to Microsoft Active Directory or Apple Open Directory.

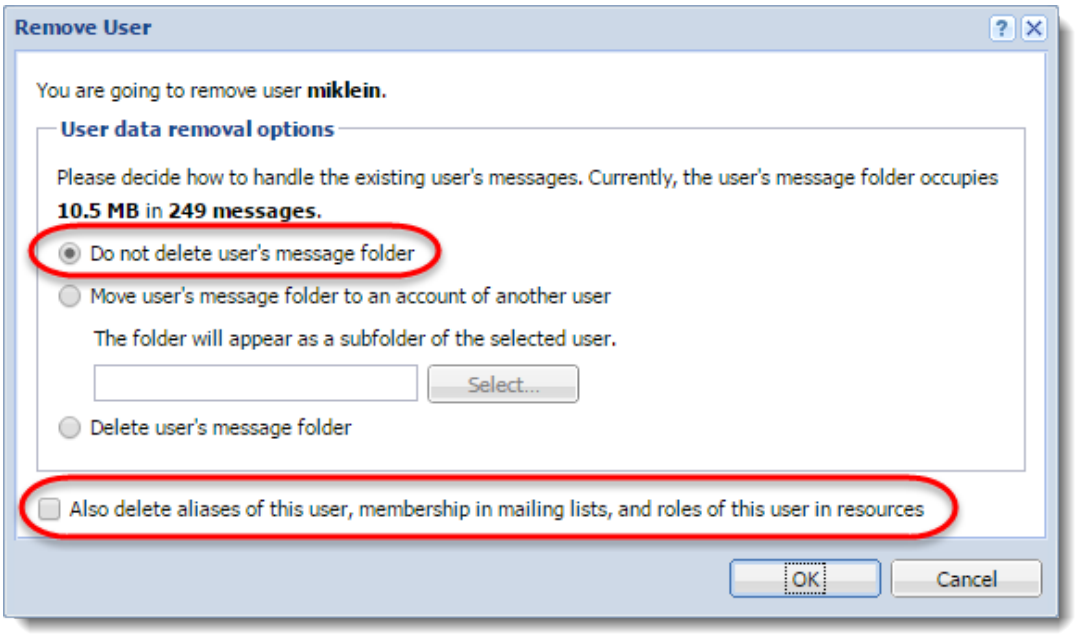
To migrate the users accounts from a local database to a directory service:

1. Remove the local accounts from Kerio Connect.
2. Connect your domain to a directory service.
3. Create new accounts in the directory service with identical usernames as before.

Migrating users

1. In the administration interface, go to **Accounts** → **Users**.
2. Remove all local users you want to migrate to a directory service.

In the **Remove User** dialog box, select **Do not delete user's message folder** and unselect the option **Also delete aliases of this user**.



3. Connect your domain to a directory service.

   See Connecting Kerio Connect to directory service for details.

4. In the directory server, create users with the same usernames as you had before.

5. In Kerio Connect, activate the users from the directory service.

   See Mapping accounts from a directory service for details.

Kerio Connect matches the users with the mailboxes and users can see all their previous messages.

Troubleshooting

All information about directory service can be found in the Debug and Warning logs.

Renaming domains in Kerio Connect

What to prepare

If needed, Kerio Connect enables you to rename your domain in a simple way. Once a domain is renamed, the original name becomes an alias. This ensures that email messages sent to addresses with the original name are always delivered.

	Original	Server restart
domain name	`old_domain.com`	`new_domain.com`
names_of_aliases	`alias.com`	`old_domain.com` `alias.com`

Table 1 Rename Domain

The domain configuration will not change after renaming.

Any calendar events created before renaming will not be available for editing or removing after application of the new name.

How to rename domains

Before you start the process, make sure:

- to purchase a domain from your provider that its name is registered in DNS records — test it
- to make a full backup of your message store before and after the renaming process

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click the domain you wish to rename.
3. On the **General** tab, click on **Rename**, enter the new name and confirm.

If you wish to cancel the domain rename action, you can do so before the next server restart. Click on **Cancel Rename** in the domain's configuration.

4. Restart the server.

Before the restart, all operations will be performed using the original name. During the restart, the original domain name will automatically be replaced with the new name in the configuration files.

Renaming distributed domains

Before you start renaming distributed domains:

1. Disconnect all servers.
2. Rename each domain separately (as described above).
3. Reconnect renamed servers to distributed domain.

Post-renaming issues

If user's mail filters include addresses of users from the renamed domain, they need to change the rules.

If users have Kerio Outlook Connector (Offline Edition) installed on their host, it is necessary to empty the cache once the domain is renamed.

Distributed domains in Kerio Connect

Distributed domains

If your company uses more Kerio Connect servers located in different cities/countries/continents, you can use distributed domain.

Distributed domain connects the servers together and moves all users across all servers into a single email domain.

Distributed domain requires users mapped from a directory service.

For details read the Distributed domains manual.

Creating user accounts in Kerio Connect

Overview

In Kerio Connect, user accounts represent physical email boxes.

With user accounts you :

- Authenticate users to their accounts (mail, calendar etc.)
- Set access rights to Kerio Connect administration

Manage users in the administration interface in **Accounts** → **Users**.

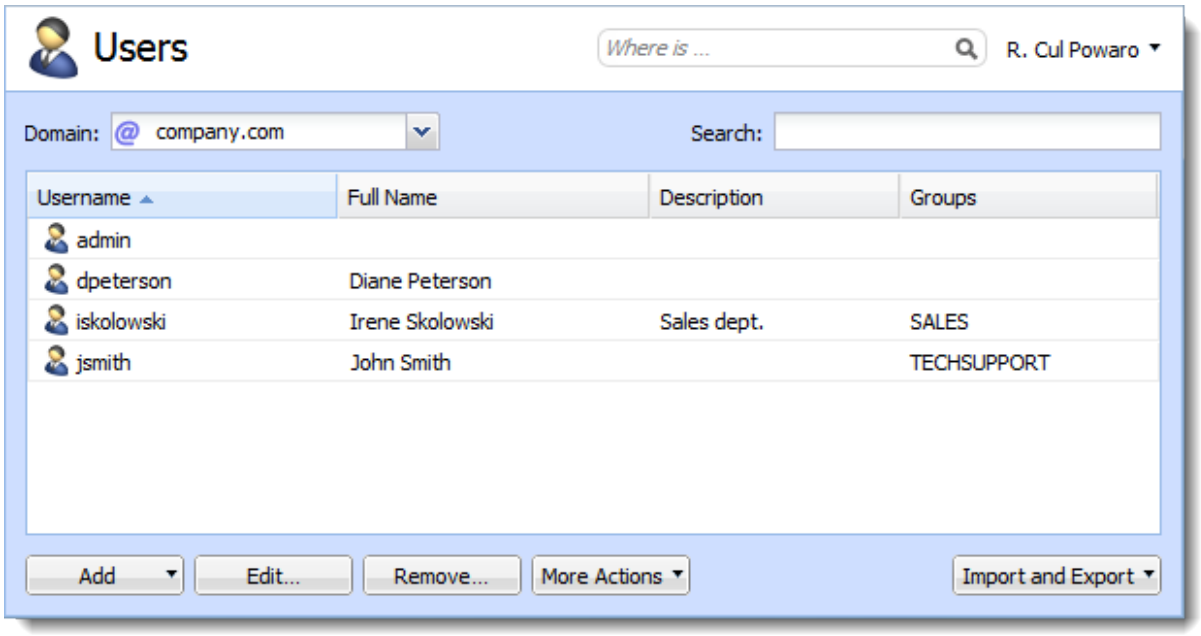


Figure 1 Users

Creating user accounts

You can create either a local user or map existing users from a directory service.

Accounts must belong to a domain. Each domain may include both local and mapped users. The number of accounts is limited only by your license.

Local accounts can also be imported to Kerio Connect. Read this article for more information.

Creating local accounts

Local accounts are created and managed through the Kerio Connect administration interface.

1. Go to **Accounts** → **Users** and select a domain for the new account.
2. Click **Add** → **Add Local User** (or use a template).
3. On the **General** tab, type a new username and password.

   The domain may require secure password (see the Password policy in Kerio Connect article).

    Usernames are not case-sensitive and cannot include spaces and special characters.

4. Optional settings:
   - create email address aliases
   - forward messages to another mailbox (within or outside Kerio Connect)
   - add users to groups
   - set space quotas for users
   - configure access rights to the administration interface
   - manage account limits (message count, sending outgoing messages, etc.)
   - maintain accounts (message clean-out, etc.)
   - restrict access to services
   - add personal and contact information

    If you store user passwords in the SHA format, use appropriate security policy.

5. Click **OK.**

The users are displayed in section **Accounts** → **Users**.

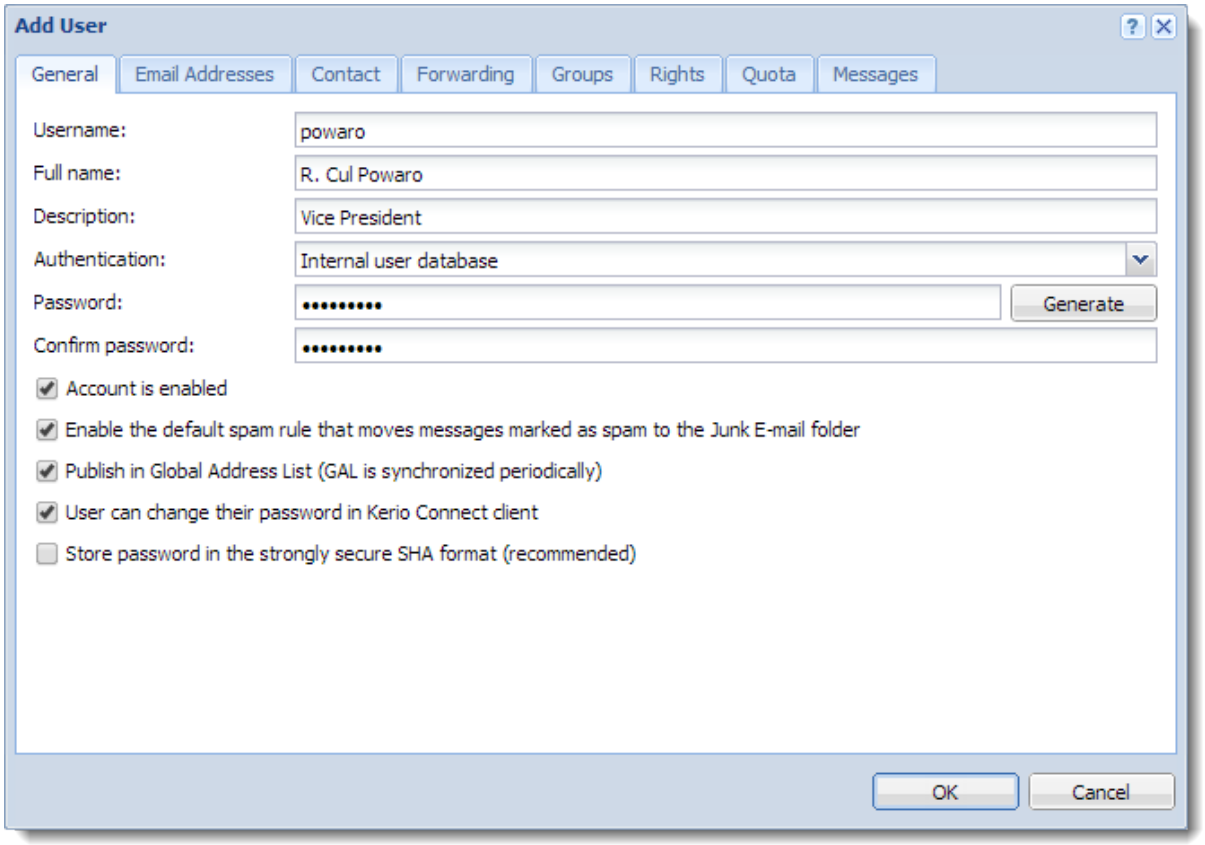


Figure 2 Adding users

Mapping accounts from a directory service

To add users from a directory service, you must:

- connect Kerio Connect to a directory service
- activate users in the administration interface

To activate users:

1. Go to section **Accounts** → **Users** and select a domain in which you want to create an account.
2. Click **Add** → **Add From a Directory Service**.
3. Select any users you wish to map to Kerio Connect (you can add users later).
4. Click **Next**.
5. Click **Finish**.

The users are displayed in section **Accounts** → **Users**.

Templates

If you plan to create numerous local accounts with similar settings, create a template.

1. In the administration interface, go to **Configuration** → **Definitions** → **User Templates**.
2. Type a name for the template and specify all settings which will be common for all users.
3. Save the settings.
4. In section **Accounts** → **Users**, Click **Add** → **Use Template** and complete the user settings.

Disabling and deleting user accounts

User accounts can be disabled temporarily or deleted permanently. Both disabling and deleting free up your license.

You cannot disable/delete the following user accounts:

- your own account
- user with higher level of administration rights

Disabling users temporarily

When you disable user accounts temporarily, users cannot login to Kerio Connect.

However, all messages and settings of this user remain available in Kerio Connect.

1. In the administration interface, go to section **Accounts** → **Users**.
2. Double-Click the user and on the **General** tab, disable the **Account is enabled** option.
3. Save the settings.

The user now cannot access Kerio Connect Client or the Kerio Connect administration.

To reverse the action, go to user's settings and select **Account is enabled**.

This action is different from blocking when a password guessing attack occurs.

Deleting users permanently

1. In the administration interface, go to **Accounts** → **Users**.
2. Select the user and Click on **Remove**.

The **Remove Users** dialog opens.

3. You can:
   - delete the user's mailbox
   - keep the user's mailbox
   - transfer it to another account in Kerio Connect
   - delete other settings of the user (aliases, roles, etc.)
4. Click **OK.**

Instant messaging files are always deleted.

Troubleshooting

All information about users can be found in the Config log.

Information about deleting users is logged in the Warning log

Adding company and user contact information in Kerio Connect

Overview

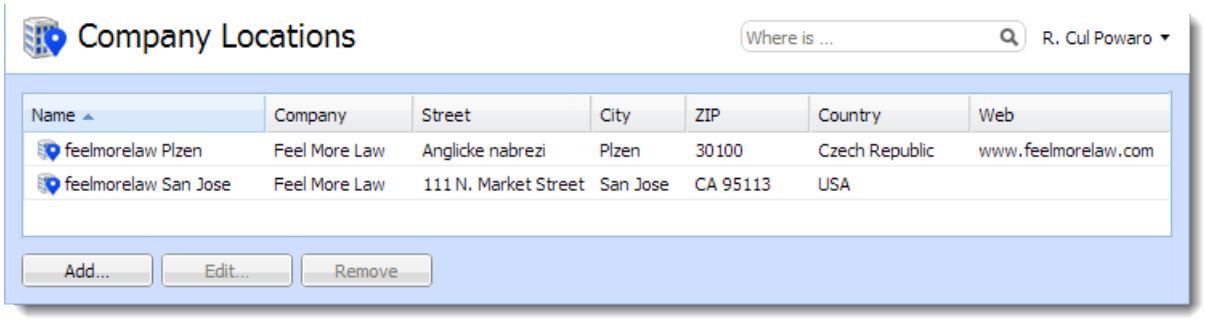
In Kerio Connect, you can add detailed contact information for your company or for individual users.

Kerio Connect:

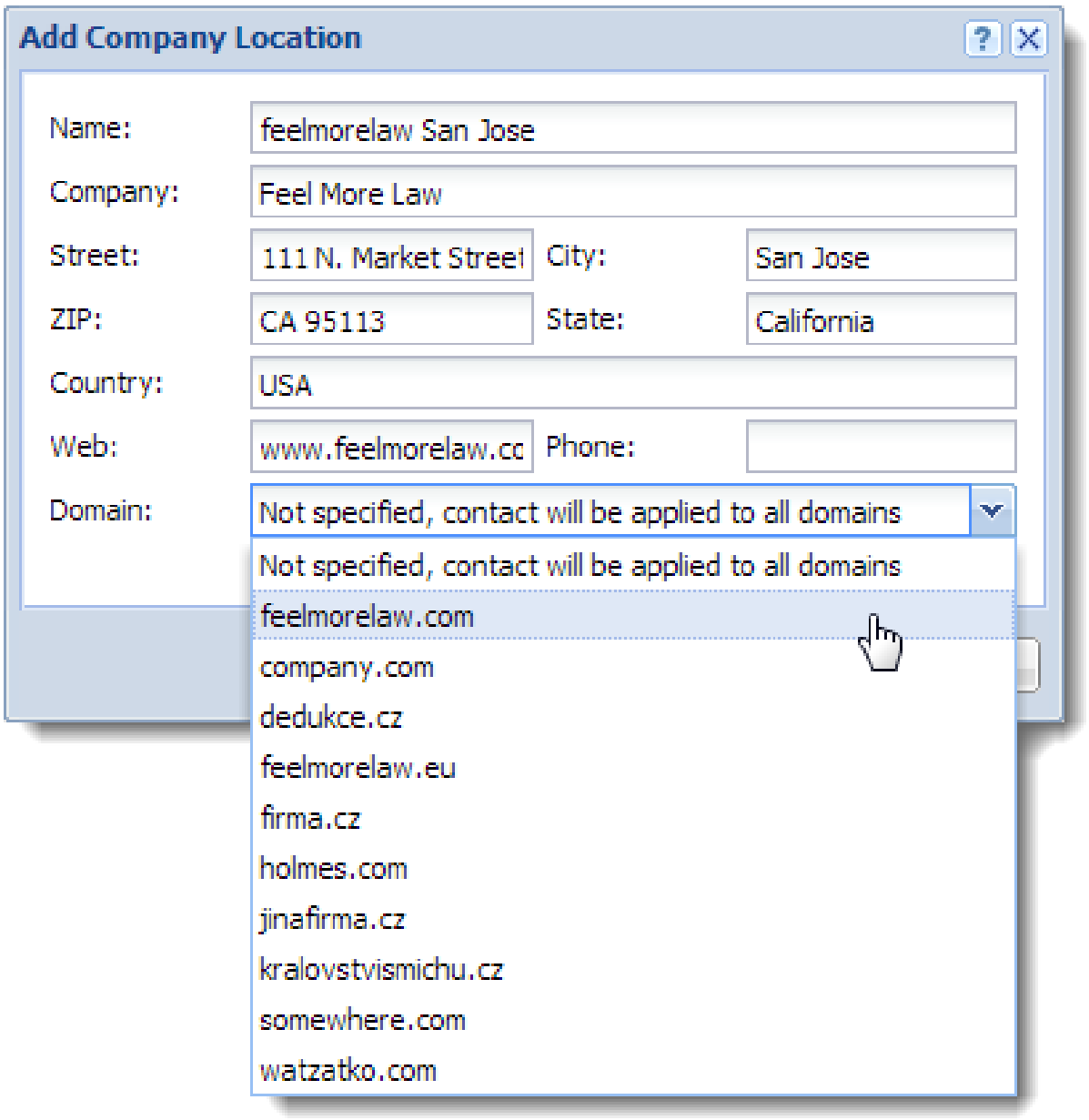
- displays this information in users' contact details
- uses this information when appending automatic domain footers (See Customizing Kerio Connect for more on footers.)

Setting company locations

If you have several different offices, you can define company locations for each of your them and assign it to a domain or individual users.

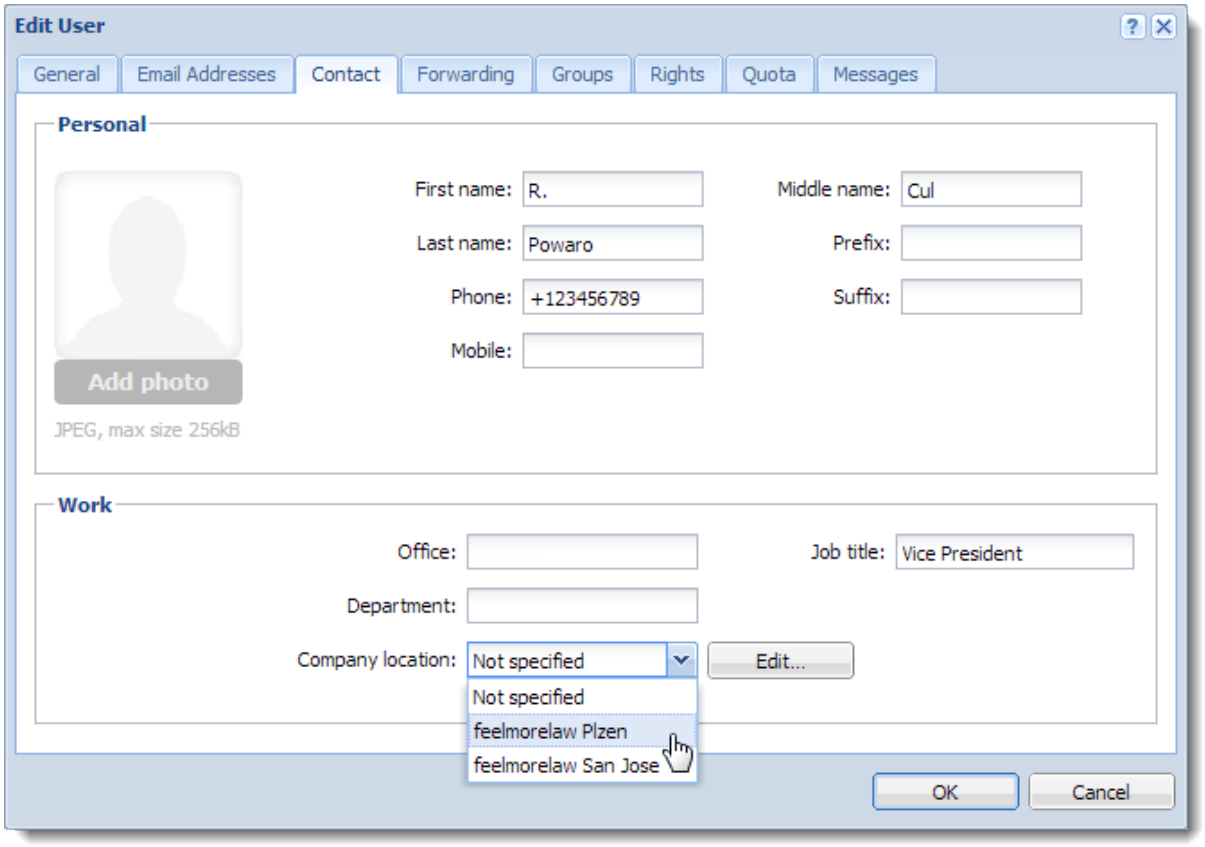


1. In the administration interface, go to **Definitions** → **Company Locations**.
2. Click **Add**.
3. Fill in the address information.
4. If you want this information to be automatically used for a specific domain, in the **Domain** drop-down menu, select the domain.
5. Click **OK**.



Adding contact details to users

1. In the Kerio Connect administration interface, go to **Accounts** → **Users**.
2. In the **Edit User** dialog box, click the **Contact** tab.
3. Fill in the user's details.
4. Add a photo of the user.
5. Select the user's company location.
6. Save the settings.



If you assign company locations to users, Kerio Connect displays this information in the contact details of the user.

Creating user groups in Kerio Connect

About user groups

You can use user groups in Kerio Connect to:

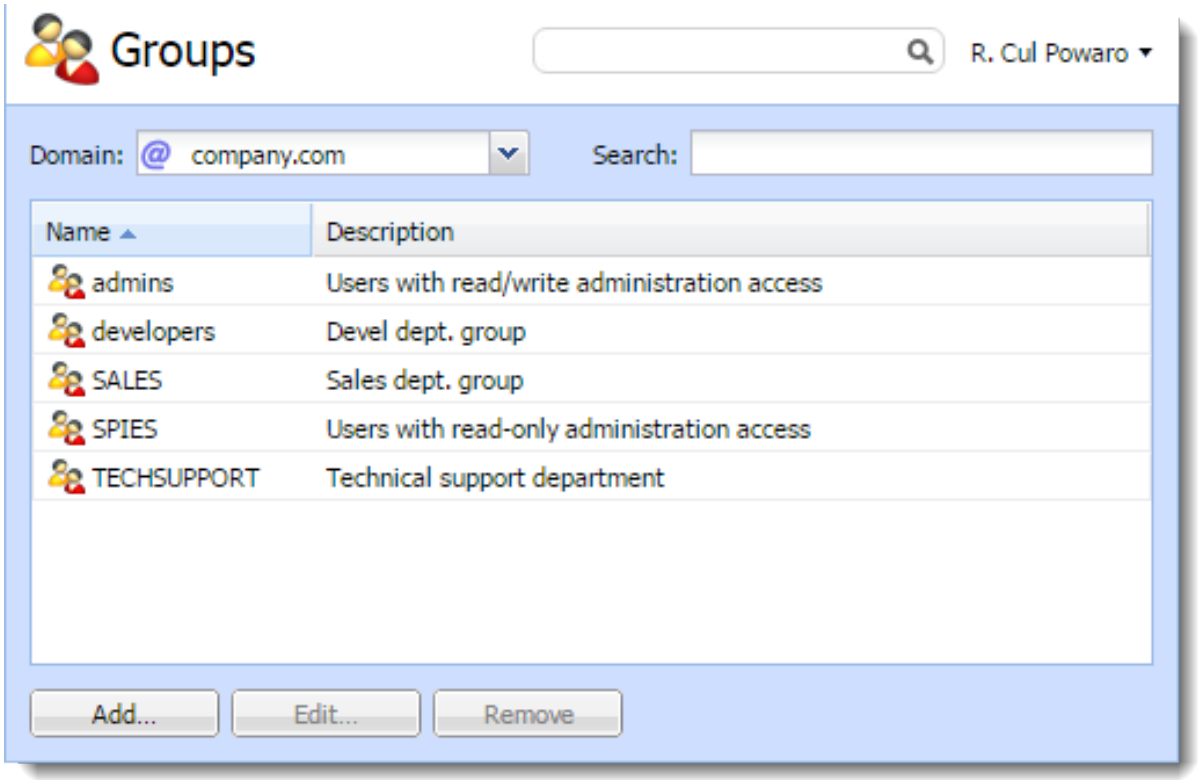
- Set access rights to Kerio Connect administration for multiple users
- Deliver a single message to multiple users via a single email address (see also mailing lists)

You can:

- Create local user groups
- Map user groups from a directory service

User groups belong to a domain. Each domain may include any number of local and mapped groups. The number of groups is **not** limited by your license.

You can manage user groups in the administration interface in section **Accounts** → **Groups**.

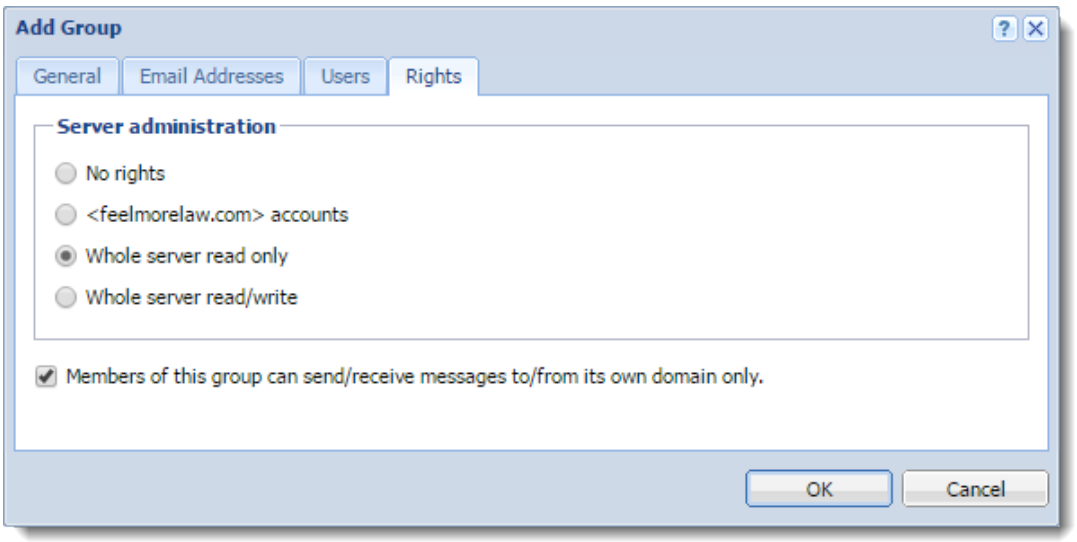


Creating user groups

1. Go to section **Accounts** → **Groups**.
2. Select a domain in which you want to create a group.
3. Click **Add**.
4. On the **General** tab, type a name for the group and description.
5. On the **Email Address** tab, add email addresses for the user group.

   You can add any number of email addresses. You can also use an existing username as the email address — any messages sent to the group email address will also be delivered to the original user.
6. On the **Users**tab, click **Add**.
7. Select the local users you want to add to the group and click **OK**.

   You can also go to **Accounts** → **Users** and select a group in user's settings.
8. On the **Rights** tab, set the access right to the administration interface (see Setting access rights in Kerio Connect for more details).



9. Click **OK**.

Mapping groups from a directory service

To add groups from a directory service, you must:

1. Connect Kerio Connect to a directory service (see the Connecting Kerio Connect to directory service article for more details)
2. Activate groups in the administration interface

To activate groups:

1. Go to section **Accounts** → **Groups**.
2. Select a domain in which you want to create a group.
3. Click **Add** → **Add From a Directory Service**.
4. Select groups you want to map to Kerio Connect.
5. Click **Next**.
6. Click **Finish**.

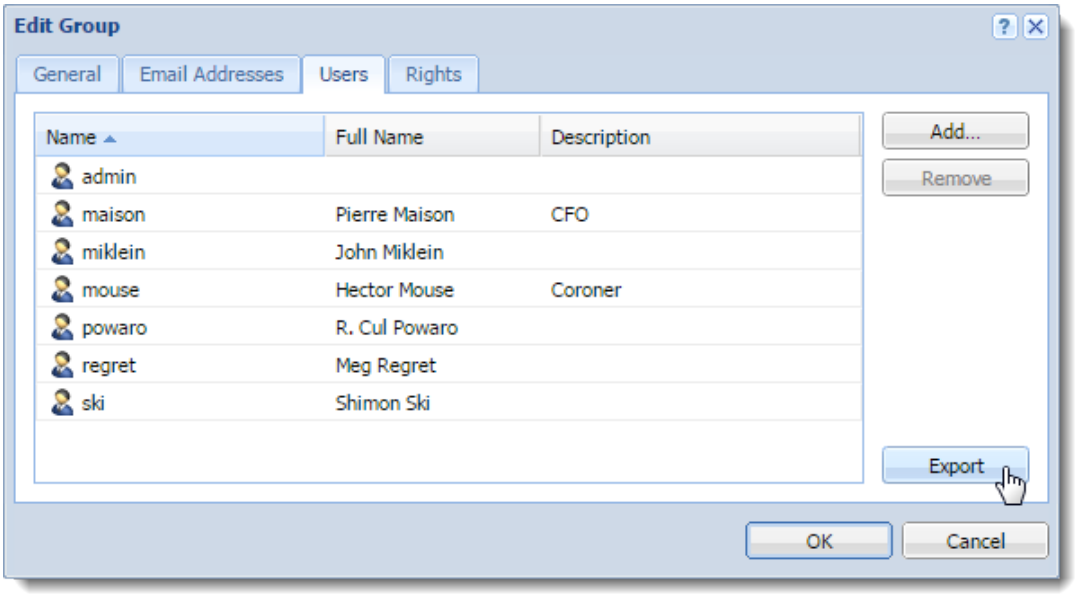
Exporting group members

To see the list of members in each group, you can export members of individual groups into a CSV file.

The data in the CSV file is organized as follows:

- Individual items are separated by semicolons
- Multiple information within individual items are separated by commas

1. In the administration interface, go to the **Accounts** → **Groups** section.
2. Double click a group.
3. On the **Users** tab, click **Export**.



Kerio Connect saves the CSV file to your hard drive.

The filename has the following format:

`users_<domain_name>_<group_name>_<date>.csv` (for example, `users_company.com_TECHSUPPORT_2015-09-09.csv`)

Use a spreadsheet or a text editor to open the file.

Setting access rights in Kerio Connect

What levels of access rights are available

Users/groups can have assigned the following levels of access rights:

- no rights
- domain read/write — can manage users, groups, aliases, mailing lists and resources in their own domain. It is recommended for large companies or Internet service providers.
- whole server read only
- whole server read/write

For access rights to public folders, read this article.
For access rights to archive folders, read this article.

How to set access rights

1. In the administration interface, go to section **Accounts** → **Users**.
2. Select a domain and double-click the user you wish to edit.
3. Go to tab **Rights** and select the desired level of access rights.
4. Confirm.

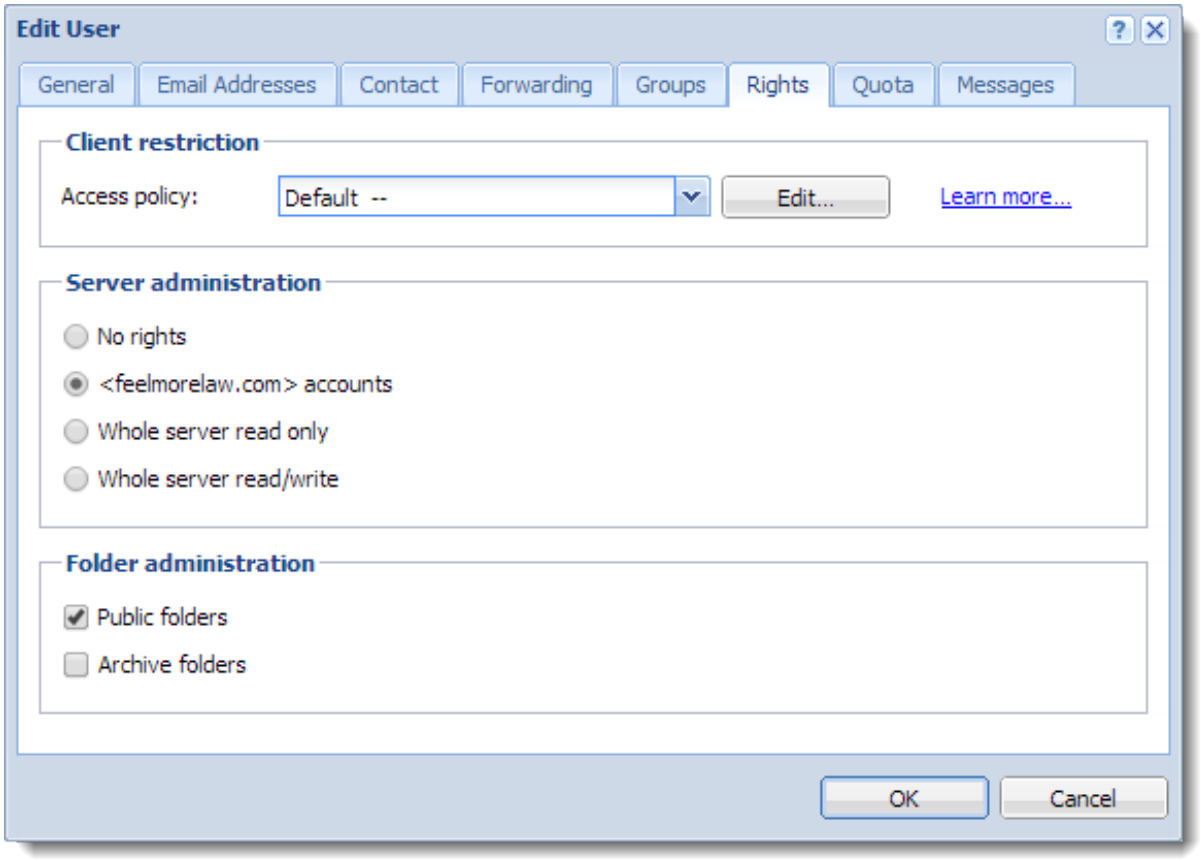


Figure 1 Access rights

Built-in administrator account

Kerio Connect allows you to enable a special administrator account. This account:

- has username `Admin`
- doesn't count into your license
- has whole server read/write rights
- doesn't have an email address and message store

To enable the built-in admin account:

1. Go to section **Configuration** → **Administration Settings**
2. Check option **Enable built-in administrator account**
3. Enter a password for this administrator.

If the built-in admin account is enabled and any of your standard users has username `Admin`, the standard user must include their domain in the login dialog.
If you wish to disable the built-in admin account, just unselect option **Enable built-in administrator account** in section **Configuration** → **Administration Settings**.
The same rules as for disabling other admin accounts apply.

Maintaining user accounts in Kerio Connect

How to maintain users accounts

In Kerio Connect, you can:

- delete old items in users' mailboxes
- recover deleted items
- limit the size of outgoing messages
- set quota for users' mailboxes

Configuring automatic items clean-out

In Kerio Connect you can set a special rule which will delete all messages older than a specified number of days (e.g. to save some space on your data store disk).

 If you do not wish to lose any messages with the clean-out, archive or backup your data store.

Automatic clean-out can be applied to the following folders:

- deleted items
- spam
- sent items
- all folders (except contacts and notes)

How to configure items clean-out

The automatic clean-out of items can be set for

- individual users
- per domain

If both are configured, settings per user are applied.

Per domain

1. Go to section **Configuration** → **Domains** and double-click the domain for which you wish to set the items clean-out.
2. On tab **Messages**, select folders for automatic clean-out and set the number of days.
3. Confirm.

Per user

By default, new users inherit settings from their domain. If you want to change settings for individual users, follow these steps:

1. Go to section **Accounts** → **Users**, double-click the user for whom you wish to set the items clean-out.
2. Go to tab **Messages** and in the **Items clean-out section** select option **Use custom settings for this user**.
3. Select folders for automatic clean-out and set the number of days.

How to recover deleted items

If anyone loses an important message which is accidentally moved to a folder which is cleaned up automatically, deleted messages can be simply recovered before the store with deleted items is completely cleared out.

The following items can be recovered — email messages, events, contacts, notes and tasks.

Enabling deleted items recovery

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click the domain and go to tab **Messages**.
3. Check option **Keep deleted items for** and specify number of days for which the items will be available after deletion.
4. Confirm.

Recovering deleted items

Once recovery is enabled for the user's domain, follow these steps to recover their items:

1. In the administration interface, go to section **Accounts** → **Users**.
2. Select the user and click on **More Actions** → **Recover Deleted Items**.
3. This will run the recovery process and you will see the result.

If any items are restored, user will find them in their **Deleted Items** folder.

If the **Recover deleted items** button is not active, deleted items recovery is not enabled for the particular domain. In such a case, the given deleted item can be looked up in the archive if archiving has been used.

How to limit size of outgoing messages

If you wish to avoid overloading your server with large email attachments, you can limit the size of outgoing messages per domain or per user.

If both are configured, settings per user are applied.

Per domain

1. Go to section **Configuration** → **Domains** and double-click the domain.
2. On tab **Messages**, check option **Limit outgoing message size to**.
3. Set the maximum size of a message for this domain.
4. Confirm.

Per user

By default, new users inherit settings from their domain. If you want to change settings for individual users, follow these steps:

1. Go to section **Accounts** → **Users** and double-click the user for whom you wish to limit the message size.
2. Go to tab **Messages** and in section **Maximum message size** set the limit for outgoing messages.

By selecting the appropriate option, you can also disable any limits on message size for individual users.

3. Confirm.

Messages sent from Kerio Connect Client

Each new message composed in Kerio Connect Client is sent to Kerio Connect via so-called HTTP POST request. Each request contains not only a message body, but also all headers and attachments. The limit set by this option narrows the size of any HTTP POST request directed from Kerio Connect Client. This means that any limit set for requests also limits the size of email messages.

1. In the administration interface, go to section **Configuration** → **Advanced Options** → **tab Kerio Connect Client**.
2. Specify the maximum size of outgoing messages.
3. Confirm.
4. Restart Kerio Connect.

How to limit size of incoming messages delivered via SMTP

You can set a limit to the size of messages delivered via SMTP:

1. In the administration interface, go to section **Configuration** → **SMT server** → **tab Security Options**.
2. Check option **Limit maximum incoming SMTP message size to** and specify the size.
3. Confirm the settings.

How to limit size of user mailboxes

Apart from limiting the size of messages, you can also set a limit to the size of users' mailbox and the number of items it contains.

1. Go to section **Accounts** → **Users** and double-click the user whom you wish to set limit to their mailbox size.
2. Go to tab **Quota**, select option you wish to limit and specify the **disk space** or **item count** for the user.
3. Confirm.

If a limit is reached, user

Notifying users about reaching their quotas

Users may be notified if the quota of their message store reaches a certain limit. Thus users may delete messages in their mailboxes.

To set the limit for notifying users:

1. In the administration interface, go to section **Configuration** → **Advanced Options** → **tab Store Directory**.
2. Set the **Warning limit** (in percent) the frequency in which users will be notified.
3. You can specify an email address to which a message will be send if a user reaches the quota.
4. Save the settings.

Creating mailing lists in Kerio Connect

About mailing lists

Mailing lists are group email addresses. Messages sent to these addresses are distributed to all members of the mailing list. Apart from the standard user groups, mailing lists allow:

- subscribing/unsubscribing of members by email messages
- mailing list moderating (moderators conduct users' subscription/unsubscription, participation and message posting)
- 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)

Special mailing list addresses

All actions (subscribing, moderating, etc.) are performed by sending email messages to a special address — `<mailing_list_name>-<suffix>@<domain>`

Users can send empty messages to those specific email addresses to performed desired actions.

The following **suffixes** are available:

- `subscribe` — to subscribe to a mailing list,
- `unsubscribe` — to unsubscribe from a mailing list,
- `help` — to receive help info for the mailing list,
- `owner`, `owners` — to send messages to the mailing list moderator (users do not have to know their email addresses).

Creating mailing lists

1. Go to section **Accounts** → **Mailing Lists** and select a domain in which you want to create a mailing list.
2. Click **Add**.

3. Enter a name for the mailing list.

   The mailing list name must not:

   - contain suffixes used for special functions
   - contain the . symbol (dot)
   - be identical to other username or alias

4. Select language for the automatic messages sent to users.

   
   You can create mailing lists in various languages on one server. Message templates for individual languages are kept in the `reports` subdirectory where Kerio Connect is installed. Files are in UTF-8. You can modify individual reports or add new language report versions.

5. Enter an automatic welcome message. Add text that will be appended to each message sent to the mailing list.

6. Decide on the mailing list policy — you can moderate it or leave it without your interference.

7. Add users on the **Members** tab or import them. You can also allow subscription via messages sent to a special email address.

8. Decide who can see the archive of the mailig list.

9. Save the settings.

Now users can subscribe and send message to mailing lsits.

Importing users to mailing lists

You can create a CSV file with users' email addresses and/or full names and import the file to a mailing list.

Separate individual items by commas (,) or semicolons (;).

The file may look as follows:

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

To import CSV files to a mailing list:

1. In section **Accounts** → **Mailing Lists**, double-click a mailing list and go to tab **Members**.
2. Click **Add** → **Import from a CSV file**.
3. Browse for the CSV file and confirm.

The users are now displayed on tab **Members**.

Accessing the mailing list archive

Mailing list archive is a special folder accessible via the NNTP service.

You can enable archiving in the mailing list settings on tab **Archiving**.

If you wish the archive to be accessible publicly (to anybody), you must allow anonymous access to the NNTP service:

1. Go to section **Configuration** → **Services**.
2. Double-click **NNTP** and on the **Access** tab check option **Allow anonymous access**.
3. Save the settings.

Troubleshooting

If any problem regarding mailing lists occurs, consult the Debug log (right-click the Debug log area and enable **Mailing List Processing** in **Messages**).

Importing users in Kerio Connect

Import options

In Kerio Connect you can import users from:

- CSV files
- Directory service

Importing creates local user accounts.

 Read Creating mailing lists in Kerio Connect for detailed information on importing users to mailing lists.

Importing from CSV files

Creating CSV files

You can import users from a CSV file. Headings of the columns in the file must correspond with the Kerio Connect categories.

Individual fields can be separated in either of two ways:

- With semicolons (;) — separate multiple entries in a field with commas (,).

  ```
  Name;Password;FullName;Description;MailAddress;Groups
  abird;VbD66op1;Alexandra Bird;Development;abird;read,all
  abird;Ahdpppu4;Edward Wood;Sales;ewood,wood;sales,all
  mtaylor;SpoiuS158;Michael Taylor;Assistant;mtaylor,michael.taylor;all
  ```

- With commas (,) — enclose multiple entries in quotations marks (" ") and separate them with (,).

  ```
  Name;Password;FullName;Description;MailAddress;Groups
  abird,VbD66op1,Alexandra Bird,Development,abird,"read,all"
  ewood,Ahdpppu4,Edward Wood,Sales,"awood,wood","sales,all"
  mtaylor,SpoiuS158,Michael Taylor,Assistant,"mtaylor,michael.taylor",all
  ```

There is no rule about the order of the columns. Only `Name` (username) is mandatory.

Importing from CSV files

To import the file:

1. Go to **Accounts** → **Users** and select a domain to which you want to import users.
2. Click **Import and Export** → **Import from a CSV File**.
3. Select the CSV file and confirm.

   This displays a list of users from the CSV file.
4. Select the users you want to import (you can even use a template) and confirm.

Importing from a directory service

Windows NT domain

If you want to import users from a Window NT domain, the computer with Kerio Connect must be installed on Microsoft Windows and must belong to this domain.

1. Go to **Accounts** → **Users** and select a domain to which you want to import users.
2. Click **Import and Export** → **Import from a Directory Service**.
3. Type the name of the Windows NT domain and confirm.

   During the import, sensitive data is transmitted (such as user passwords) — Secure the communication using SSL encryption.

   This displays a list of users.
4. Select the users you want to import (you can use a template), and confirm.

Microsoft Active Directory

1. Go to **Accounts** → **Users** and select a domain to which you want to import users.
2. Click **Import and Export** → **Import from a Directory Service**.

3. Type the name of the Microsoft Active Directory domain, the name of the server with Active Directory, and the username and password of an Active Directory user who has at least read rights. Then confirm.

    During the import, sensitive data is transmitted (such as user passwords) — Secure the communication using SSL encryption.

   This displays a list of users.

4. Select the users you want to import (you can use a template), and confirm.

Novell eDirectory

1. Go to **Accounts** → **Users** and select a domain to which you want to import users.
2. Click **Import and Export** → **Import from a Directory Service**.
3. Type the name of the organization users will be imported from, the name or IP address of the server on which the service for this domain is running, and the username and password of a user in this domain who has at least read rights. Then confirm.

    During the import, sensitive data is transmitted (such as user passwords) — Secure the communication using SSL encryption.

   This displays a list of users.

4. Select the users you want to import (you can use a template), and confirm.

Troubleshooting

To log information about the import, enable the **Directory Service Lookup** option in the Debug log before the import.

Exporting users in Kerio Connect

What can be exported

In Kerio Connect, administrators with at least read rights can export lists of

- Users from a domain
- Members of a group
- Members of a mailing list

Kerio Connect exports users to a CSV file. Individual fields in the file are separated with semicolons (;). Multiple entries in a field are separated with commas (,).

Exporting users from a domain

1. In the administration interface, go to **Accounts** → **Users**.
2. Select the domain you want export from.
3. Click **Import and Export** → **Export to a CSV file**.
4. Save the file.

The file names use this format: `users_<DomainName>_<date>.csv`

Exporting users from a group

1. In the administration interface, go to **Accounts** → **Groups**.
2. Select the domain you want to export from, and double-click a group.
3. On the **Users** tab, click **Export**.
4. Save the file.

The file names use this format: `users_<DomainName>_<GroupName>_<date>.csv`

Exporting users from a mailing list

1. In the administration interface, go to **Accounts** → **Mailing Lists**.
2. Select the domain you want to export from, and double-click a mailing list.
3. On the **Members** tab, click **Export**.
4. Save the file.

The file names use this format: `users_<DomainName>_<MailingListName>_<date>.csv`

Creating aliases in Kerio Connect

Aliases in Kerio Connect

In Kerio Connect, aliases create **virtual (alternative)**:

- domain names (the part after @ changes)
- user names (the part before @ changes)

You can combine both types of aliases:

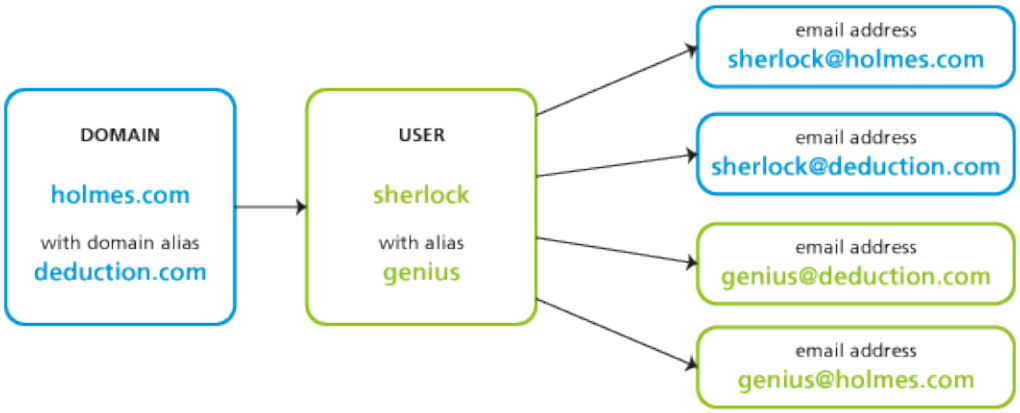


Figure 1 Map of aliases for a single user account

Domain aliases

Each domain can have any number of alternative names — aliases.

You can use domain aliases for email delivery. Users **cannot** use them to:

- login to the Kerio Connect administration interface
- login to Kerio Connect Client
- view the **Free/Busy** server

Each user in a domain with domain aliases has an according number of email addresses (within a single mailbox):

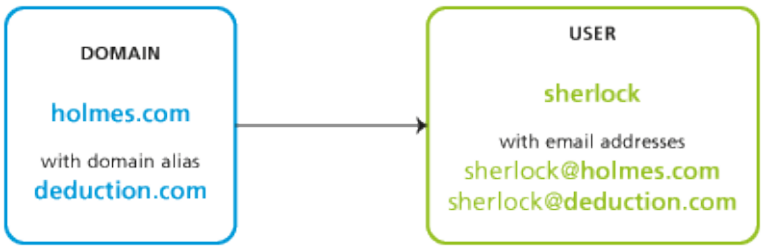


Figure 2 Domain aliases

Once you rename a domain, an alias is automatically created from the original name.

Creating domain aliases

To create a domain alias in Kerio Connect:

1. In the administration interface, go to **Configuration** → **Domains**.
2. Double-click a domain and go to the **Aliases** tab.
3. Click on **Add** and type an alias.
4. Confirm and save.

To make the alias exist in the Internet, create a corresponding MX record in DNS for each alias.

Username aliases

Each account or group can be associated with any number of aliases (i.e. different names).

Aliases can be linked to:

- a user
- a group
- an existing alias

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.

Each user with, for example, *four* aliases has *four* email addresses (within a single mailbox):

If users have username aliases defined, they can select from which addresses they want to sent their messages.

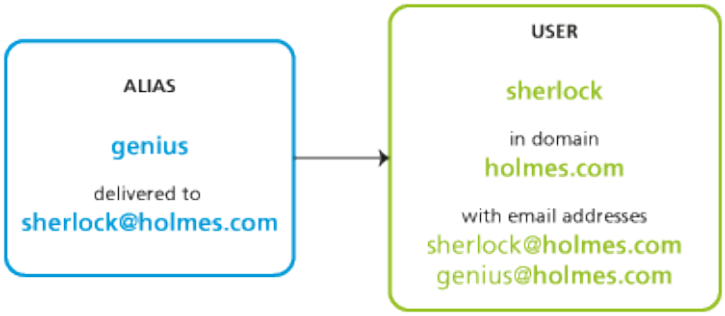


Figure 3 Username aliases

Creating username aliases

To create an email alias in Kerio Connect, follow these steps:

1. In the administration interface, go to **Accounts** → **Aliases**.
2. Select a domain for the alias and click **Add**.
3. Type the name of the alias.

   The alias may contain the following characters:

   - `a-z` — all lower-case letters (no special characters)
   - `A-Z`— all upper-case letters (no special characters)
   - `0-9` — all numbers
   - `.` — dot
   - `-` — dash
   - `_` — underscore
   - `?` — question mark
   - `*` — asterisk
4. The messages can be delivered to:

   - an email address — type the email address or click **Select**
   - public folder — select the public folder form the menu

This item is active only in case at least one email public folder.

5. Confirm and save.

Example:
Mr Sherlock Holmes has an account with username **sherlock** in domain **holmes.com** (therefore, his email address is `sherlock@holmes.com`).
Since he finds himself very smart (what else), he wants another email address — **genius@holmes.com**. The problem is he does not want to manage two accounts.
He orders Dr Watson to create an alias in section **Accounts** → **Aliases**. The alias is **genius** and is delivered to email address **sherlock@holmes.com**.
From now on, all messages sent to **genius@homes.com** will be delivered to **sherlock@holmes.com**

In user's settings on tab **Email Addresses**, you can also specify aliases for individual users:

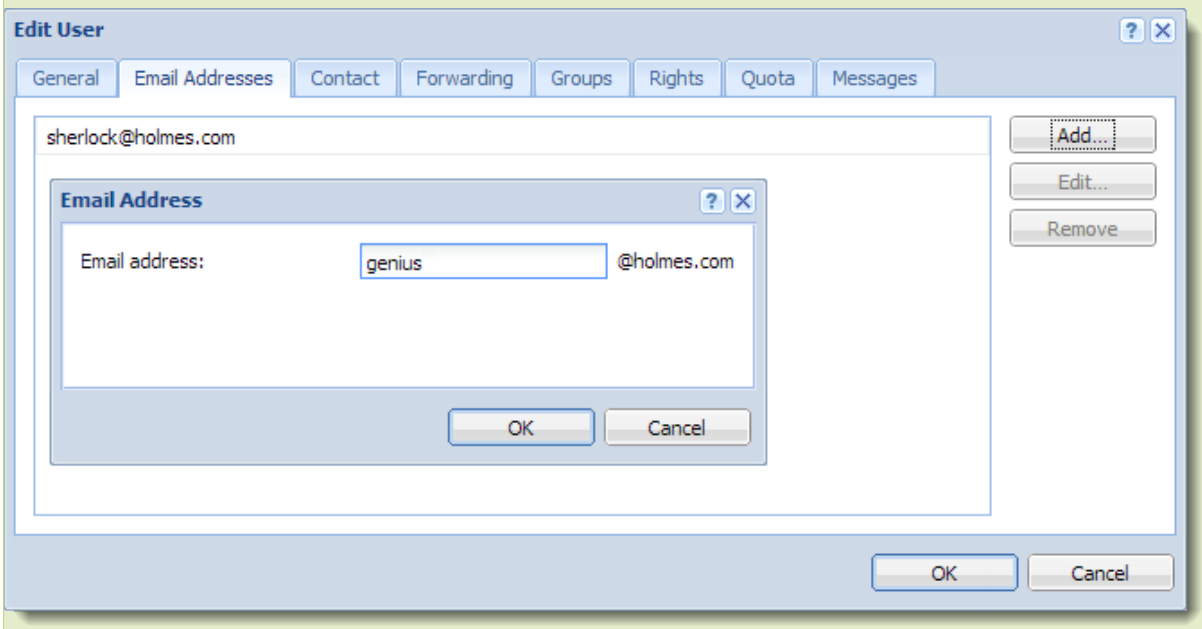


Figure 4 Domain aliases

The same goes for groups — specify aliases on tab **Email Addresses** in the group's settings.

Special scenarios

Alias for messages to be stored in a public folder

Mr Holmes wants messages sent to `info@holmes.com` to be store in the *Info* public folder. The alias is:
`Info` → `#public/Info`

Alias for messages sent to invalid addresses to be delivered to a specific user

Mr Holmes does not want to be troubled with people who cannot write correct addresses. Therefore, he has created an alias for such messages to be sent to Dr Watson so that he does not need to deal with them. This is done by this alias:
`*` → will be sent to `watson`

If this alias is not defined, Kerio Connect returns such messages to their senders as undeliverable.

Alias as a protection against wrong spelling — one character

Mr Sherlock Holmes wishes to filter messages which may contain interesting cases. These are messages sent to addresses like `kill@holmes.com` (potential murder cases) or `will@holmes.com` (interesting inheritance cases). To avoid creating many aliases, Mr Holmes creates only the following one which will cover both addresses:
`?ill` → will be sent to `sherlock`

Alias as a protection against wrong spelling — numerous characters

Some languages have different spellings for one sound. Thus, Mr Holmes's first name can be written, for example, as `sherlock`, `scherlock`, `serlock` etc. The following alias will cover all these cases:
`*erlock` → will be sent to `sherlock`

Checking aliases

In Kerio Connect you can verify all the aliases.

1. In the administration interface, go to section **Accounts** → **Aliases**.
2. Click the **Check Address** button (bottom right corner).
3. Enter any email address — real, misspelled, virtual, alias, made-up, etc.
4. Click **Check**.

The **Result** table displays the target addresses to which messages sent to the entered address will be delivered.

Configuring resources in Kerio Connect

Overview

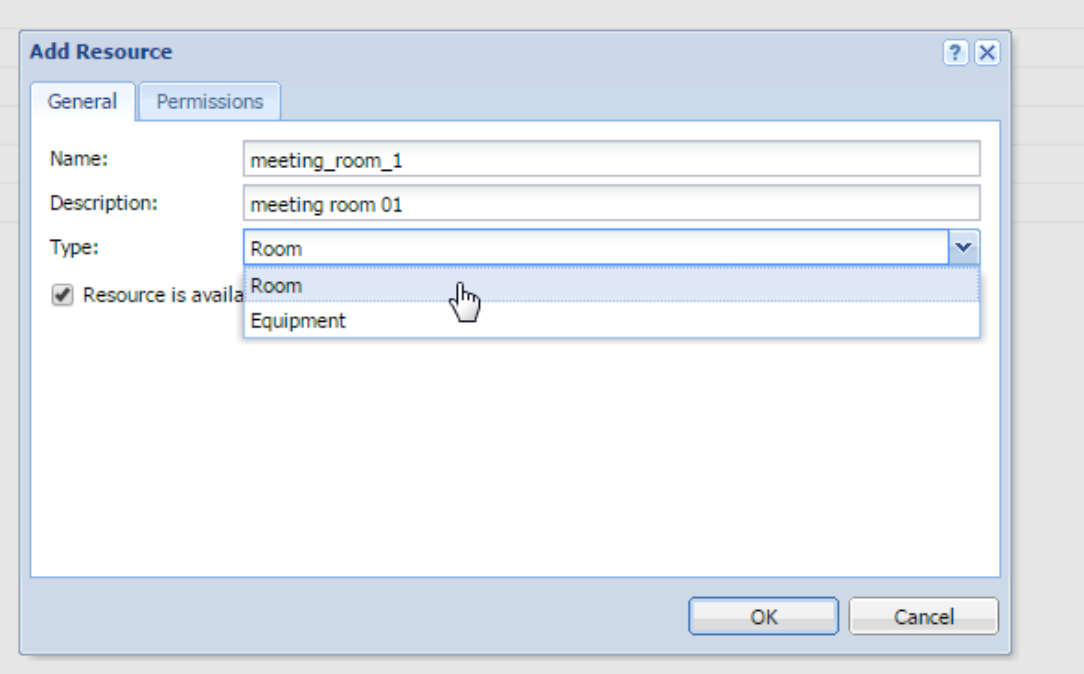
Resources are meeting rooms and other facilities, such as conference rooms, cars, parking lots.

In email clients, you can schedule resources when creating new events in calendars.

Resources do not count into your license.

Creating new resources

1. In the administration interface, go to **Accounts** → **Resources** and select the domain to which you want to add resources.
2. Click **Add**.
3. Type a name for the resource and select the resource type.



4. Select the **Resource is available** option.
5. By default, permissions to use resources are set to all users from the domain.

   You can add or remove any user or group on the **Permissions** tab.
6. On the **Permissions** tab, select a reservation manager.

   By default, the domain administrator is the resource manager.
7. Click **OK**.

Kerio Connect publishes all resources to a public calendar.

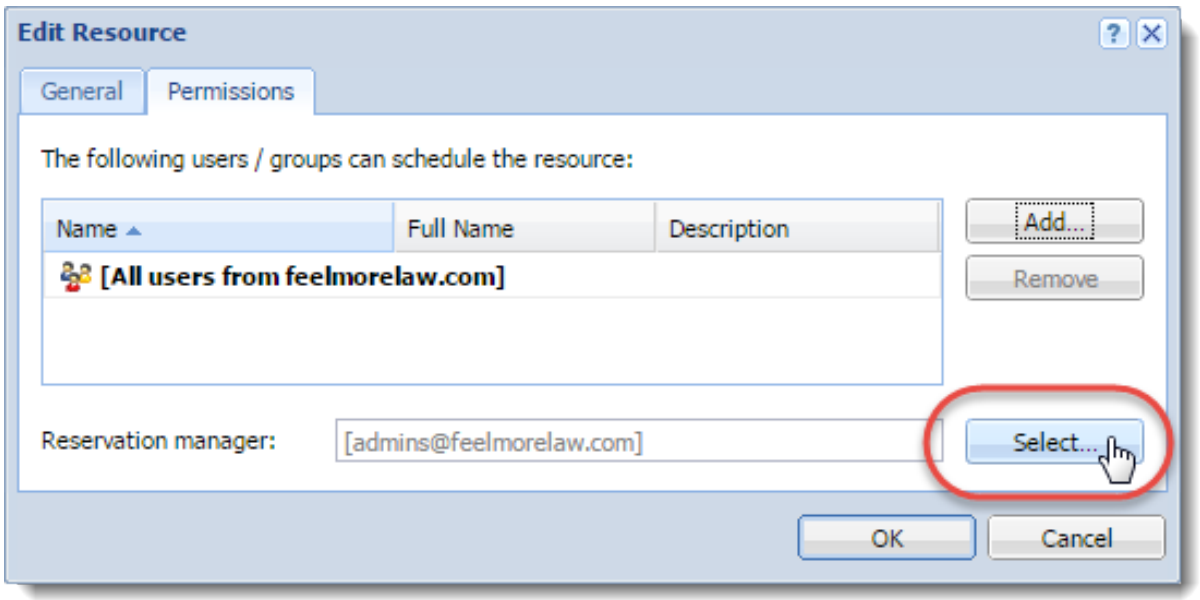
Assigning reservation managers

Each resource has a reservation manager. Reservation managers are users who manage the resource calendar. In Kerio Connect Client, they can delete other users' reservations for the resource.

1. In the administration interface, go to **Accounts** → **Resources**.
2. Double-click a resource and switch to the **Permissions** tab.
3. Click **Select** in the **Reservation manager** section.

   Kerio Connect displays a list of all users and groups.
4. Switch to the desired domain and select a user as the resource manager.

   To select multiple users as resource managers, select a group of users.
5. Click **OK**.



Removing resources

You can remove resources:

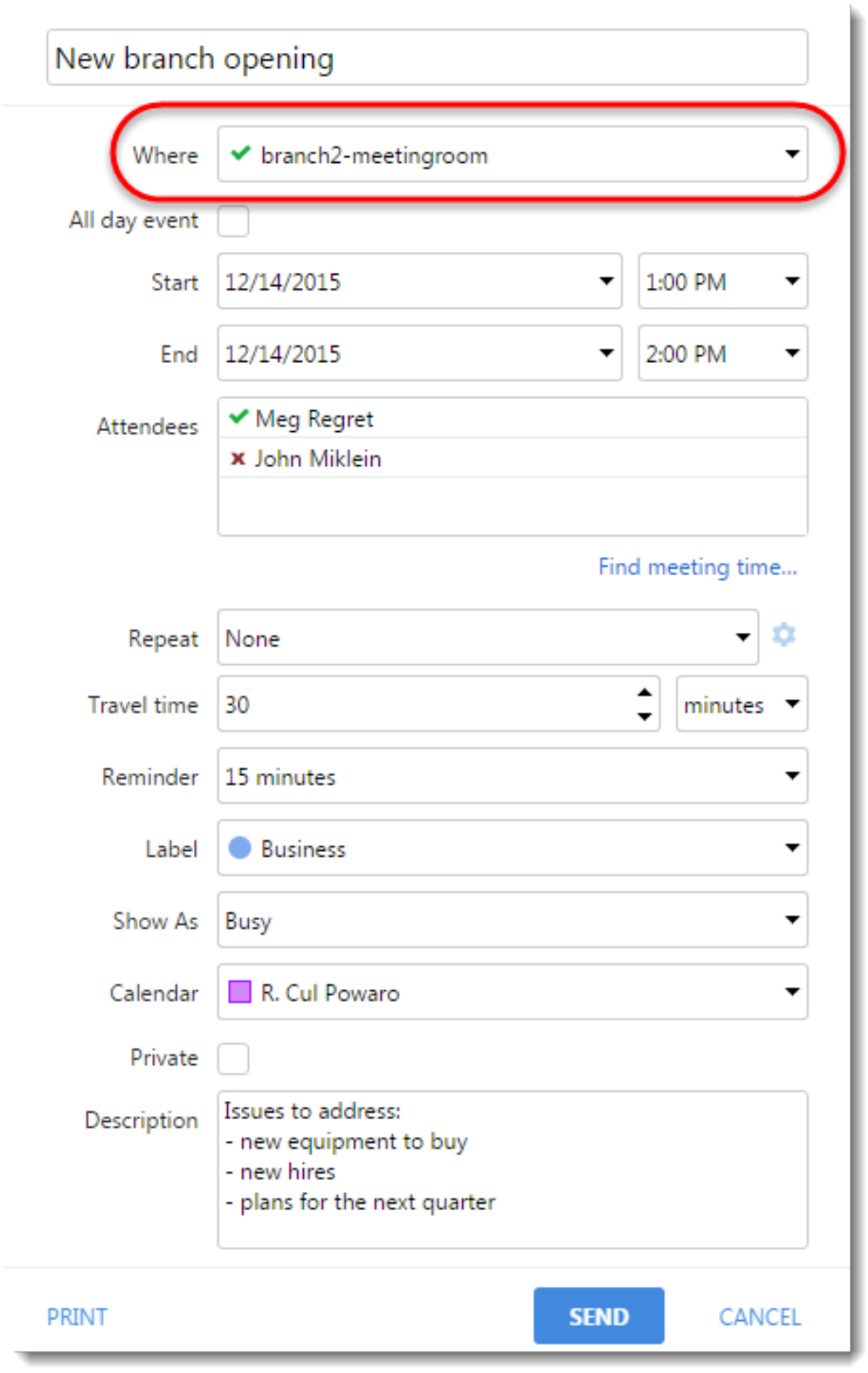
- **Temporarily** — Double-click the resource in the **Accounts** → **Resources** section, and unselect the **Resource is available** option.
- **Permanently** — Select the resources in the **Accounts** → **Resources** section, and click **Remove**.

Scheduling resources in Kerio Connect Client

To schedule a resource:

1. Open your calendar.
2. Click **New Event**.
3. Configure the event.
4. In the **Where** section, select the resource you want to reserve.
5. Save the event.

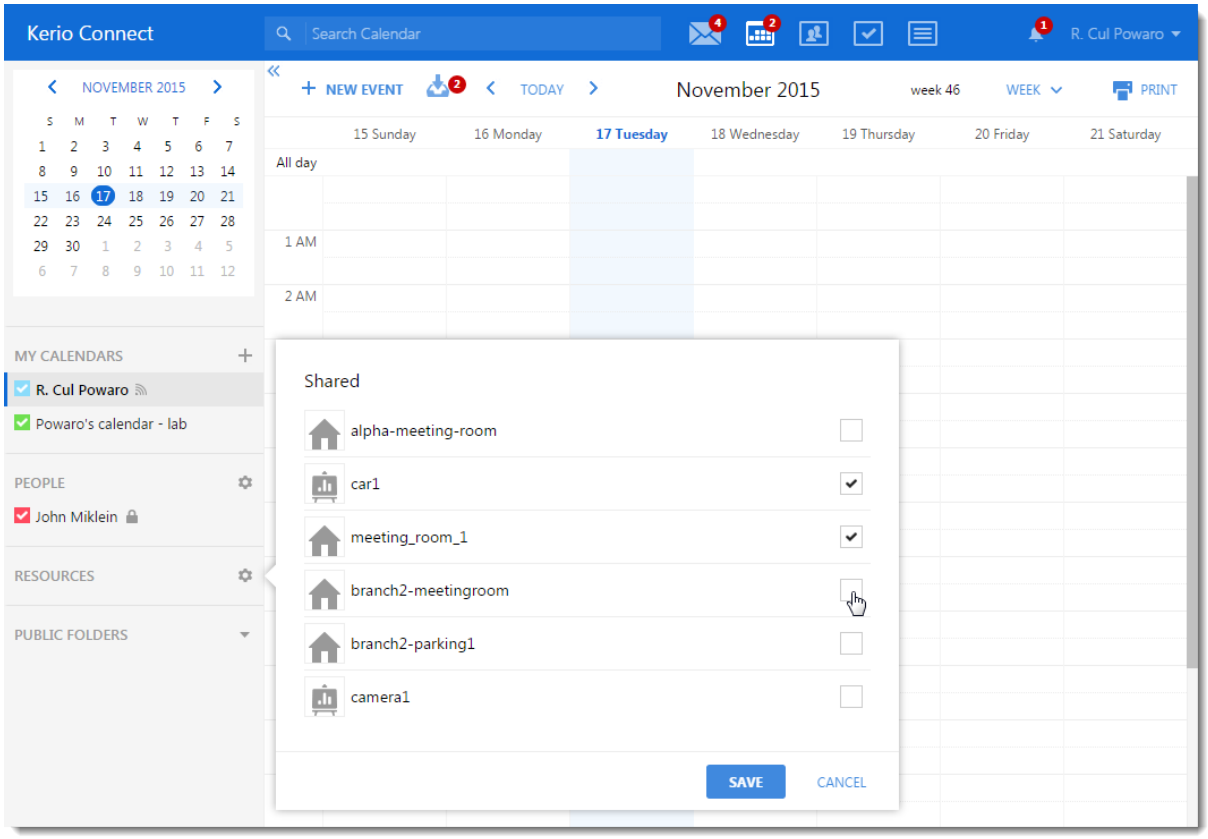
Other mail clients have similar procedures.


New branch opening
Where
branch2-meetingroom
All day event
Start
12/14/2015
1:00 PM
End
12/14/2015
2:00 PM
Attendees
Meg Regret
John Miklein
Find meeting time...
Repeat
None
Travel time
30
minutes
Reminder
15 minutes
Label
Business
Show As
Busy
Calendar
R. Cul Powaro
Private
Description
Issues to address:
- new equipment to buy
- new hires
- plans for the next quarter
PRINT
SEND
CANCEL

Displaying resource calendars in Kerio Connect Client

All users who can schedule resources can display the resource calendars. This can help you when you are planning a meeting

1. Log in to your Kerio Connect Client and switch to **Calendars**.
2. Click the gear icon next to **Resources** on the left.
3. Select the resource calendar you want to display



Troubleshooting

If any problem regarding resources occur, consult the Debug log (right-click the Debug log area and enable **Resource Service**).

Monitoring Kerio Connect

Monitoring overview

In Kerio Connect, administrators can:

- monitor incoming and outgoing messages
- view connections to services, number of messages
- view statistics (including antivirus and spam filter)
- view who's connected
- monitor the CPU and RAM usage

Monitoring incoming and outgoing messages

An administrator can view all activities in Kerio Connect in great detail. The following information can be monitored:

- status of all sent and received messages
- connections to Kerio Connect interfaces

Viewing message status

All messages that are being sent or received through Kerio Connect are stored in Kerio Connect installation directory in folder `store/queue` as the following file types:

- `*.eml` — message itself
- `*.env` — SMTP envelope of the message

These messages are also displayed in section **Status** → **Message Queue** → **tab Messages in Queue**.

In this section you can:

- check whether messages are sent/received properly
- remove messages from the queue
- immediately send messages waiting in the queue

The **Queue ID** displayed in **Status** → **Message Queue** → **tab Messages in Queue** equals the filename in `store/queue`.

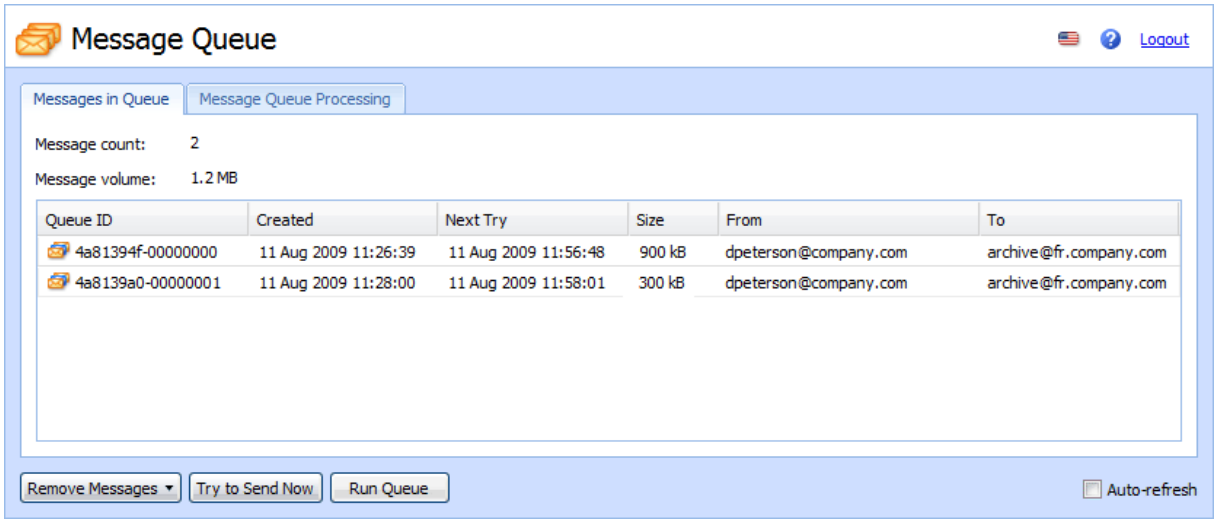


Figure 1 Viewing message queue

Processing message queue

When processing the message queue, Kerio Connect 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.

Section **Status** → **Message Queue** → **tab Messages Processing** displays information about the current statuses of messages currently processed.

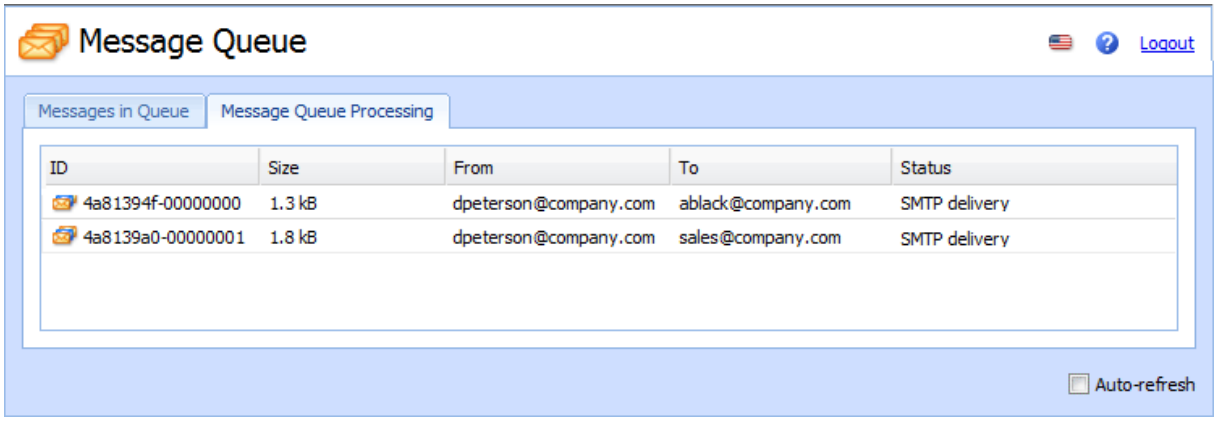


Figure 2 Processing message queue

Configuring message queue parameters

In the administration interface in section **Configuration** → **SMTP Server** → **tab Queue Options**, you can specify:

- limit the maximum number of messages being delivered at a time
- interval in which Kerio Connect will retry to deliver messages

- interval in which the undelivered message will be sent to sender
- interval in which the sender will be notified that their message has not been delivered yet and language for the notification

These settings do not apply if you use a relay SMTP server.

Traffic charts

In the **Status** →**Traffic Charts** section of the Kerio Connect administration interface you can view (in graphical format) the number of connections to individual services of Kerio Connect and the number of processed messages (both incoming and outgoing) for a given period.

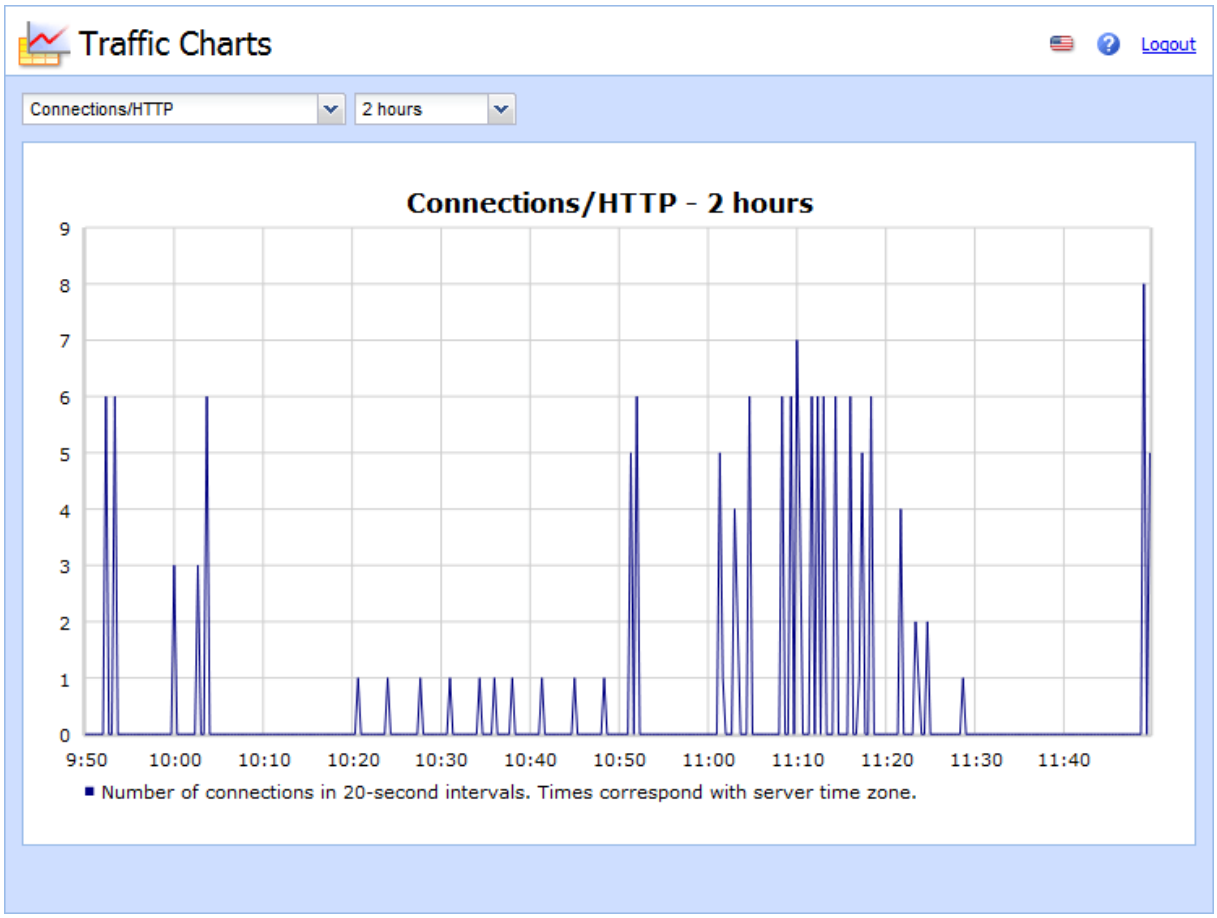


Figure 3 Traffic charts

Viewing 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.

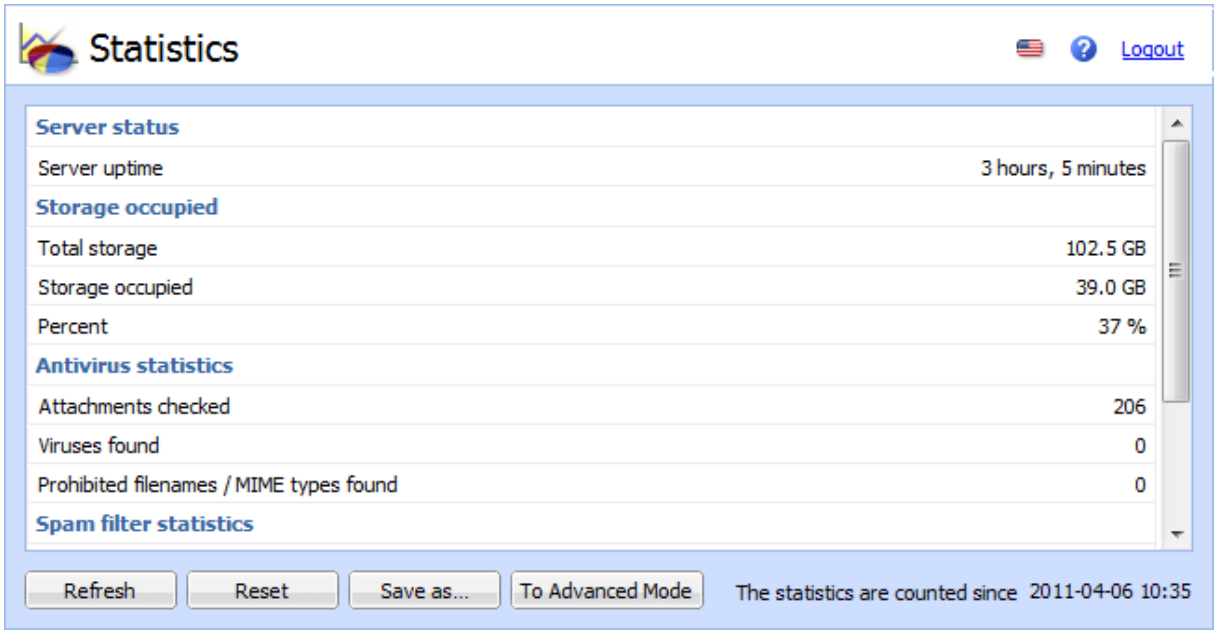


Figure 4 Kerio Connect statistics

Displaying users currently connected to Kerio Connect

To display all network connections established with Kerio Connect, including all its services (SMTP, POP3, etc.) and the administration interface, go to section **Status** → **Active Connections**.

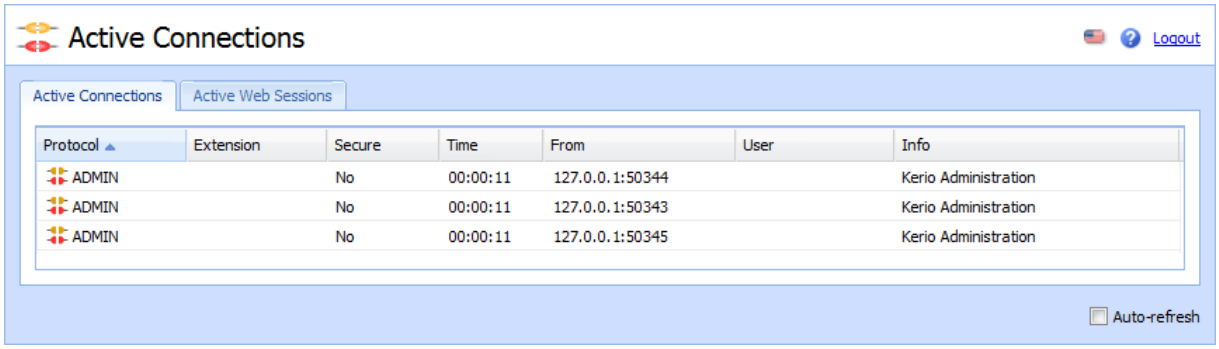


Figure 5 Active connections

To display connections established to Kerio Connect's web interfaces and session expiry times, go to section **Status** → **Active Connections**.

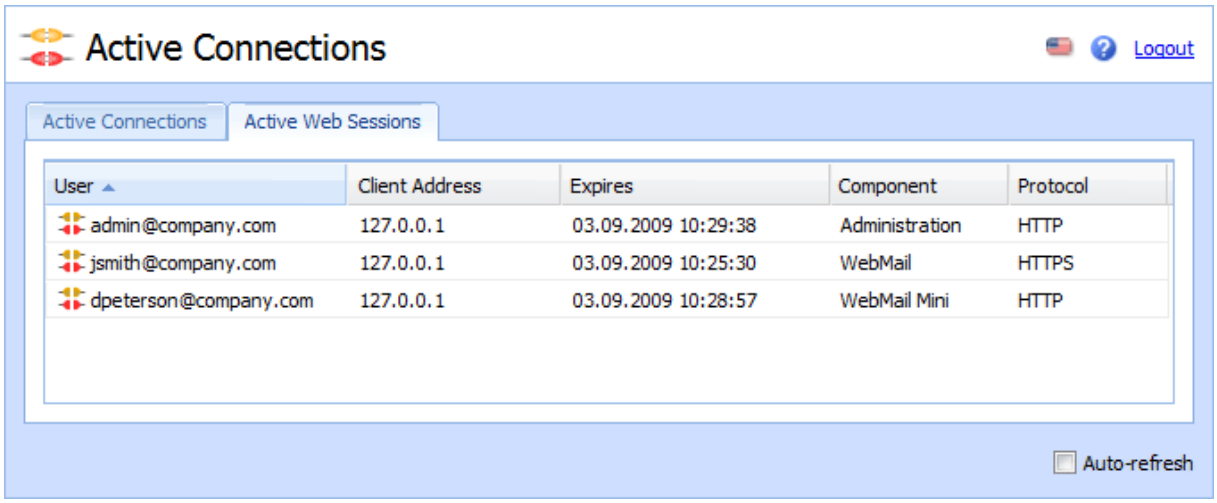


Figure 6 Active connections

Kerio Connect also allows to view which email folders are being used by the users.

To display currently opened folders, go to section **Status** → **Opened Folders**.

Monitoring CPU and RAM usage

System → **System Health** shows the current usage of CPU, RAM and the disk space of the computer or device where Kerio Connect is running.

Time interval
: Selection of time period for which CPU load and RAM usage is displayed.

CPU
: Timeline of the computer's CPU load. Short time peak load rates ("peaks" of the chart) are not unusual and can be caused for example by the network activity.

RAM
: RAM usage timeline.

Storage usage
: Currently used and free space on the disk or a memory card.

Tasks
: Restart of Kerio Connect.
Lack of system resources may seriously affect functionality of Kerio Connect. If these resources are permanently overloaded, restart Kerio Connect and then check system resources usage again.

Services in Kerio Connect

Setting service parameters

Go to section **Configuration** → **Services** to set parameters for services in Kerio Connect.

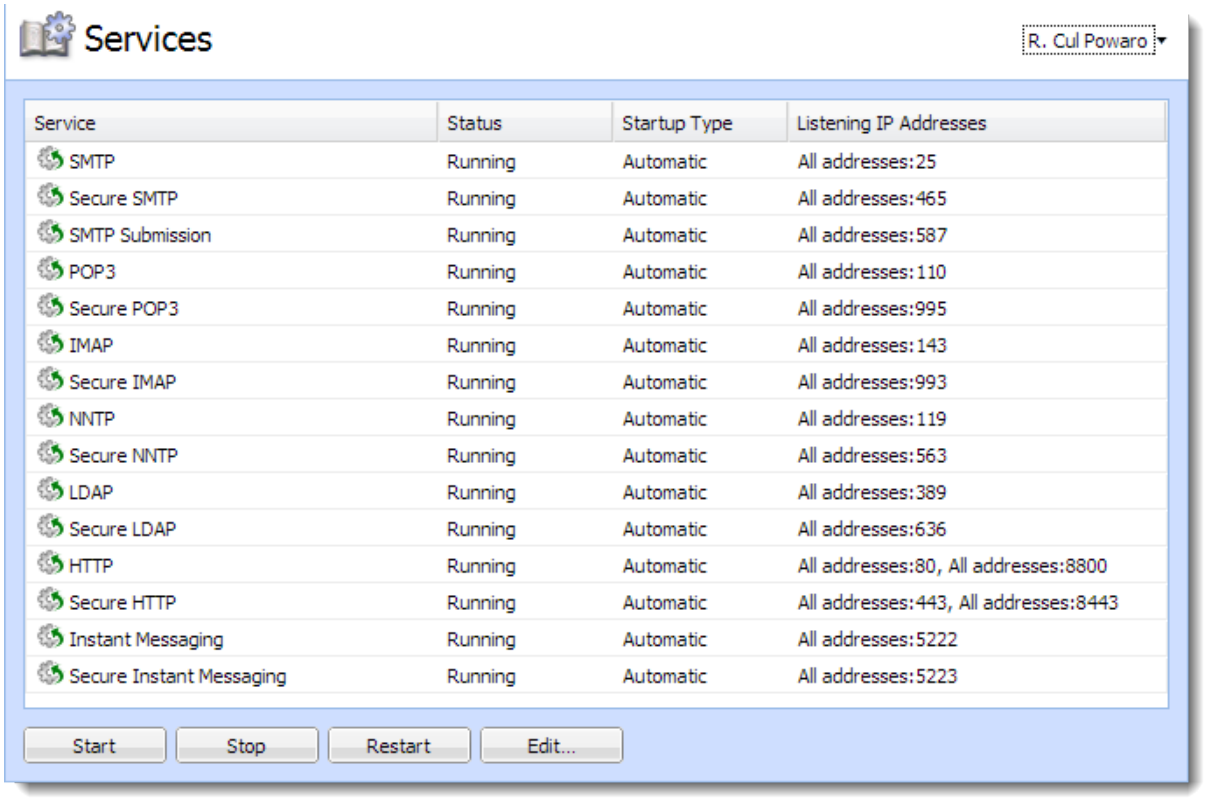
By default, all services are running on their standard ports.

 For security reasons, enable only the services you know will be used. See Configuring your firewall for additional information.

For each service, you can:

- Specify whether the service runs automatically on Kerio Connect startup
- Add or remove listening IP addresses and ports
- Limit access to the service for specific IP addresses
- Specify the maximum number of concurrent connections

  Consider the number of server users — For an unlimited number of connections set the value to 0



Port collisions

If any services available in Kerio Connect are already running on the server, you have two possibilities:

- Change the traffic port for one of the services
- Reserve a different IP address for each instance of the service on the same port (not recommended if you reserve IP addresses dynamically, for example, via DHCP)

What services are available

Each service is available in both unsecured and secured version (encrypted by SSL). The following sections describe individual services.

SMTP

The SMTP protocol server is used for sending outgoing email messages, for receiving incoming messages and messages created via mailing lists in Kerio Connect.

Two methods can be used for encryption of SMTP traffic:

- **SMTP on port 25** with STARTTLS, if TLS encryption is supported — traffic on port 25 starts as unencrypted. If both sides support TLS, TLS is started via STARTTLS.
- **SMTP on port 465** with SSL/TLS — the traffic is encrypted from the start.

 Since public WiFi networks often do not support traffic on unencrypted protocols, SMTP on port 25 can be blocked. In such cases users cannot sent email out of the network. SMTPS on port 465 is usually allowed.

SMTP Submission is a special type of communication which enables messages sent by an authenticated user to be delivered immediately without antispam control. Allow SMTP Submission if you use a distributed domain.

POP3

POP3 protocol server allows users to retrieve messages from their accounts.

IMAP

IMAP protocol server allows users to access their messages. With this protocol, messages stay in folders and can be accessed from multiple locations at any time.

NNTP

NNTP is a transfer protocol for discussion groups over the Internet. The service allows users to use messages of the news type and use the protocol to view public folders. Public folders cannot be viewed via NNTP if their name includes a blank space or the . (dot) symbol.

LDAP

LDAP server enables users to access centrally managed contacts. It provides read-only access — users are not allowed to create new nor edit the existing ones.

If Kerio Connect is installed on a server which is used as a domain controller (in Active Directory), it is necessary to run this service on non-standard ports or to disable them.

HTTP

HTTP protocol is used to:

- access user mailboxes in Kerio Connect Client
- access the Free/Busy server
- automatically update Kerio Outlook Connector (Offline Edition)
- synchronize via ActiveSync or NotifyLink (BlackBerry)
- publish calendars in iCal format

- (HTTPS) access Kerio Connect administration
- (HTTPS) access Kerio Connect Client (if set)

Instant Messaging

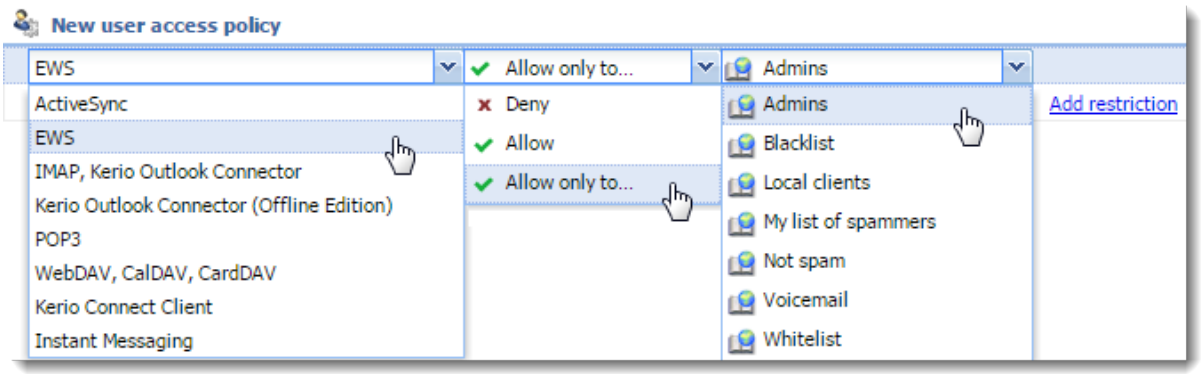
Instant messaging allows users to chat with other users in or outside of their domain.

Restricting access to some services

If you need to restrict access to any service for any users, you can define so-called **User Access Policies**. This means that you can allow or deny access to individual protocols from certain IP addresses to individual users.

Defining access policies

1. In the administration interface, go to section **Configuration** → **Definitions** → **User Access Policies**.
2. Click on **Add Policy** and enter a name for the policy.
3. Click on the **Add restriction** link and select a protocol.
4. Decide whether to allow it, allow it for certain IP addresses or deny it.
5. Add as many restrictions as you wish.
6. The group of the remaining (unselected) protocols can be also set in the same way.
7. To remove a restriction or policy, select it and click on **Remove**.
8. Save the settings.



Assigning access policies to users

Every new user is assigned the **Default** policy. To assign a different one:

1. In the administration interface, go to section **Accounts** → **Users**.
2. Double-click the user and go to tab **Rights**.
3. Select a **User policy** from the drop-down menu.
4. Save the settings.

Troubleshooting

If any problem regarding services occurs, consult the Debug log — right-click the Debug log area and check the appropriate message type (service to be logged).

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

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

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

LDAP
: When problems with the 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 *Microsoft Entourage* or *Apple Mail* where problems with Exchange accounts arise.
  - **PHP Engine Messages** — enables a log which may be helpful when solving problems with the Kerio Connect Client interface.

Instant messaging
: When problems with the IM server arise, a log that can be enabled by **Messages** → **Instant Messaging Server** might help.

Once your problems are solved, it is recommended that logging is disabled.

Configuring the SMTP server

Overview

The SMTP server defines who can send outgoing messages via your Kerio Connect and what actions they can perform.

If an unprotected SMTP server is accessible from the Internet, anyone can connect and send email messages through Kerio Connect. Spammers can use your SMTP server to send out spam messages and your company may be added to spam blacklists.

 Kerio Connect does not check messages from the allowed IP addresses with SPF, Caller ID and SpamAssassin.

Configuring the SMTP server

To specify who can send messages outside your server:

1. In the administration interface, go to the **Configuration** → **SMTP Server** → **Relay Control** section.
2. Select the **Allow relay only for** option.
3. To specify a group of IP addresses from which users can send outgoing messages, select the **Users from IP address group** option and the IP address group from the drop-down list..
4. To always require authentication when sending outgoing messages, select the **Users authenticated through SMTP for outgoing mail** option.

   When you enable this option, users from the allowed IP address group must also authenticate.

    If you select both the **Users from IP address group** and **Users authenticated through SMTP** options, and the SMTP authentication fails, Kerio Connect does not verify if the user belongs to the allowed IP address and users cannot send outgoing messages.

5. To allow sending outgoing messages for users who have previously authenticated through POP3 from the same IP address, select the **Users previously authenticated through POP3 ....** option and specify the time allowed for the SMTP relay.

6. Click **Apply**.

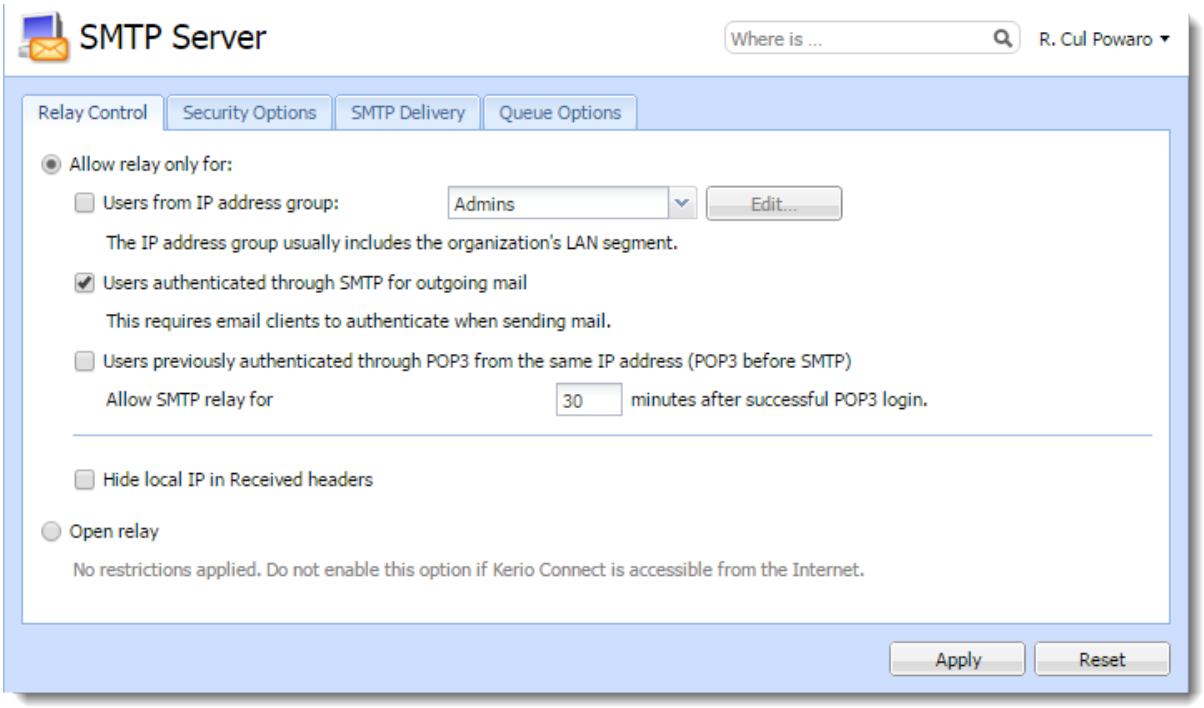


Figure 1 SMTP server

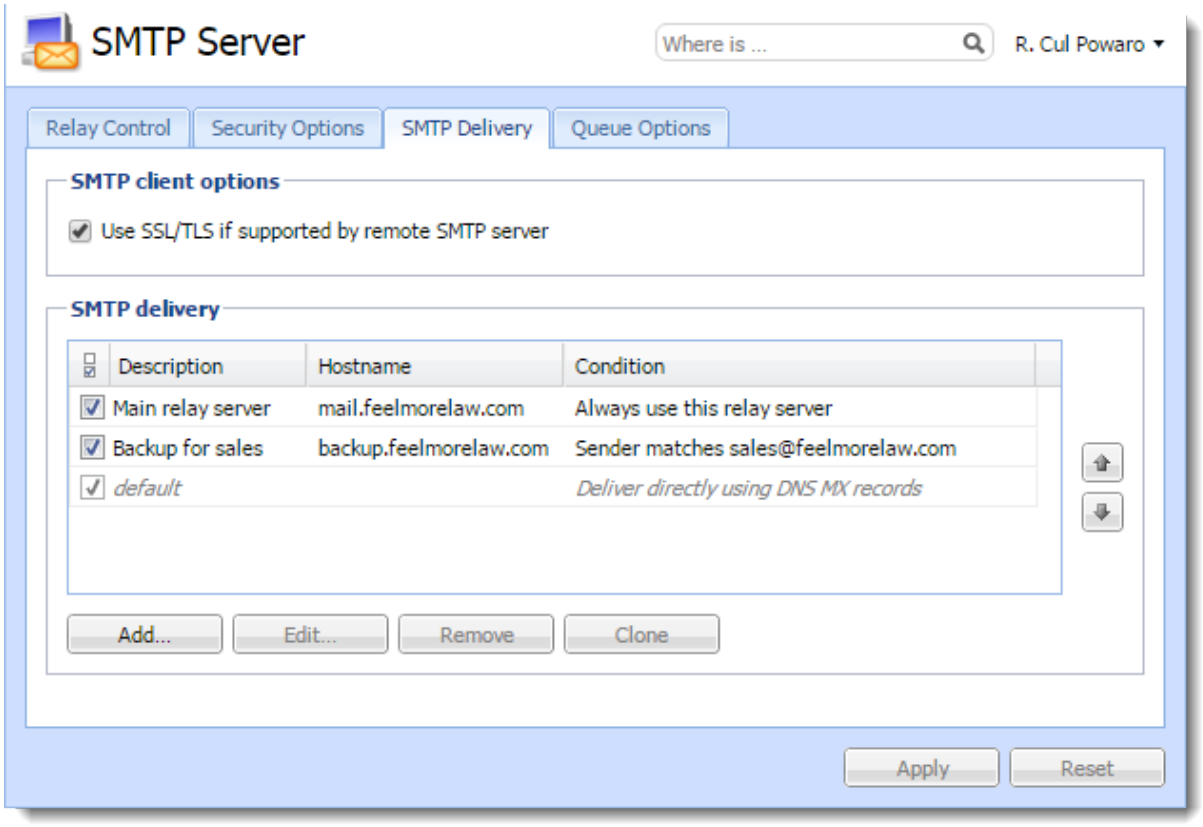
Sending outgoing messages through multiple servers

New in Kerio Connect 9!
In Kerio Connect 8 and older, you can define only a single SMTP relay server.

Kerio Connect can deliver messages:

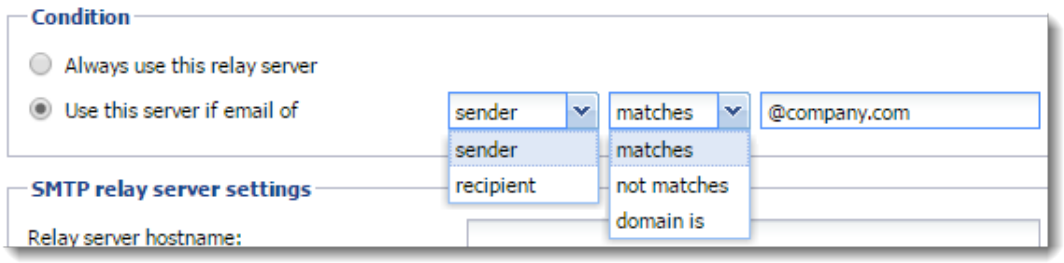
- Directly to destination domains using their MX records (the default SMTP relay server rule)
- Through multiple SMTP servers

  For example, Kerio Connect can use different SMTP relay servers for different domains in Kerio Connect.

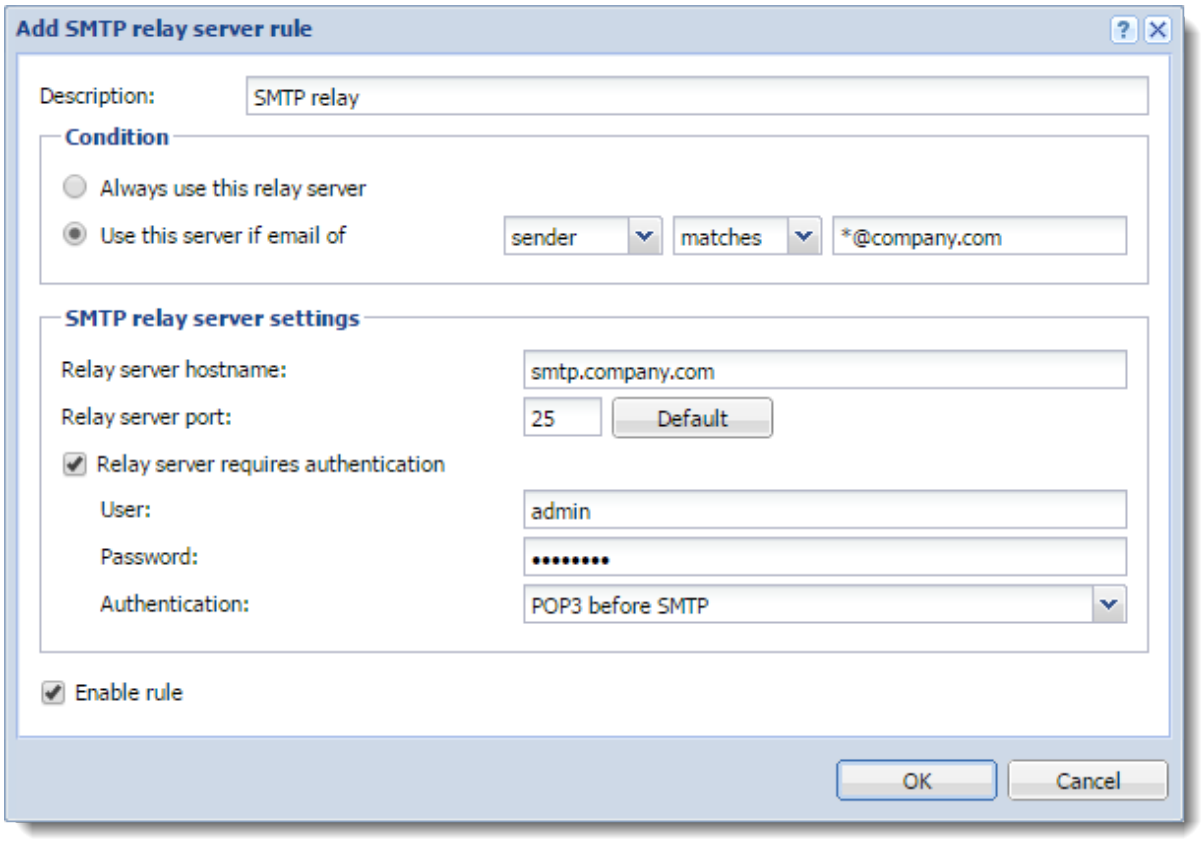


To define a SMTP relay server:

1. In the administration interface, go to **Configuration → SMTP Server → the SMTP Delivery tab**.
2. Click **Add**.
3. Type the description for the server.
4. To use only a single SMTP server to send messages, select **Always use this relay server**
5. To specify rules for the SMTP server:
   a. Select **Use this server if email of**.
   b. Define the rule for the sender or recipient.

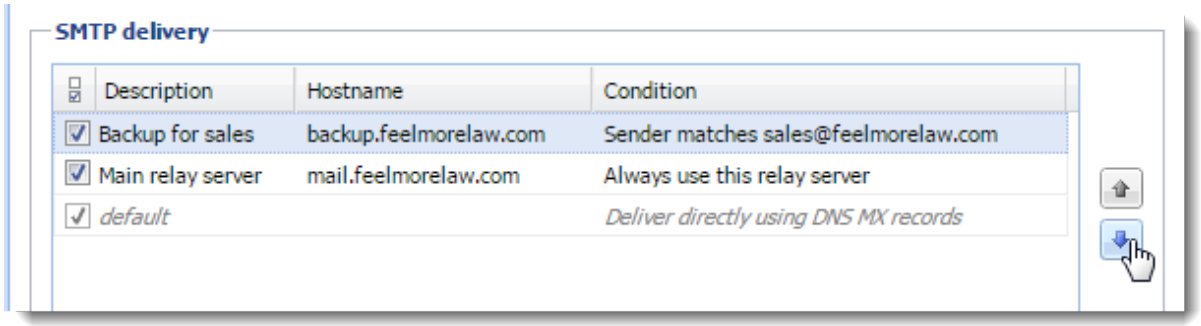


6. Type the relay server hostname and the server port.
7. If the server requires authentication, select the **Relay server requires authentication** option and type the username and password and specify the authentication method.
8. Click **OK**.
9. Click **Apply**.

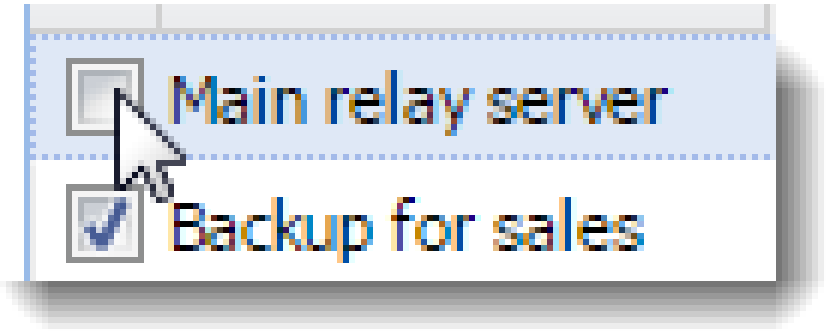


Kerio Connect processes the rules from the top — the first server that matches is used to send the message.

To change the order of the rules, select the rule and use the arrows on the right side.



To temporarily disable a rule, clear the dialog box next to the rule name.



Securing the SMTP server

For information about secure SMTP server, read Securing the SMTP server.

Troubleshooting

Sometimes a correct message is rejected. This may happen, for example, when a sales person sends multiple messages to customers and exceeds the limits set for the SMTP server. See troubleshooting in Securing the SMTP server.

Securing the SMTP server

Overview

In Kerio Connect, you can configure the SMTP server to protect Kerio Connect from misuse.

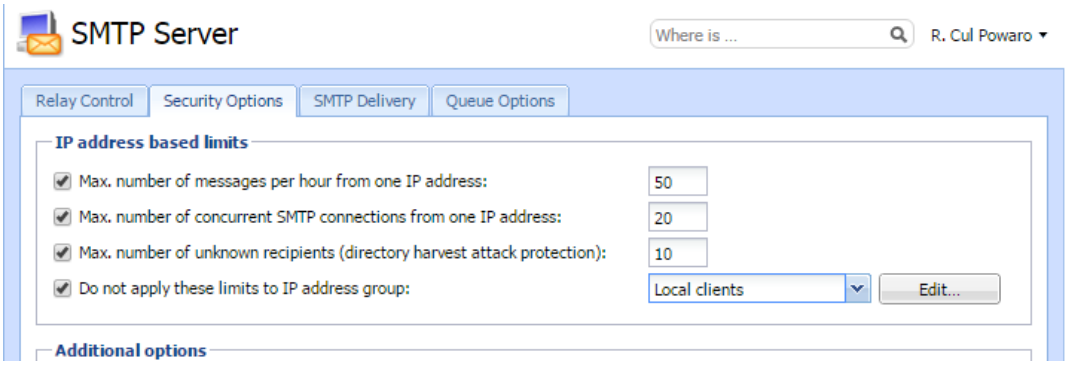
Anyone can connect to an unprotected SMTP server from the Internet and send email messages through Kerio Connect. Spammers can use your SMTP server to send out spam messages and your company may be added to spam blacklists.

 For detailed information about configuring the SMTP server, read Configuring the SMTP server.

Securing the SMTP server

In Kerio Connect, you can configure several limits for IP addresses to secure your SMTP server:

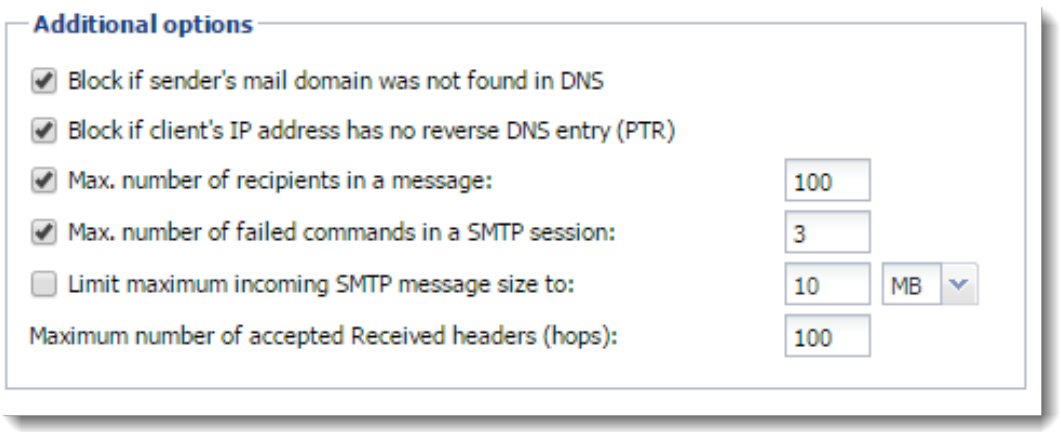
1. In the administration interface, go to the **Configuration** → **SMTP Server** → **Security Options** section.
2. Switch to the **Security Options** tab.
3. For a single IP address you can set the following **IP address based limits**:
    - **Max. number of messages per hour** — Discards any new message sent from the same IP address after reaching the set limit.
    - **Max. number of concurrent SMTP connections** — Gives protection from so-called DoS attacks which overload the server.
    - **Max. number of unknown recipients** — Protects Kerio Connect from so-called directory harvest attacks when an application connects to your server and uses dictionary to generate possible usernames.
4. Enable the **Do not apply these limits to IP address group** option and select a group of trusted IP addresses which are not affected by the above settings.



5. With the following **Additional options** you can protect Kerio Connect from:

   - Senders with fictional email addresses — the **Block if sender's domain was not found in DNS** and **Block messages if client's IP address has no reverse DNS entry (PTR)** options
   - Spam messages sent to a large number of recipients — the **Max. number of recipients in a message** option
   - Spammers who often send messages by special applications that connect to SMTP servers and ignore its error reports — the **Max. number of failed commands in a SMTP session** option

     With this option enabled, Kerio Connect closes the SMTP connection automatically after the defined number of failed commands.
   - Messages with large attachments which can overload your server — the **Limit maximum incoming SMTP message size to** option



6. On the **SMTP Delivery** tab, select the **Use SSL/TLS if supported by remote SMTP server** option.

7. Click **Apply**.

Troubleshooting

Sometimes a correct message is rejected. This may happen, for example, when a sales person sends multiple messages to customers and exceeds the limits set for the SMTP server. Adjust the settings on the **Security Options** tab.

Configuring POP3 connection

About POP3

Kerio Connect can retrieve messages from remote mailboxes via POP3. The retrieval is triggered by a scheduled action, and the downloaded messages are processed by sorting rules.

Defining remote mailboxes

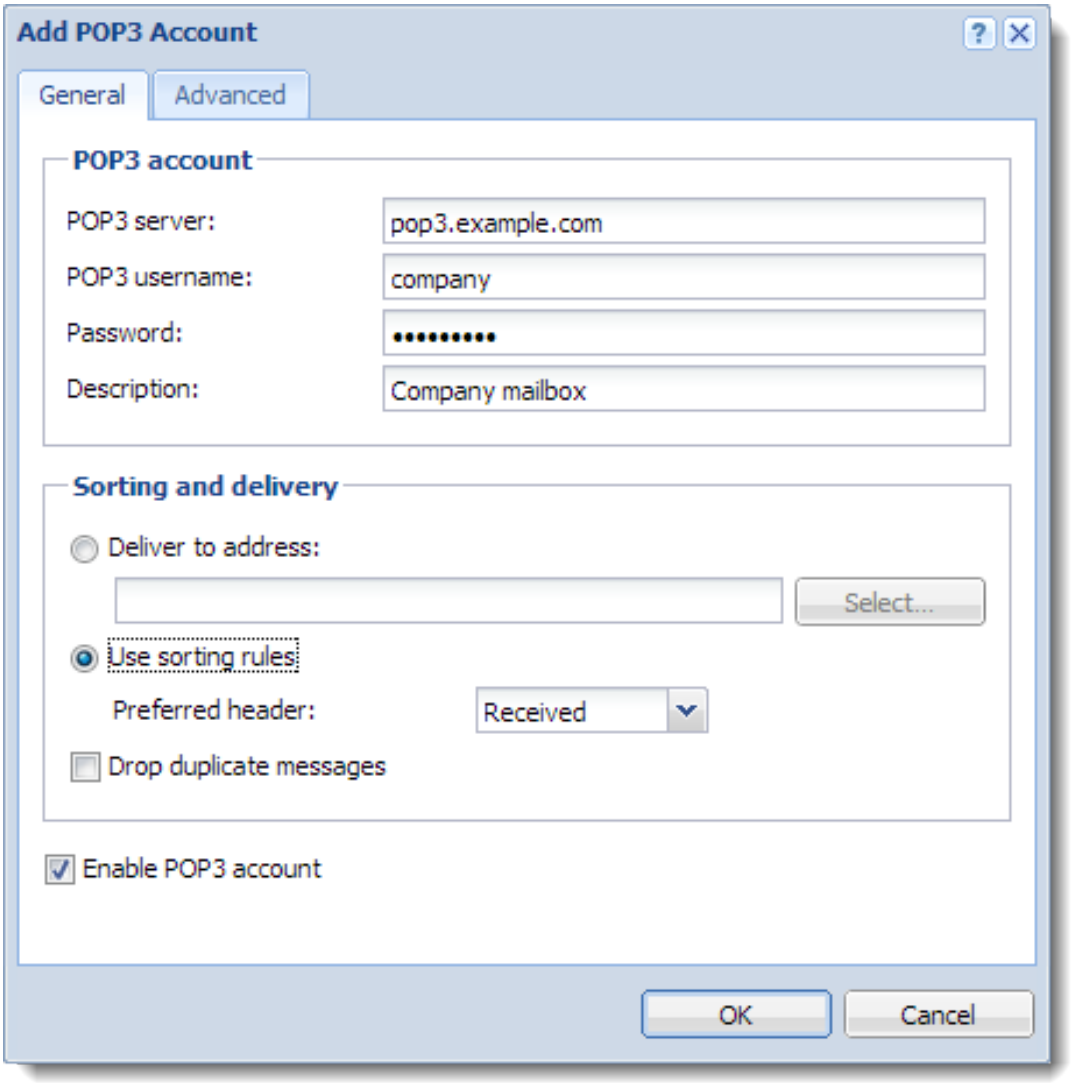
1. In the administration interface, go to **Configuration** → **Delivery** → **tab POP3 Download**.
2. In the **Accounts** section, click **Add**.
3. On the **General** tab, type the name of the POP3 server, and username and password of the POP3 account.

   The password length is max. 119 characters.

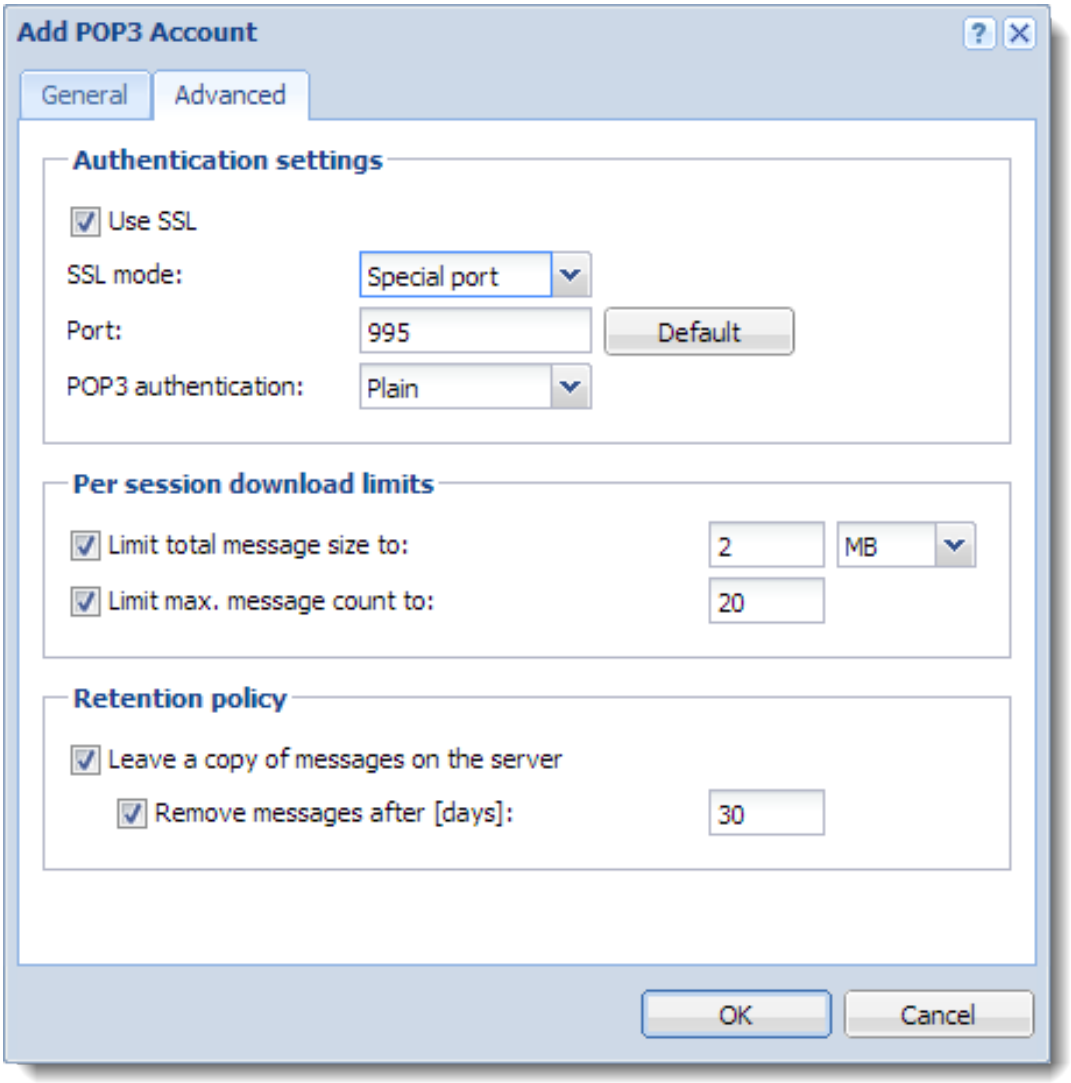
   Kerio Connect can:

   - deliver the messages to a specific address, or
   - use predefined sorting rules

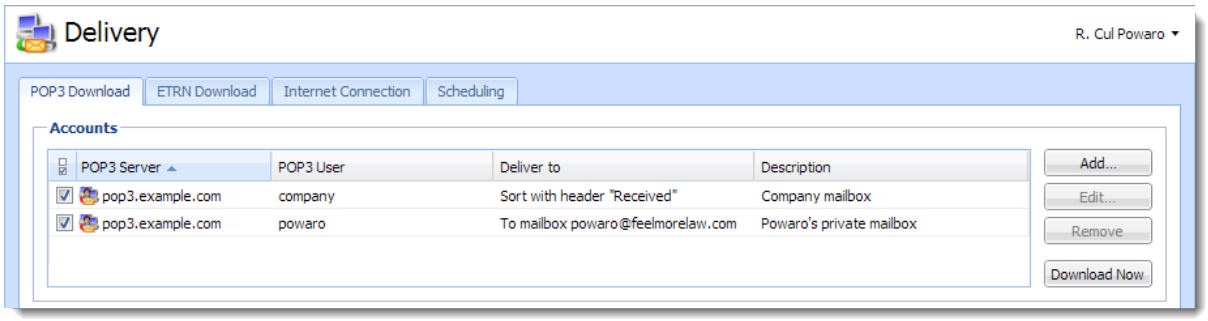


4. On the **Advanced** tab, you can:

   - require secure connection for POP3 download,
   - set download limits per session,
   - set retention policy.


Add POP3 Account
General
Advanced
Authentication settings
Use SSL
SSL mode:
Special port
Port:
995
Default
POP3 authentication:
Plain
Per session download limits
Limit total message size to:
2
MB
Limit max. message count to:
20
Retention policy
Leave a copy of messages on the server
Remove messages after [days]:
30
OK
Cancel

5. Click **OK**.

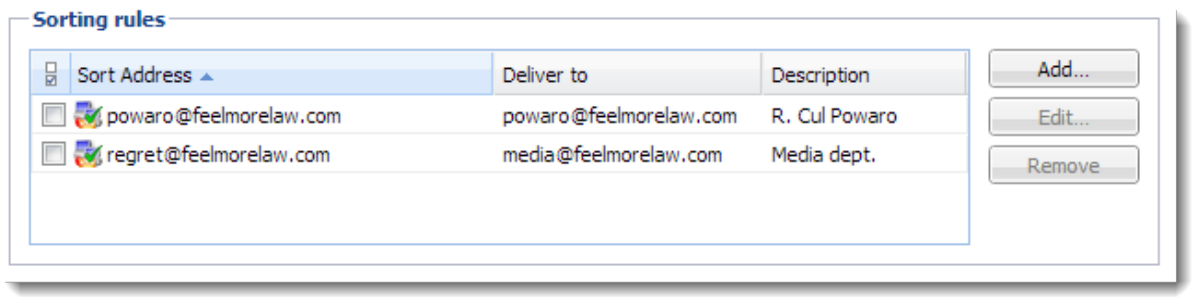

Delivery
R. Cul Powaro
POP3 Download
ETRN Download
Internet Connection
Scheduling
Accounts
POP3 Server
POP3 User
Deliver to
Description
pop3.example.com
company
Sort with header "Received"
Company mailbox
pop3.example.com
powaro
To mailbox powaro@feelmorelaw.com
Powaro's private mailbox
Add...
Edit...
Remove
Download Now

Sorting rules

Sorting rules define how Kerio Connect delivers messages downloaded from a remote POP3 mailbox. You can deliver messages to specific users, or forward messages to an email address.

1. In the administration interface, go to **Configuration** → **Delivery** → **tab POP3 Download**.
2. In section **Sorting rules**, click **Add**.
3. Type the **Sort address** — the email address according to which messages will be sorted.
4. Type the **delivery address** — an external address or **Select** an address form the Kerio Connect server.

5. Click **OK**.



Special sorting rules

*** → admin@example.com**

Kerio Connect delivers all messages not complying to any rule to the defined email address.

Without this rule, such messages are discarded.

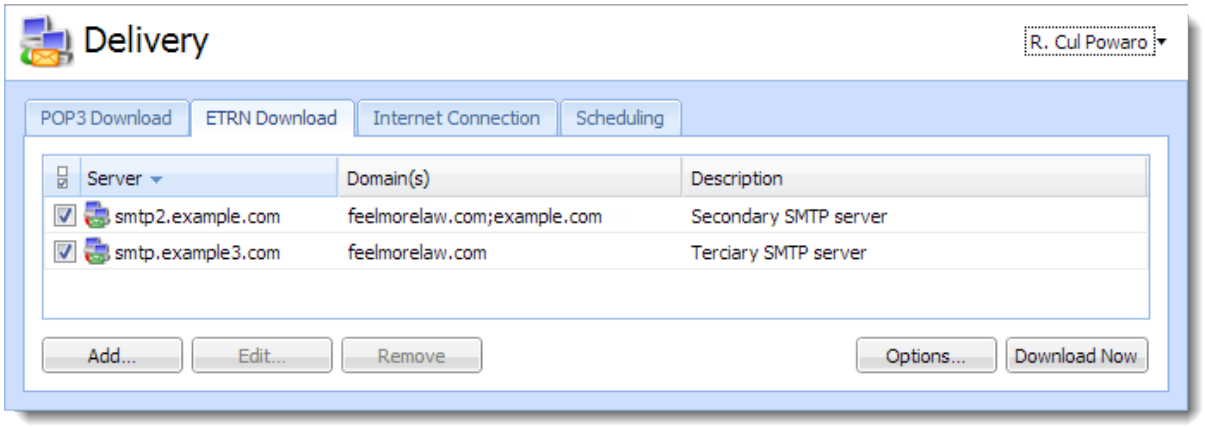
***@example.com → *@example.com**

Kerio Connect sorts messages according to the email addresses and aliases.

Receiving email via ETRN

About ETRN

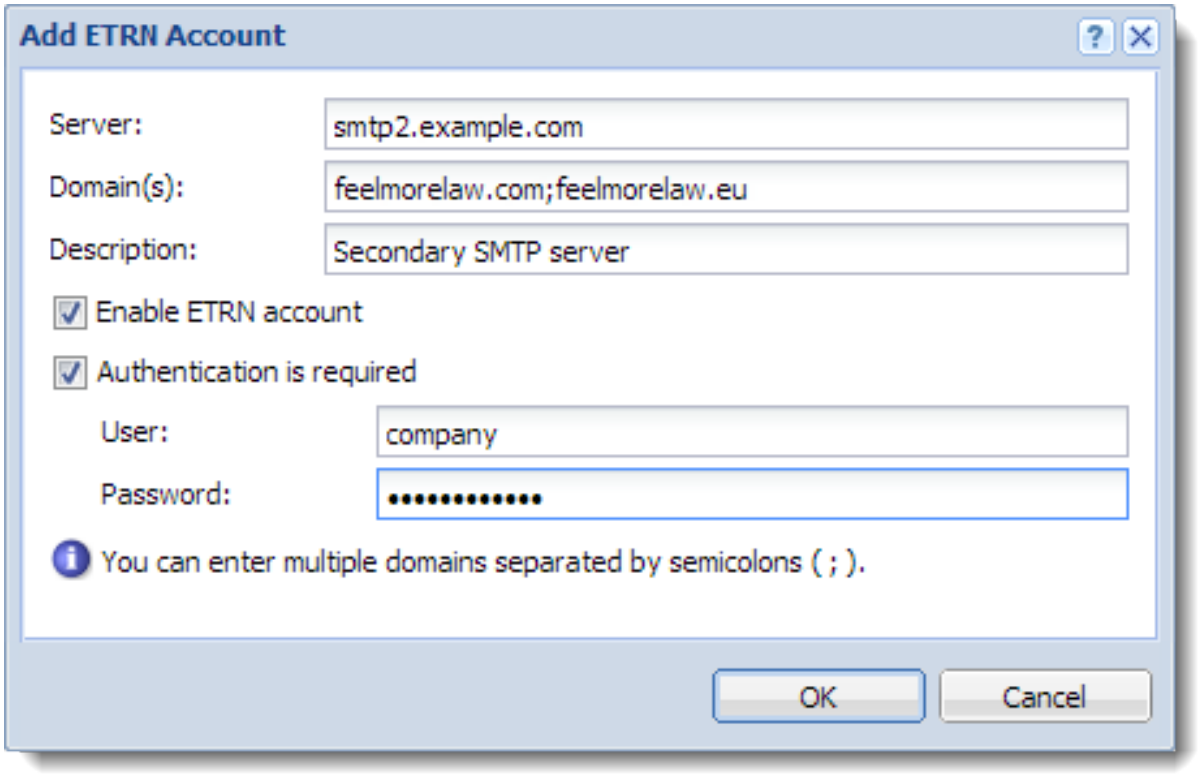
ETRN is a command of SMTP protocol. It serves for requesting emails stored on another SMTP server (usually secondary or tertiary SMTP servers).



Configuring the ETRN account

1. In the administration interface, go to section **Configuration** → **Delivery** → **ETRN Download**.
2. Click **Add**.

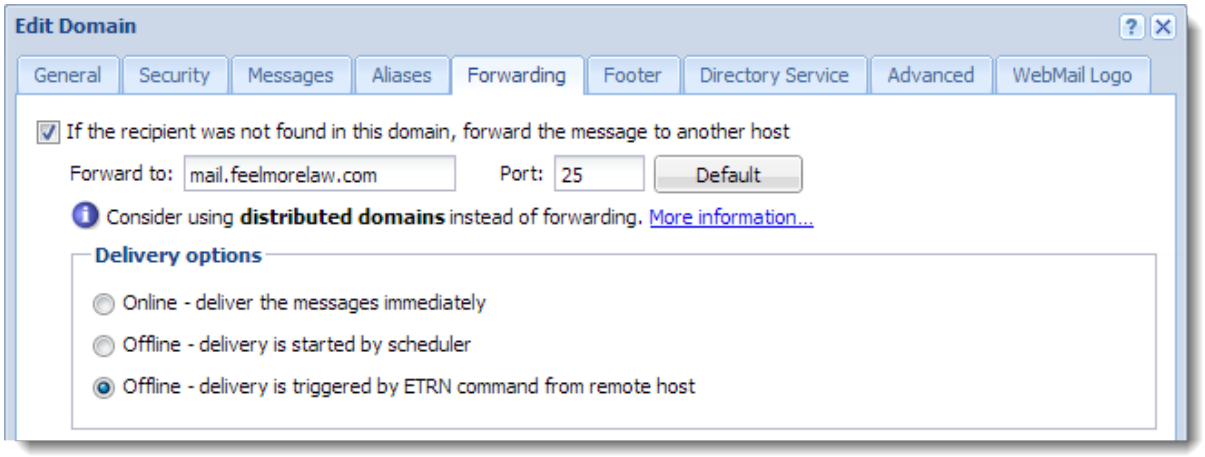
   The **Add ETRN Account** dialog opens.
3. Type the server name, domain names (can be separated by semi-colon).
4. If authentication is required, type the username and password.
5. Click **OK**.
6. Schedule an action for the ETRN download.



Forwarding email

If you set up a backup mailserver for your domain, you can use the ETRN command to forward messages from the backup server to your primary server.

1. On your primary server, enable and schedule sending of the ETRN command.
2. Go to **Configuration** → **Domains** and double-click the backup server.
3. On the **Forwarding** tab, select **If the recipient was not found in this domain, forward the message to another host**.
4. Type the primary server hostname and port.
5. Select **Offline - delivery is triggered by ETRN command from remote host**.
6. Click **OK**.



The primary server queries the backup server regularly using the ETRN command.

Scheduling email delivery

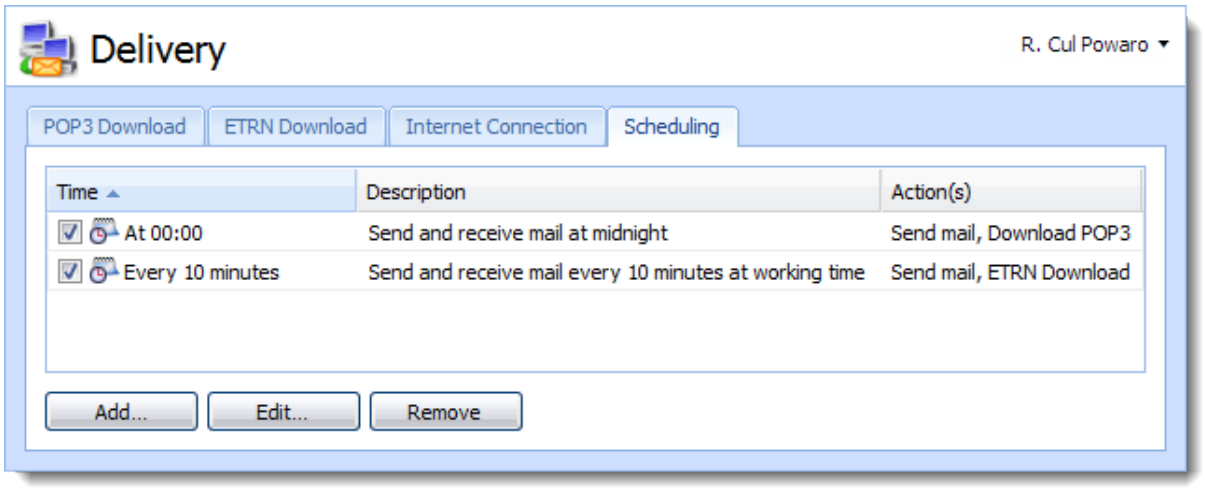
About scheduling

Kerio Connect can schedule the following actions:

- downloding messages from a remote POP3 server
- receiving messages using the ETRN command to defined servers
- sending messages from the message queue

Configure scheduling if you:

- have permanent Internet connection and use POP3 and/or ETRN,
- connect to the Internet via a dial-up line and use POP3 and/or ETRN



Configuring scheduling

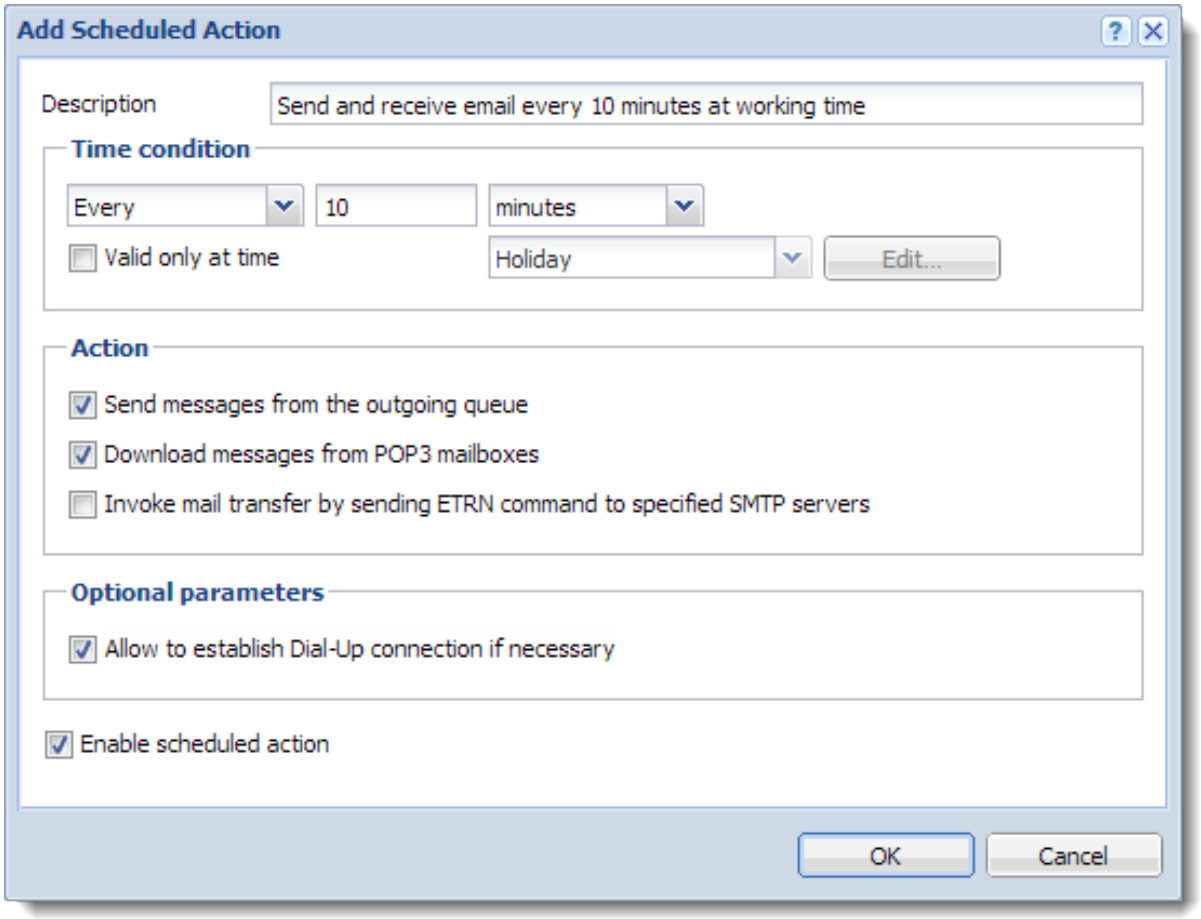
To add a new scheduled task, follow these steps:

1. In the administration interface, go to **Configuration** → **Delivery** → **tab Scheduling**.
2. Click **Add**.

   The **Add Scheduled Action** dialog opens.
3. Specify the **time condition**:

- **every** — number of minutes or hours
- **at** — a specific time every day
- **valid only at time** — you can specify a time interval when the scheduled action is valid

4. Specify the **action**, Kerio Connect performs.
5. Click **OK**.



Securing Kerio Connect

Issues to address

- Restricting communication on firewall to necessary IP addresses and ports
- Creating a strong passwords policy
- Configuring a security policy
- Configuring an SMTP server
- Using antispam and antivirus
- Enabling DKIM signature
- Enabling sender anti-spoofing protection

Configuring your firewall

If you install Kerio Connect in a local network behind a firewall, map these ports as follows:

Service (default port)	Incoming connection
SMTP (25)	allow
SMTPS (465)	allow
SMTP Submission (587)	allow
POP3 (110)	deny
POP3S (995)	allow
IMAP (143)	deny
IMAPS (993)	allow
NNTP (119)	deny
NNTPS (563)	allow
LDAP (389)	deny
LDAPS (636)	allow
HTTP (80, 4040, 8800)	deny
HTTPS (443, 4040, 8443)	allow

Table 1 Services to be allowed on the firewall

Password policy

Read Password policy in Kerio Connect for detailed information on user passwords.

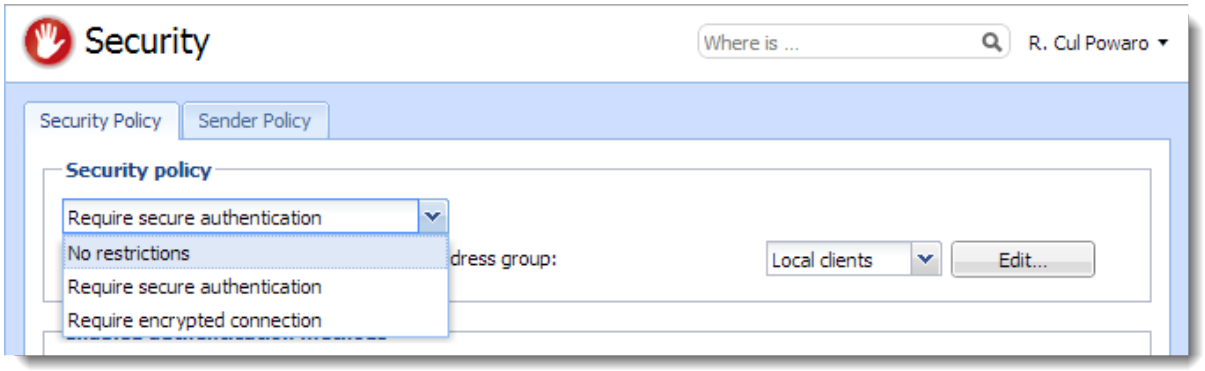
Configuring a secure connection to Kerio Connect

Kerio Connect can do either of the following:

- Secure user authentication
- Encrypt the whole communication

Go to **Configuration** → **Security** → **Security Policy** to select your preferred **security policy**.

You can define a group of IP addresses that can authenticate insecurely (for example, from local networks).

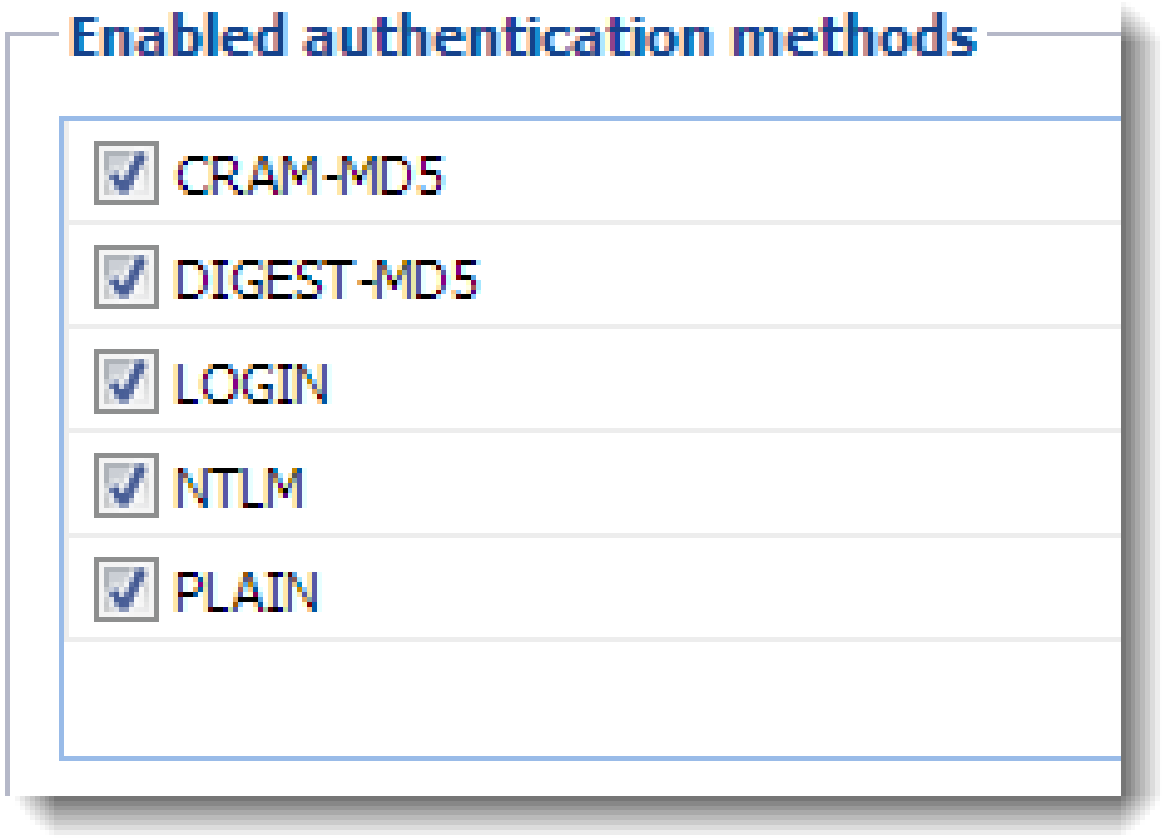


Securing user authentication

If you select the **Require secure authentication** option, users must authenticate securely when they access Kerio Connect.

You can select any of the following authentication methods:

- CRAM-MD5 — password authentication using MD5 digests
- DIGEST-MD5 — password authentication using MD5 digests
- NTLM — use only with Active Directory
- SSL tunnel if no authentication method is used



If you select more than one method, Kerio Connect performs the first available method.

If users' passwords are saved in the SHA format:
- Select **PLAIN** and/or **LOGIN**.
- Do not map users from a directory service.

Encrypting user communication

If you select the **Require encrypted connection** option, clients connect to any service via an encrypted connection (the communication cannot be tapped).

You must allow the secured version of all service you use on your firewall.

Many SMTP servers do not support SMTPS and STARTTLS. To provide advanced security, the SMTP server requires secure user authentication.

Configuring anti-spoofing in Kerio Connect

About anti-spoofing

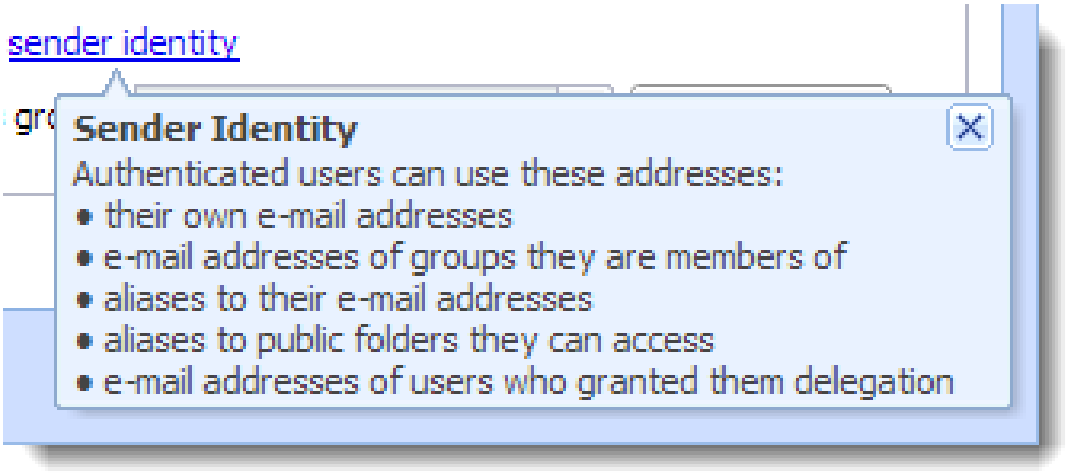
Spammers can "spoof" your email address and pretend their messages are sent from you.

To avoid such possibility, enable anti-spoofing in Kerio Connect.

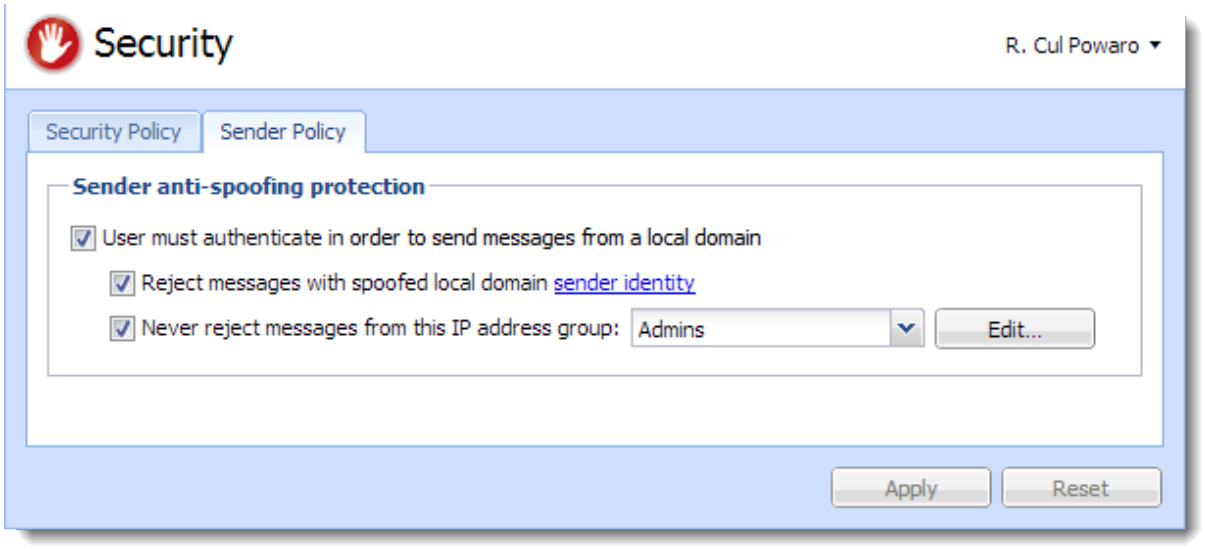
First, configure anti-spoofing for your server. Then, enable anti-spoofing for each domain.

Configuring anti-spoofing in Kerio Connect

1. Go to section **Configuration** → **Security** → **tab Sender Policy**.
2. Check option **User must authenticate in order to send messages from a local domain**.
3. Kerio Connect can automatically **Reject messages with spoofed local domain**.
   Click the sender policy link to see which types of addresses will be available to your users.



   You can define a group of trusted IP addresses.

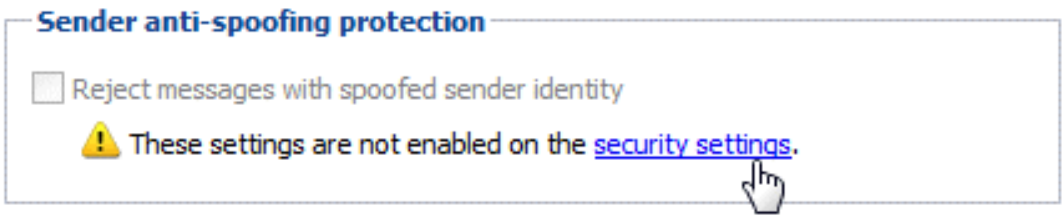


For more information about the security features in Kerio Connect, read article Securing Kerio Connect.

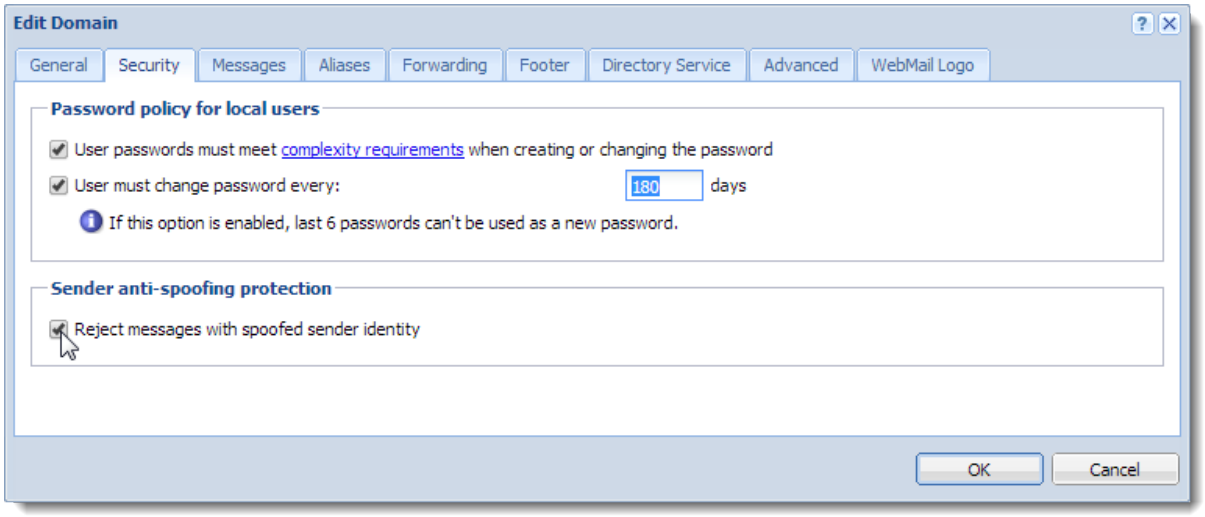
Enabling anti-spoofing per domain

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click a domain and go to tab **Security**.
3. Check option **Reject messages with spoofed sender identity**.

   If the option is not available, you haven't configured anti-spoofing for the server. Click the **security settings** link, which will take you to the appropriate section.



4. Save the domain settings.


Edit Domain
General
Security
Messages
Aliases
Forwarding
Footer
Directory Service
Advanced
WebMail Logo
Password policy for local users
User passwords must meet complexity requirements when creating or changing the password
User must change password every:
180
days
If this option is enabled, last 6 passwords can't be used as a new password.
Sender anti-spoofing protection
Reject messages with spoofed sender identity
OK
Cancel

Password policy in Kerio Connect

About password policy

To secure users and their passwords in Kerio Connect:

- advise users to create strong passwords
- require complex passwords (for local users)
- enable password expiry (for local users)
- protect against login guessing

Creating strong user passwords

Strong user passwords should be long and complex. The following guidelines may help you in advising your users:

Long
Passwords should be at least 8 characters long.

Complex
Passwords should contain all of the following:

- lowercase letters
- uppercase letters
- numbers
- special characters

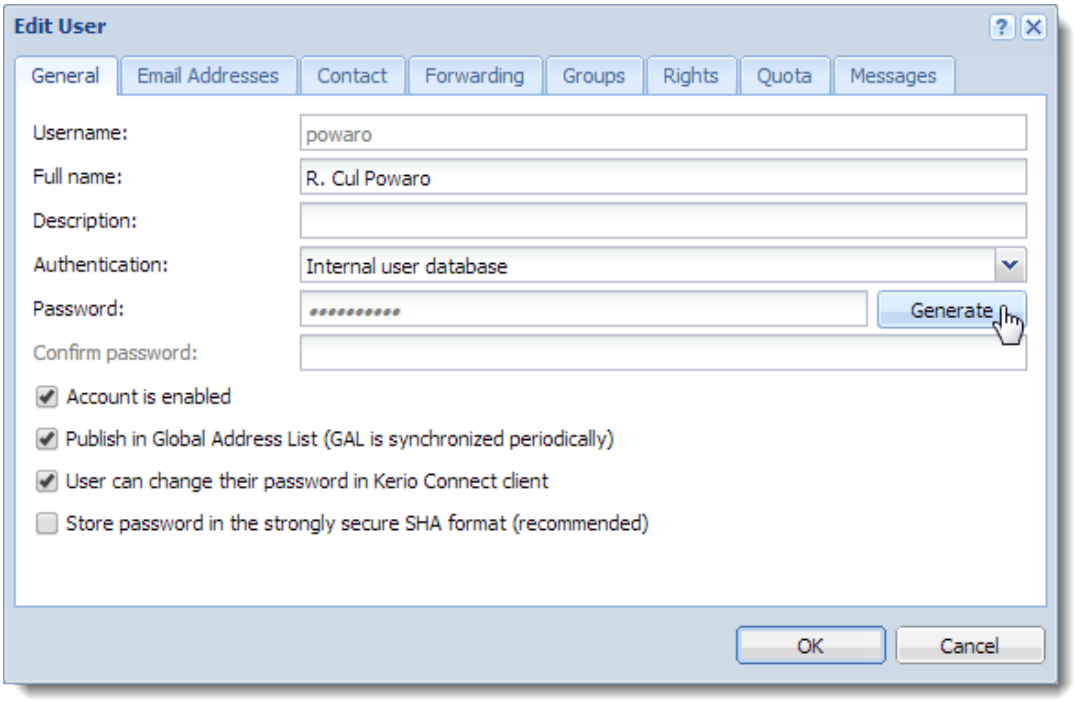
Valid
Users should change their password often.

You can also read this Wikipedia article for more information.

Generating strong passwords

Kerio Connect can generate strong passwords for your users:

1. Go to section **Users** and double-click a user.
2. On tab **General**, click the **Generate** button.



3. Copy the generated password and give it to user.
4. Save the settings.

Requiring complex passwords (for local users)

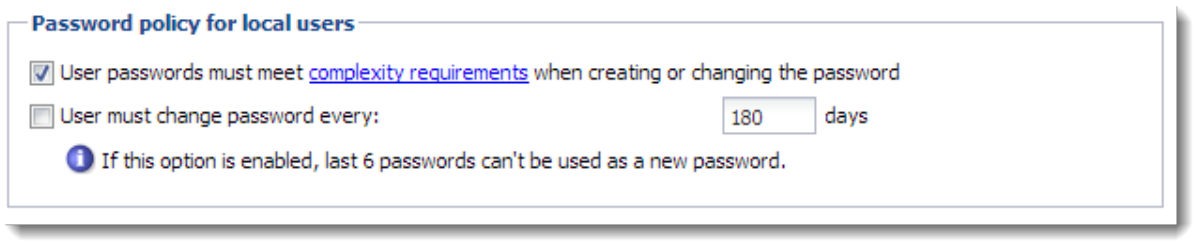
In Kerio Connect, you can force local users to create strong and complex passwords.

Complex password:

- must be at least 8 characters long,
- must include at least 3 types of characters (lowercase, uppercase, numbers, symbols),
- cannot include user's domain and username, and any part of user's fullname (longer than 2 characters).

The settings are configured per domain.

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click a domain and go to tab **Security**.
3. Enable option **User passwords must meet complexity requirements**.
4. Confirm.



From now on, whenever a local user changes their password in Kerio Connect Client, they will have to create new password which complies with Kerio Connect's complexity requirements.

Remember to enable users to change their passwords in Kerio Connect Client.

Enabling password expiry (for local users)

To secure local user passwords, you can enable password expiration.

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click a domain and go to tab **Security**.
3. Enable option **Enforce user password expiration after**.
4. Set the number of days after which users will have to change their password.
5. Confirm.

Any change to these settings (checking/unchecking the option) will reset the counter for password expiry.

Notifying about expiration

Kerio Connects sends notifications to users before their password expires. The notifications are sent 21, 14 and 7 days before expiration, and then every day until the password expires.

Users have to change their password in Kerio Connect Client.

If the user fails to change their password, they will not be able to login to their acount and will have to contact their administrator (who changes the password for them in their user settings).

If an administrator password expires, the administrator will be able to login to the administration interface to change their password.

Protecting against password guessing attacks

Kerio Connect can block IP addresses suspicious of password guessing attacks (ten unsuccessful attempts in one minute).

1. Go to section **Configuration** → **Security** → **tab Security Policy** (**Configuration** → **Advanced Options** → **tab Security Policy** for Kerio Connect 8.1 and older).

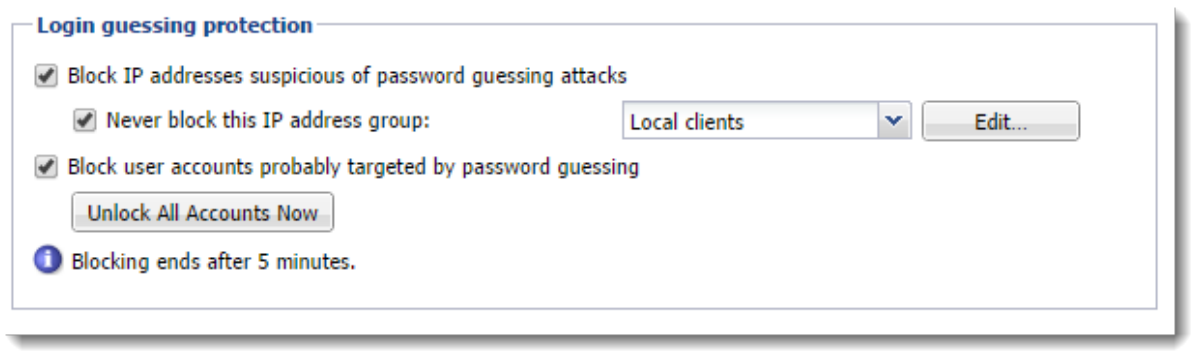
2. Check option **Block IP addresses suspicious of password guessing attacks**.

   IP address is blocked for individual services. If POP3 is blocked, attacker can attempt logging via IMAP.

3. You can select a group of trustworthy IP addresses.

4. To block all services, check option **Block user accounts probably targeted by password guessing** to lock the affected accounts.

5. Save the settings.



When an account is blocked, user cannot log in. Kerio Connect unlocks the blocked accounts after 5 minutes. For immediate unlocking (throughout all the domains), click **Unlock All Accounts Now**.

This action is not identical with temporary disabling user accounts.

Authenticating messages with DKIM

About DKIM

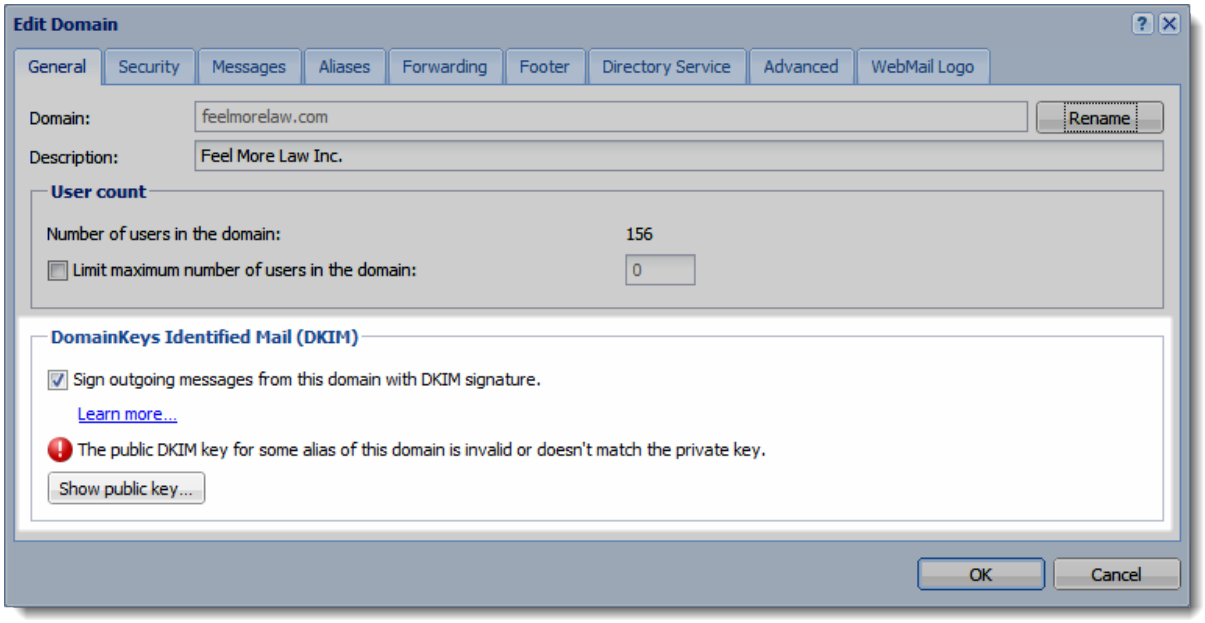
DomainKeys Identified Mail (DKIM) signs outgoing messages from Kerio Connect with a special signature to identify the sender. Your users thus take responsibility for the messages they send and the recipients are sure the messages came from a verified user (by retrieving your public key).

To sign messages with a DKIM signature:

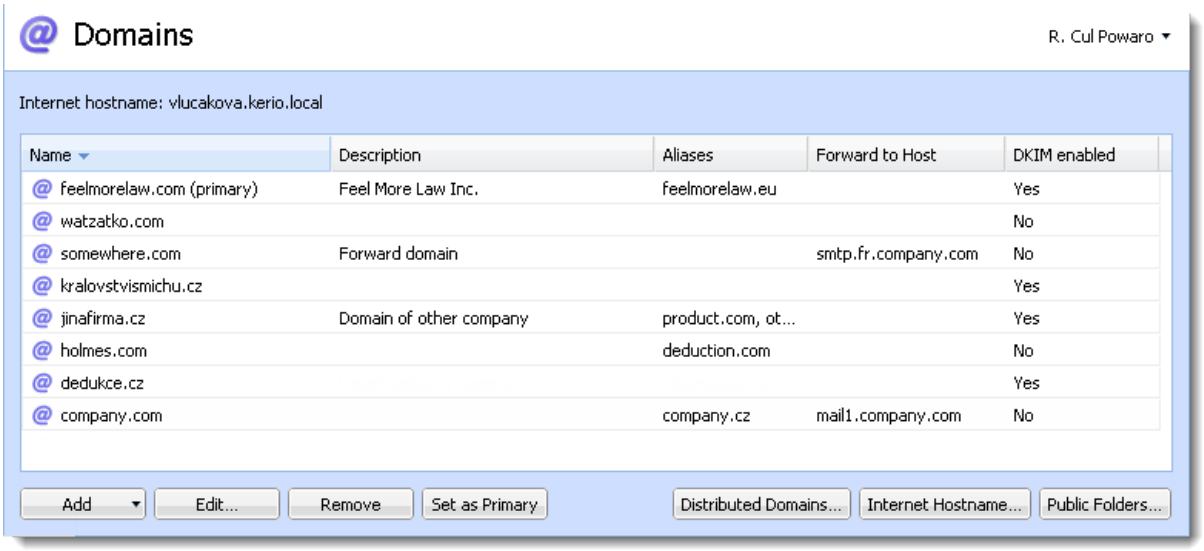
1. Enable DKIM authentication in your domain settings.
2. Add the DKIM public key to your DNS settings.

Enabling DKIM in Kerio Connect

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click your domain and go to tab **General**.
3. Enable option **Sign outgoing messages from this domain with DKIM signature**.
4. Save the settings.



To see which domains have DKIM enabled, add column **DKIM enabled** in section **Configuration** → **Domains**.



Your DNS records must include the DKIM public key for your domain. Without proper DNS records, Kerio Connect will send messages without the DKIM signature. Each message your users send will create an error message (see Error log).

Read article Configuring DNS for DKIM for more information.

Aliases

If the domain includes also aliases, add the DNS record also to all aliases.

Testing the DKIM signature

If you want to test whether your domain signs messages with DKIM, you can use for example the DomainKeys Test online tool.

Configuring DNS for DKIM

Adding a DKIM record to your DNS

The process of adding a DKIM record to your DNS may vary according to your provider.

To add your DKIM public key to DNS, you can:

- ask your provider to add the record for you
- do it yourself in your DNS administration

You can find the public key in Kerio Connect. The key includes two parts:

- **Record name** (or selector)

  Example:

  `mail._domainkey.feelmorelaw.com.`

- **TXT value**

  Example:

  ```
  v=DKIM1;
  p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z
  Oo3N+Il22OoK2Cp+NZw9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn
  AB3DGAQ6+/7UVXf9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb
  bcBhthrnETKoCg8wOwIDAQAB
  ```

  The public key TXT value consists of one single line of text.

The DKIM public key is the same for all domains on a single server (in a single Kerio Connect).

The DKIM public key in Kerio Connect is 2048-bit. Some providers may restrict the length of the key (the TXT value) — read section Creating a short DKIM public key to get detailed information.

Domain aliases

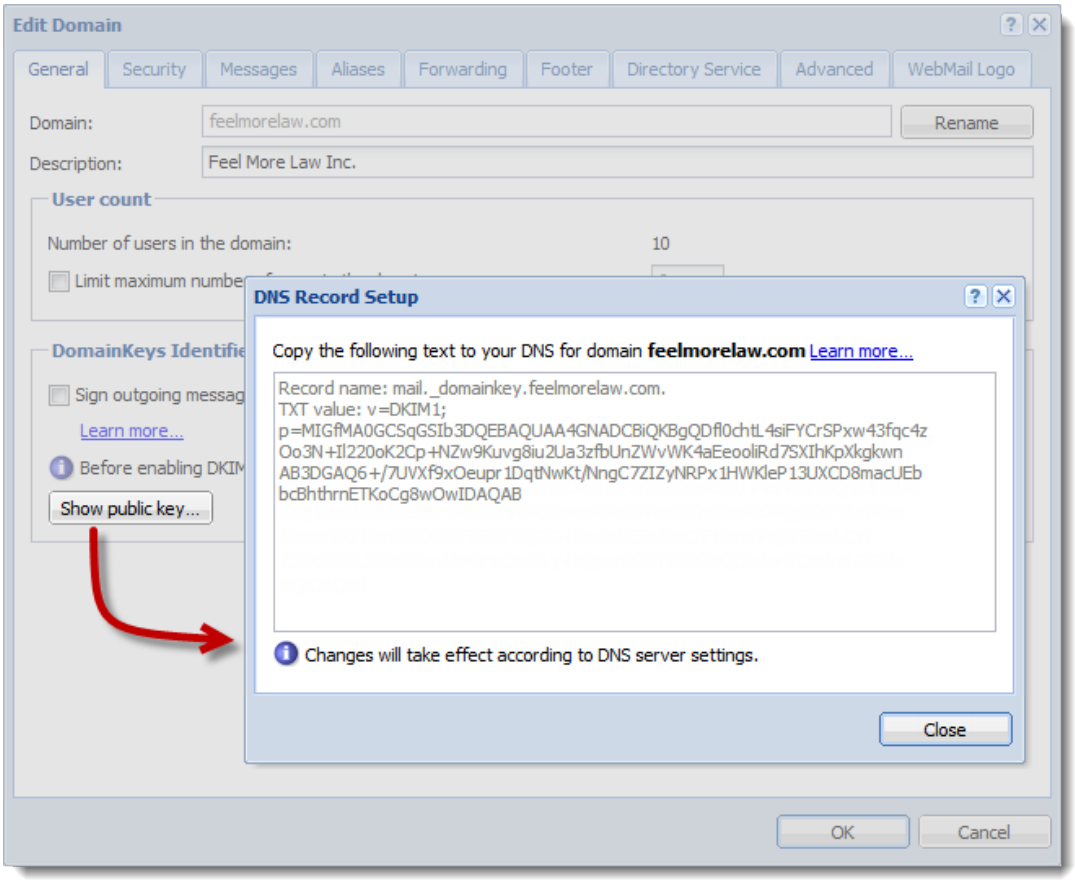
If a domain includes aliases, also add DNS record for DKIM to all aliases.

Acquiring DKIM public key in Kerio Connect

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click your domain and go to tab **General**.
3. Click the **Show public key** button.

   This opens a dialog with you domain public key.

   Copy the text to create your DNS DKIM record. Make sure the record contains the whole text.

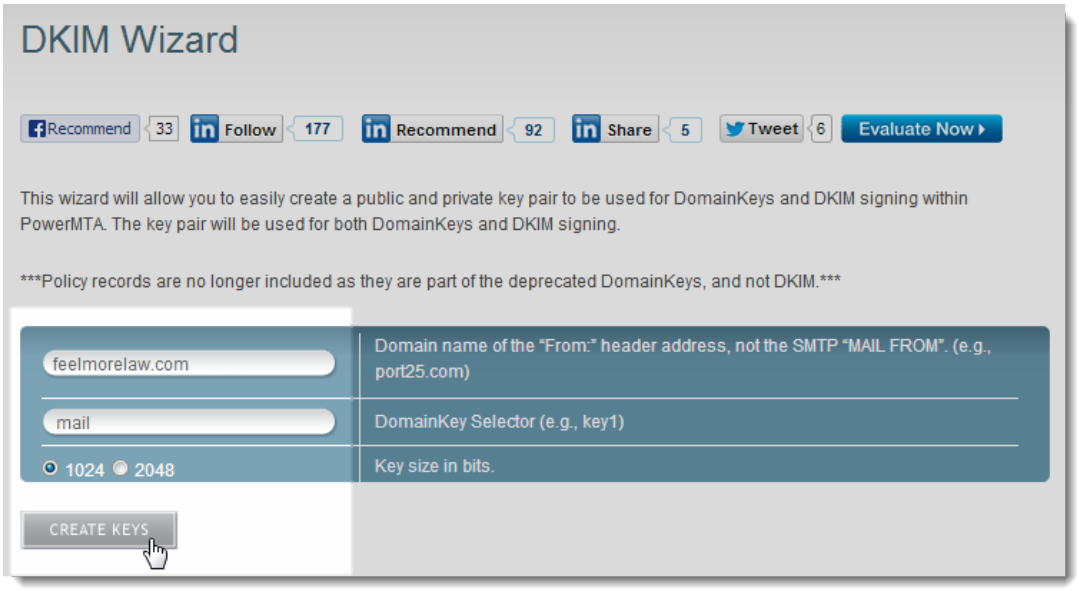


Creating a short DKIM public key

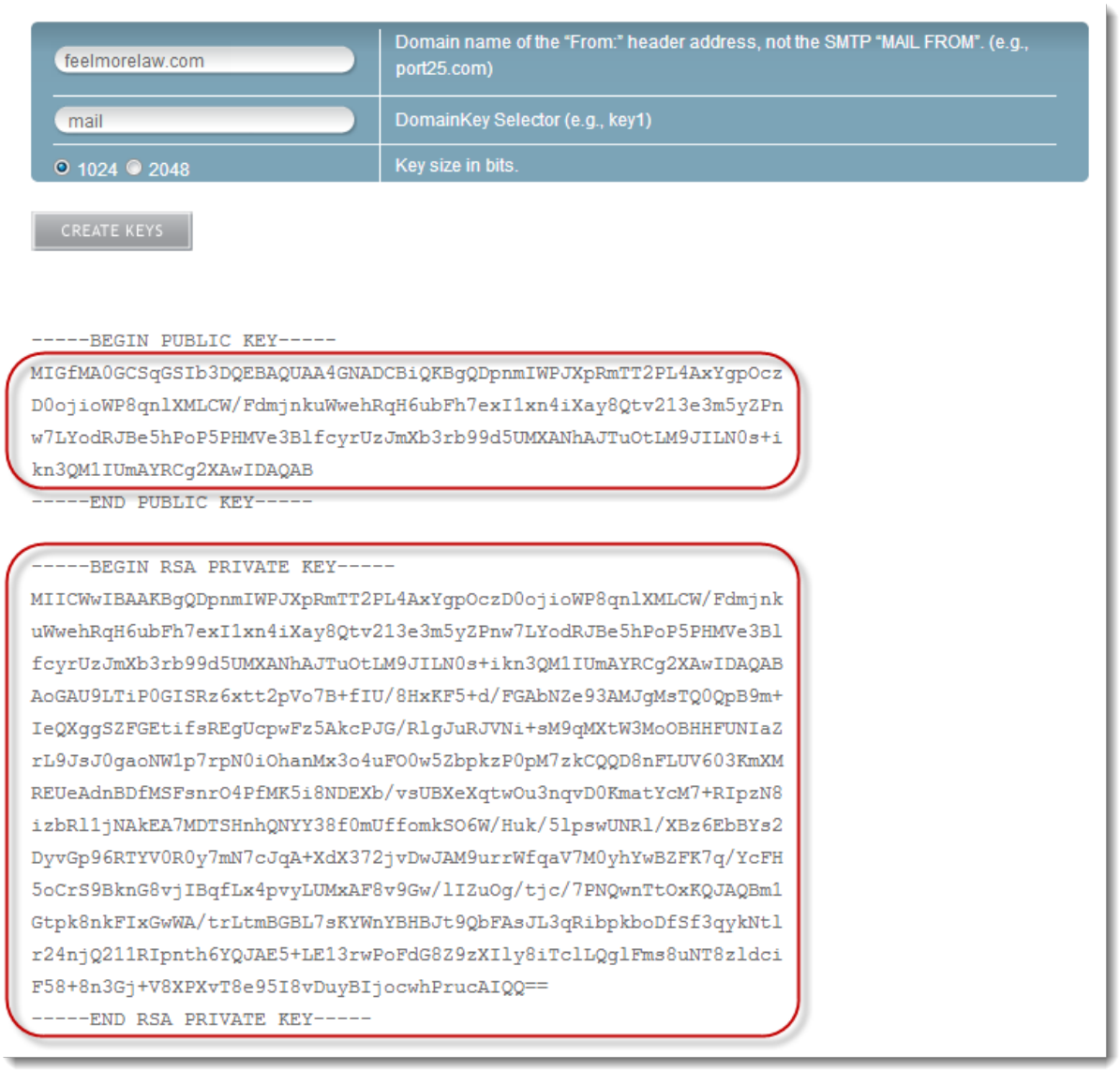
Kerio Connect includes a 2048-bit DKIM public key. If the public key is too long (some providers may restrict the length of the TXT value), you can use an online DKIM key creator to create a 1024-bit key. See an example below.

Generating a short DKIM key with DKIM wizard

1. Go to the DKIM wizard page.
2. Fill in your **Domain name** and **DomainKey Selector** (use `mail`).
3. Select **Key size** 1024.
4. Click **Generate**.



The page will display your public and private keys. Now, add the private key to Kerio Connect.



Adding a new private key to Kerio Connect

1. Stop the Kerio Connect server.
2. Go to Kerio Connect's installation directory to folder **sslcert/dkim**.
3. Copy the generated private key to file `private.key`.

   We recommend backing up the original private key.

4. Start the Kerio Connect server.

Kerio Connect will now show the shorter public key in the domains' configuration. You can now create the DNS DKIM record with the new public key.

If you use distributed domains, make sure the new private key is available on all servers.

BIND DNS server

If you use a BIND DNS server, you can split the original Kerio Connect DKIM public key TXT value by using the following format:

```
TXT ( "part 1" "part 2" ...  "part x")
```

Example:

```
TXT ("v=DKIM1;"
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z"
"Oo3N+Il22OoK2Cp+NZw9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn"
"AB3DGAQ6+/7UVXf9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb"
"bcBhthrnETKoCg8wOwIDAQAB")
```

Configuring spam control in Kerio Connect

Antispam methods and tests in Kerio Connect

Spam is unwanted email, usually advertisements. Kerio Connect includes many options and features to dispose of spam.

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

- **Black/white lists** — You can create and use lists of servers and automatically block or allow all messages they send. For detailed information, see Blocking messages from certain servers
- **SpamAssassin** — Apache SpamAssassin is a widely used antispam filter that employs several testing methods.
- **Caller ID** and **SPF** — These allow you to filter out messages with fake sender addresses. For detailed information, see Configuring Caller ID and SPF in Kerio Connect
- **Greylisting** — The greylisting method uses a special server that stores information about messages and delivers only messages from known senders. For detailed information, see Configuring greylisting
- **Delayed response to SMTP greeting (Spam Repellent)** — You can set a delayed SMTP greeting that will prevent delivery of messages sent from spam servers.

   Messages rejected by Spam Repellent are not processed by other antispam and antivirus tests, so this method decreases the load on your server.

- **Custom rules** — You can create your own rules that will satisfy your needs. For detailed information, see Creating custom rules for spam control in Kerio Connect

 These tests can be used separately or combined with the others. For efficiency, it is recommended that you combine as many antispam features as possible. The more tests you use, the tighter the antispam filter and the less spam that will be delivered to user's mailbox. Also, spam detection will be more granular, which will reduce the number of messages marked as spam by mistake ("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 to specify how spam messages are handled:

- Messages are denied — This helps to reduce the load on the server
- The message's spam score is raised — This helps eliminating possible "false positives"

To set the Kerio Connect spam filter, go to **Configuration** → **Content Filter** → **Spam Filter**.

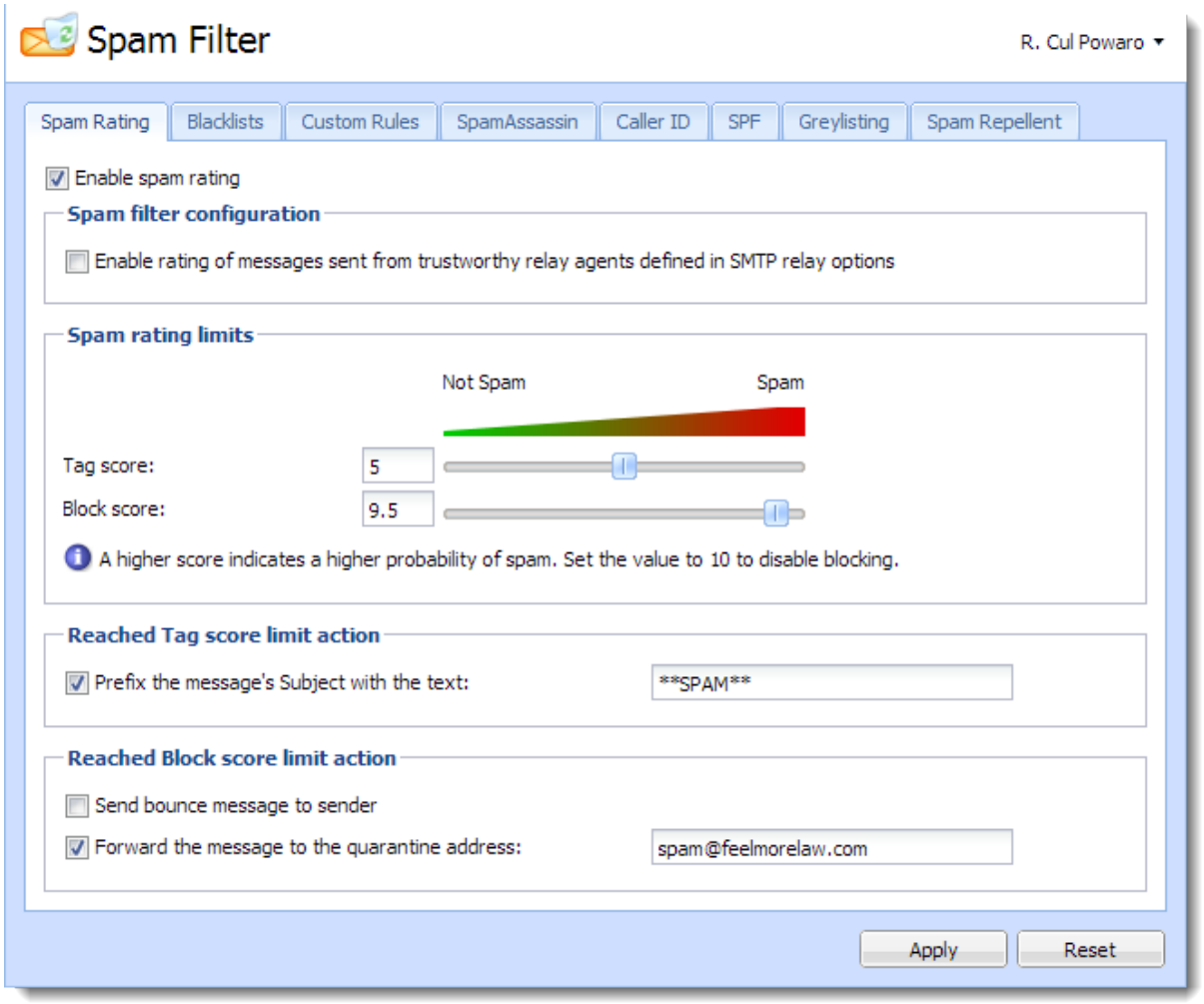
Setting the spam score

Once a message is tested by all enabled tests and filters, it is rated by its resulting spam score. Kerio Connect then marks the message as spam or delivers it as a legitimate message.

You can set limits where messages are simply marked as spam and where the spam score is so high that there is no doubt it is spam and can be blocked:

- **Tag score** — If the rating reaches or exceeds the value set, the message is marked as spam.
- **Block score** — If the rating reaches or exceeds the value set, the message is discarded.

If you set a tag value that is too low, legitimate messages might be discarded along with spam. Therefore, it is recommended that you 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 are delivered and stored.



Monitoring a spam filter's functionality and efficiency

Kerio Connect includes several options for how to monitor spam filter's functionality.

Spam filter statistics

Kerio Connect generates statistics of its spam filter. The statistics can be found in **Status** → **Statistics**.

Spam filter statistics	
Messages checked	5
Spams detected (tagged)	2
Spams detected (rejected)	3
Messages marked by users as spam	1
Messages marked by users as not spam	0

Figure 1 Spam Filter statistics

Graphical overviews

Kerio Connect also uses traffic charts to trace certain values about spam email. There are several spam-related traffic charts, which can be found in the **Status** → **Traffic Charts** section.

The following graphs focus on spam:

- **Connections/Rejected SMTP** displays the number if SMTP connection attempts that were rejected by the Spam Repellent tool in a certain time period.
- **Messages/Spam**. With time dependence, the chart displays how much spam is delivered to Kerio Connect and when.

Logs

Problems possibly related to the antispam filter may be solvable with the help of Kerio Connect logs.

These logs could be helpful:

- **Spam**. All messages marked as spam are recorded in this log.
- **Debug**. Logging of particular information can be performed with this special log. You may be able to resolve spam issues using the following information (right-click in the **Debug** log area and click **Messages**):
  - **Spam Filter** — This option logs the spam rating of each message that passed through the Kerio Connect antispam filter.
  - **SPF Record Lookup** — This option gathers information about SPF queries sent to SMTP servers.
  - **SpamAssassin Processing** — This option enables you to trace of processes that occurred during SpamAssassin antispam tests.

Configuring greylisting

Overview

To fight spam more efficiently, Kerio Connect supports **greylisting**.

Greylisting is an antispam method that complements other antispam methods and mechanisms in Kerio Connect.

How greylisting works

With greylisting enabled, the following happens when Kerio Connect receives a message:

1. Kerio Connect contacts the greylisting server and provides information about the message.

   The greylisting server includes a list of trustworthy IP addresses.

2. If **the list contains** the message sender's IP address, the message passes the greylisting check immediately.

3. If **the list does not contain** the sender's IP address, the greylisting server delays the delivery. Trustworthy mailservers try to redeliver messages later. Spam senders usually do not.

4. Once the message is received again, the Kerio Greylisting Service adds the sender's IP address to the whitelist. All future messages from this sender will pass the greylisting check immediately (see step 2).

To learn more about greylisting, consult greylisting.org or Wikipedia.

What data is sent to Kerio Technologies

If the greylisting is enabled, the Kerio Technologies greylisting server receives the following information:

- One-way hash (MD5) of the sender's envelope email address and recipient's envelope email addresses
- IP address of the host delivering the message

The data is periodically deleted from the greylisting server.

If greylisting is disabled, no data is sent to Kerio Technologies.

Kerio Technologies uses the received data solely for the greylisting feature.

To see the data sent by Kerio Greylisting Service, enable **Greylisting** in the Debug log.

Configuring greylisting

Kerio Greylisting Service in Kerio Connect is hosted by Kerio Technologies.

It is available to:

- Registered trial users
- Licensed users with valid Software Maintenance

Greylisting is disabled by default. To enable it:

1. In the administration interface, go to **Configuration** → **Content filter** → **Spam Filter** → **Greylisting**.
2. Select the **Check incoming messages by Kerio Greylisting Service** option.

   Make sure your firewall allows outgoing connection on port 8045.
3. (Optional) Create a list of IP addresses to skip in the greylisting check.
4. Click **Test Connection** to check the connection with Kerio Greylisting Service.

   The connection is established every time Kerio Connect server is restarted.
5. Click **Apply**.

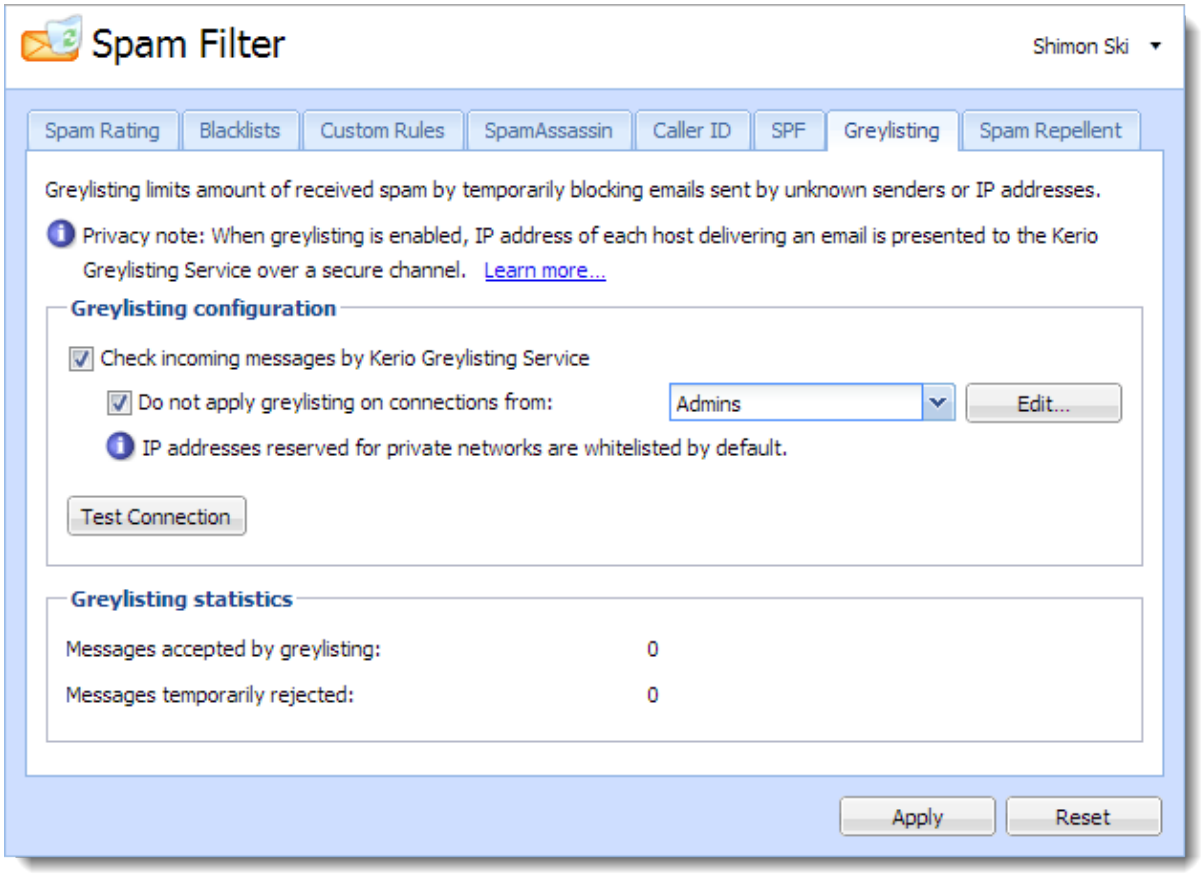


Figure 1 Greylisting

Troubleshooting

If the connection between your Kerio Connect server and Kerio Greylisting Service fails, make sure your firewall allows outgoing connections on port 8045.

Users may experience a delay in delivery. This happens when the message with the particular parameters is received, as described in section What data is sent to Kerio Technologies. The greylisting server delays the delivery. This problem is solved once another message is received.

Messages can also be delivered in a different order than they were sent, due to the greylisting server. This problem is solved once another message with the same parameters is received.

If you want to see what data are sent to Kerio Technologies, enable **Greylisting** in the Debug log.

If Kerio Connect cannot contact the greylisting server, all incoming messages are delivered immediately. Kerio Connect will try to contact the greylisting server again.

If you acquire a new license or renew your license, it may take several minutes before the Kerio Greylisting Service recognizes it. You may get warning messages in the meantime. Message delivery is not affected.

Blocking messages from certain servers

Automatically blocking or allowing messages from certain servers

In Kerio Connect you can automatically block servers (IP addresses) that are known to be sending spam messages. You can also automatically allow messages from those you trust.

You can this in one (or both) of two ways:

- By creating your own lists of spam servers (**blacklists**) and trusted servers (**whitelists**)
- By using public Internet databases of spam servers

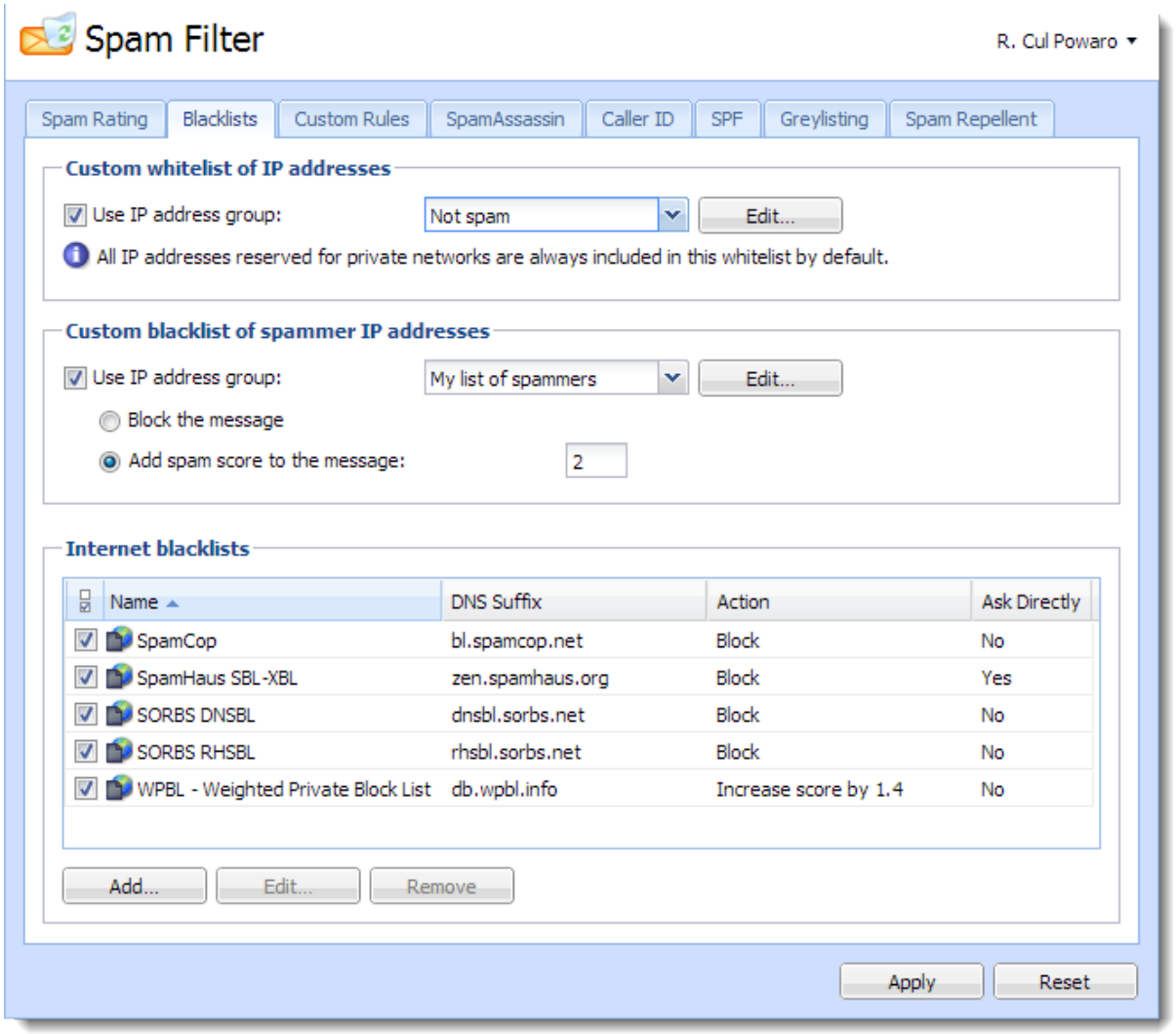


Figure 1 Blacklists tab

Blocking messages from spam servers — Custom blacklists

To create your own blacklists you first need the IP addresses of the servers you want to block

1. Go to In section **Configuration** → **Definition** → **IP Address Groups** and create a new group with IP addresses of spam servers.
2. Go to **Configuration** → **Content Filter** → **Spam Filter** → **Blacklists**.
3. In the **Custom blacklist of spammer IP addresses** section, select the option **Use IP address group**.
4. Select or create a group of IP addresses to block from the drop-down menu.
5. Select the option corresponding the action you want performed when messages arrive that meet your criteria:
    - Block the messages (this marks them as spam)
    - Add spam score to the message
6. Click **Apply** in the bottom right corner.

Blocking messages from spam servers — Public databases

By default, Kerio Connect contains a few databases that can be downloaded from the Internet for free. It is also possible to define other databases.

To use blacklists from **public databases**:

1. Go to section **Configuration** → **Content Filter** → **Spam Filter** → **Blacklists**.
2. In the **Internet blacklists** section, select all the public databases you want to use.
3. Double-click a blacklist and select the option corresponding to the action you want performed when messages arrive that meet the blacklist's criteria:
    - Block the messages (this marks them as spam)
    - Add spam score to the message
4. Click **Apply** in the bottom right corner.

You can also add **other blacklists** from the Internet:

1. In the same section, click **Add**.
2. Type the DNS name of the server that handles the of Kerio Connect enquires.

3. Select the option corresponding to the action you want performed when messages arrive that meet the blacklist's criteria:
    - Block the messages (this marks them as spam)
    - Add spam score to the message
4. Click **Apply** in the bottom right corner.

Once you have set up your blacklists, you can change any of them by double-clicking it.

 If you use a paid blacklist, always select the option **Ask blacklist DNS server directly**. The licenses are associated with a particular IP address, and queries are sent directly to the database, not to parent DNS servers.

Allowing messages from trusted servers — Custom whitelists

Messages from servers included in your whitelist will not be checked by spam filters in Kerio Connect.

To create your own whitelist:

1. Go to **Configuration** → **Definition** → **IP Address Groups** and create a new group with the IP addresses of trusted servers.
2. Go to **Configuration** → **Content Filter** → **Spam Filter** → **Blacklists**.
3. In the **Custom whitelist of IP addresses** section, select the option **Use IP address group**.
4. Select the group of IP addresses from the drop-down menu.
5. Confirm your settings.

Configuring Caller ID and SPF in Kerio Connect

Overview

Caller ID and SPF (Sender Policy Framework) allow you to filter out messages with fake sender addresses.

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.

You can use Caller ID and SPF only if messages are delivered by the SMTP protocol.

Configuring Caller ID

To configure Caller ID in Kerio Connect:

1. In the administration interface, go to **Configuration** → **Content Filter** → **Spam filter** → **Caller ID.**
2. Enable the option **Check Caller ID of every incoming message**.
3. If a message is intercepted, Kerio Connect can
    - Log it in the Security log
    - Reject it
    - Increase/decrease its spam score
4. Caller ID is often used by domains in testing mode only. We recommend that you enable **Apply this policy also to testing Caller ID records**.
5. If messages are sent through a backup server, create a group of IP addresses of those servers that will not be checked by Caller ID.
6. Confirm your settings.

Kerio Technologies enables you to check your own DNS records. The link **Check my email policy DNS records** in this same tab will display a website where you can do that. Learn more about crating SPF and Caller ID records.

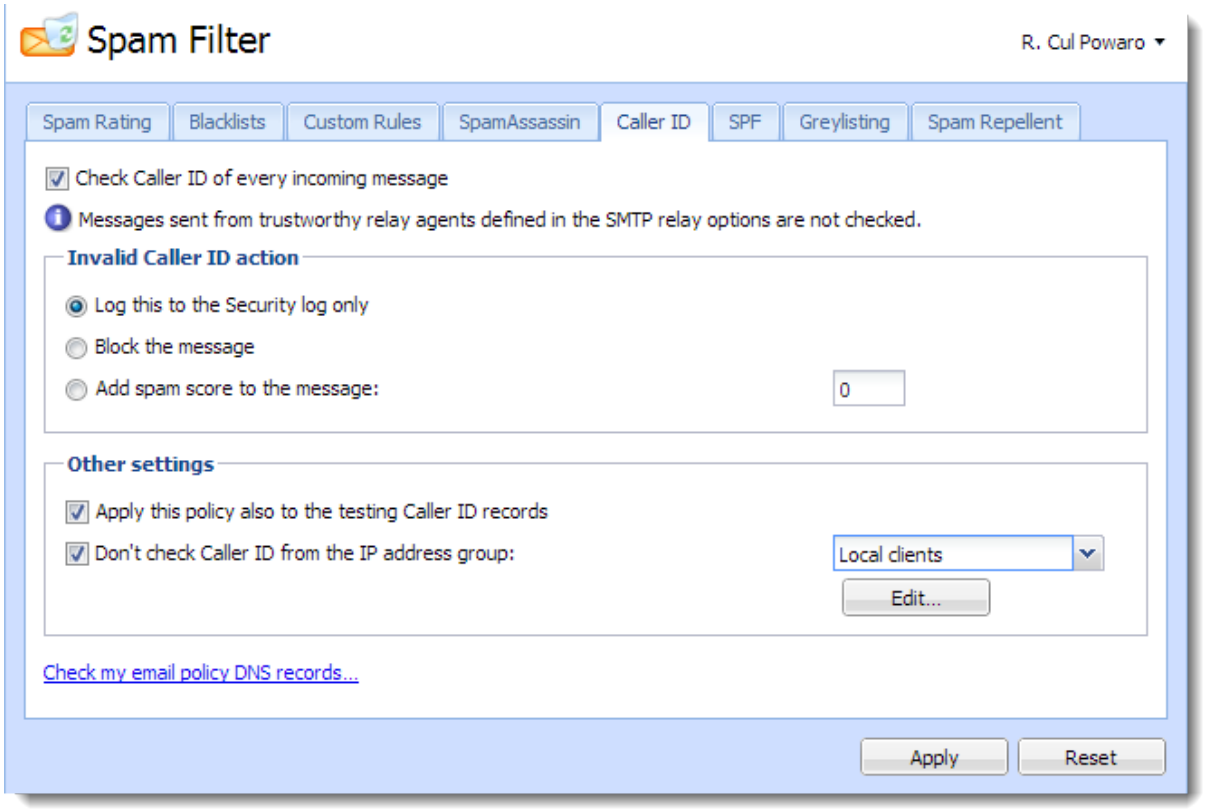


Figure 1 Caller ID

Configuring SPF

To configure SPF in Kerio Connect:

1. In the administration interface, go to **Configuration** → **Content Filter** → **Spam filter** → **SPF.**
2. Enable the option **Enable SPF check of every incoming message**.
3. If a message is intercepted, Kerio Connect can
   - Log it in the Security log
   - Reject it
   - Increase/decrease its spam score
4. If messages are sent through backup server, create a group of IP addresses of those servers that will not be checked by SPF.
5. Confirm your settings.

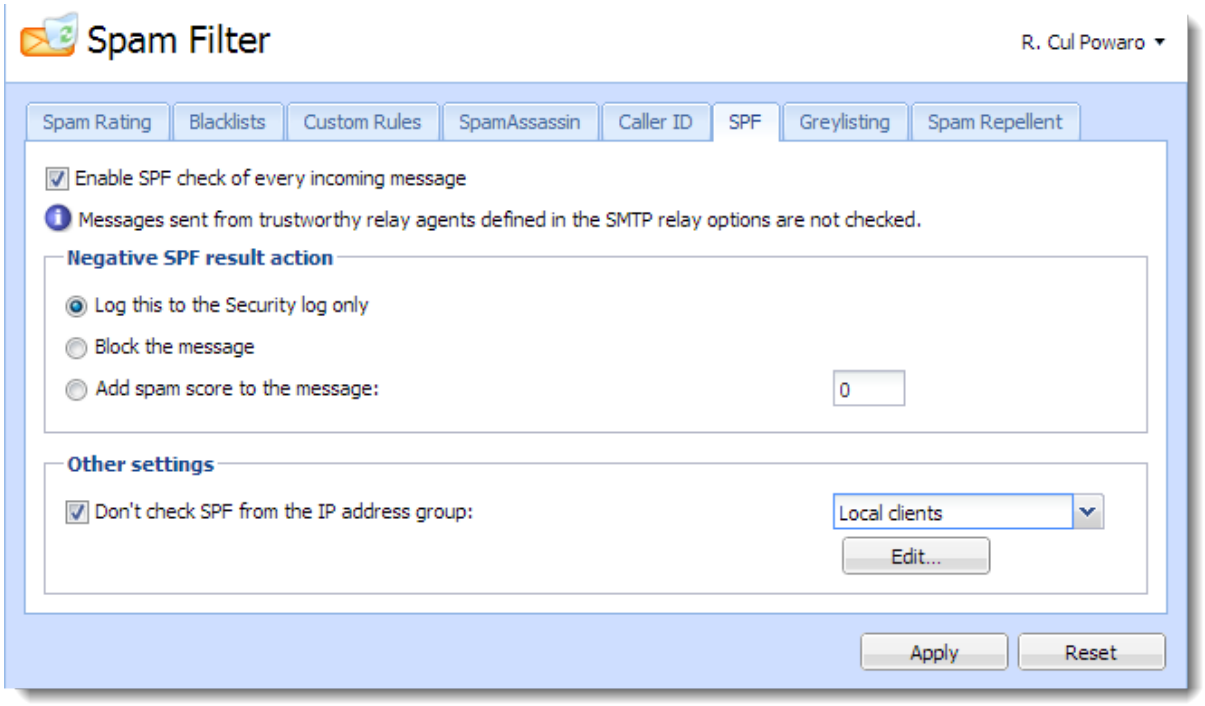

Spam Filter
R. Cul Powaro
Spam Rating
Blacklists
Custom Rules
SpamAssassin
Caller ID
SPF
Greylisting
Spam Repellent
Enable SPF check of every incoming message
Messages sent from trustworthy relay agents defined in the SMTP relay options are not checked.
Negative SPF result action
Log this to the Security log only
Block the message
Add spam score to the message:
0
Other settings
Don't check SPF from the IP address group:
Local clients
Edit...
Apply
Reset

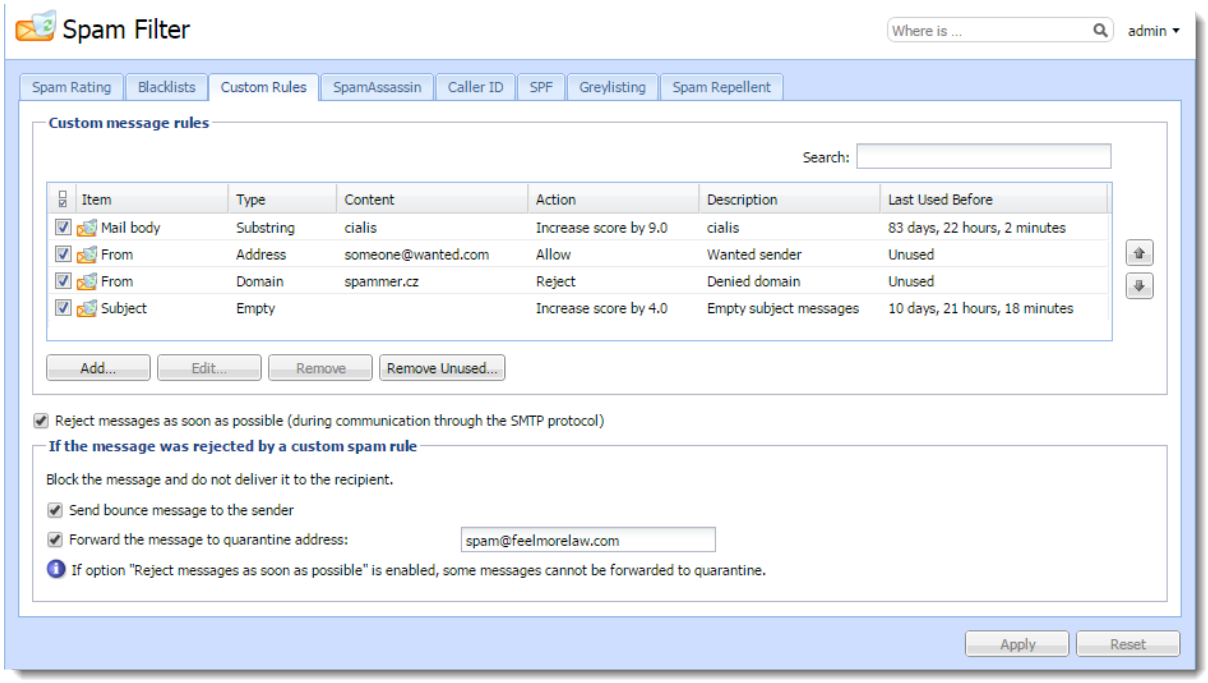
Figure 2 SPF

Creating custom rules for spam control in Kerio Connect

Overview

In Kerio Connect, you can create your own antispam rules. The rules filter email headers or email bodies.

You can create custom rules for spam control by using **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules**.



Creating custom rules

You can create as many rules as you like.

1. In the administration interface, go to **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules**.
2. Click **Add**.
3. In the **Add Rule** dialog, type a name for the rule.
4. Select **Mail header** or **Mail body** filter.

5. Type the string you want to filter.

   You can use:

   - Any text
   - `*` to represent any number of characters
   - `?` to represent a single character
   - Regular expressions (mail body only)

6. For any message that matches the rule, you can:

   - Treat the message as non-spam
   - Treat the message as spam and reject it
   - Add spam score to the message

7. Click **OK**.

Kerio Connect processes the rules in the order they are listed. If the spam filter marks a messages as non-spam or rejects it, Kerio Connect stops processing the remaining rules.

 To decrease the load on your server, place the `From` and `To` header rules at the top. If Kerio Connect rejects messages using this rule, no other antispam or antivirus tests are performed on these messages.

Example for regular expressions

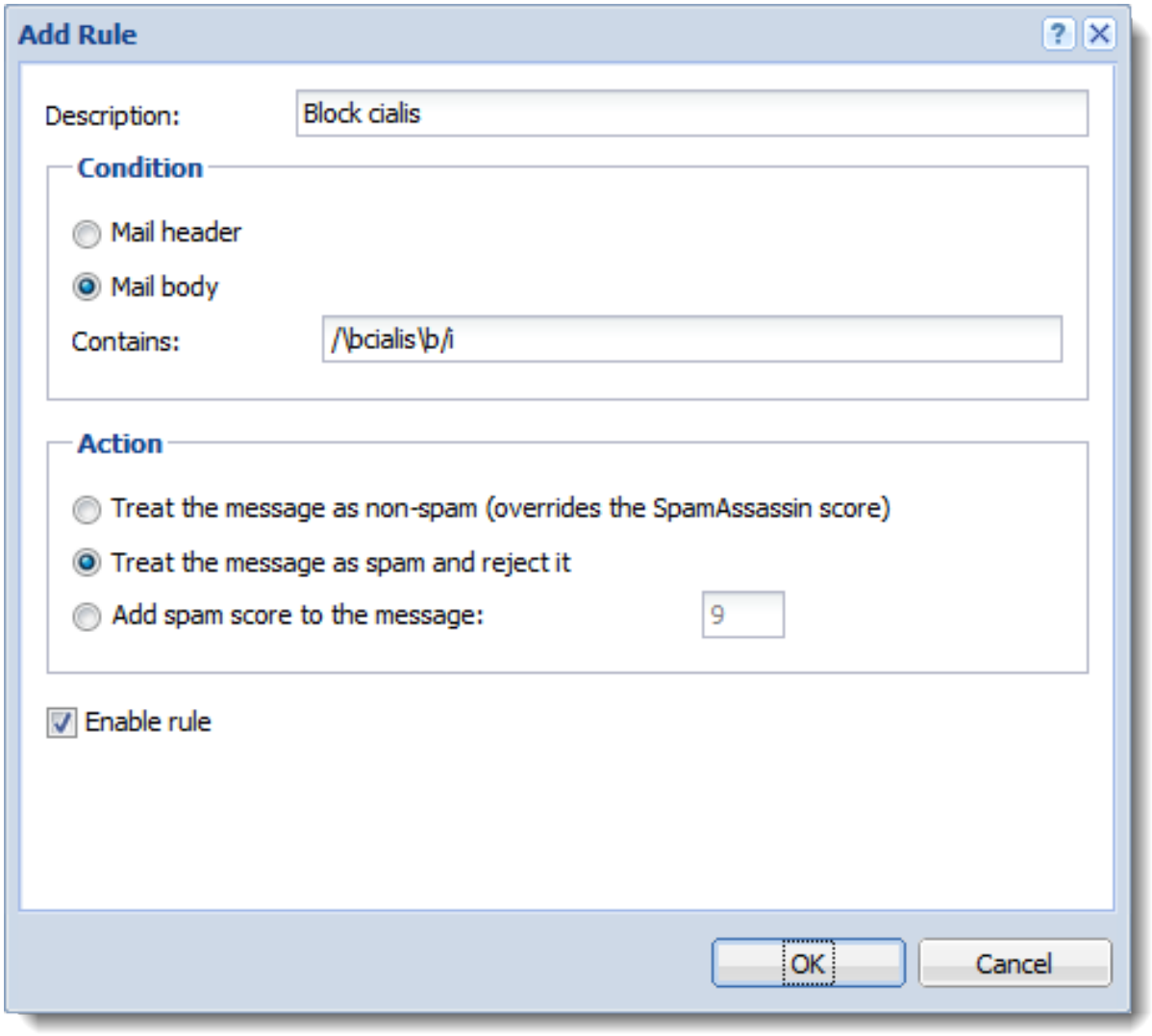
You want to block all messages that contain the word `cialis`.

Use regular expressions to exclude words containing the substring “cialis”, such as specialist, socialist.

1. In **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules**, click **Add**.
2. Select **Mail body** and type the following regular expression:

   ```
   /\bcialis\b/i
   ```

3. Select **Treat the message as spam and reject it**.
4. Click **OK**.



From now on, all messages that include “cialis” as a single word are rejected.

For detailed information on regular expressions, see the SpamAssassin wiki page.

Defining actions for custom rules

To decrease the load on the server, Kerio Connect can reject messages during the SMTP session. However, if you select the **Reject messages as soon as possible...** option, Kerio Connect cannot perform the two actions described below.

If your custom rule rejects a message, Kerio Connect can:

- Send a bounce message to the sender — We do not recommend this option because spammers usually fake addresses, so your bounce message will be undeliverable.
- Forward the message to a quarantine address — We recommend this option so that important messages are not falsely identified as spam.

Antivirus control in Kerio Connect

Overview

Kerio Connect can check all incoming messages for viruses.

Immediately after Kerio Connect is installed, the internal Sophos antivirus automatically starts working.

Sophos antivirus is an optional component and is not available for unregistered trial versions. See Licenses in Kerio Connect.

External antivirus

Kerio Technologies issued an **Antivirus SDK for Kerio Connect and Kerio Control**. The Antivirus SDK includes a public API that you can use to write plugins for third-party antivirus solutions.

Read Using external antivirus with Kerio products and this Kerio Blog post for detailed information.

Configuring Sophos in Kerio Connect

To configure the integrated Sophos:

1. In the administration interface, go to **Configuration** → **Content Filter** → **Antivirus**.
2. Select the option **Use the integrated Sophos antivirus engine**.
3. To update the virus database automatically, select **Check for update every [hours]**.

   Kerio Connect downloads the database files via the HTTP protocol. You must provide a persistent connection and allow the communication on your firewall or proxy server.
4.

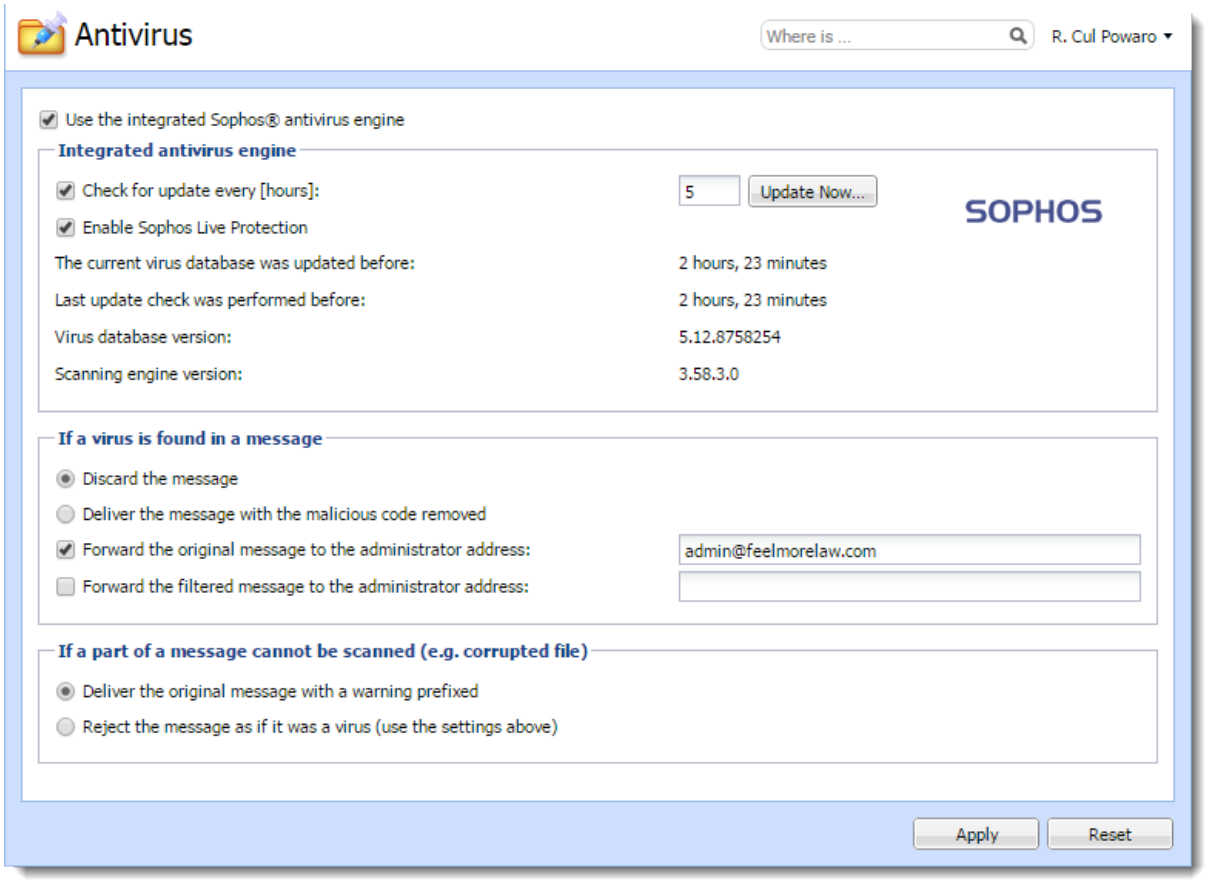
   New in Kerio Connect 8.4.2!

   To allow Kerio Connect to contact Sophos servers for the antivirus check, select **Enable Sophos Live Protection**.

This option ensures that the antivirus software performs this check against an always up-to-date cloud database before Kerio Connect downloads the database with the regular update.

 Kerio Connect sends only a one-way hash of the attachments to the Sophos servers.

5. For any message that contains a virus, Kerio Connect can do either of the following. Select the option you prefer:
   - **Discard the message**
   - **Deliver the message with the malicious code removed**
6. In addition, you can choose from two options for forwarding messages:
   - **Forward the original message to an administrator address**
   - **Forward the filtered message to an administrator address**
7. For any message that Sophos cannot scan, you can choose to have Kerio Connect do one of the following:
   - **Deliver the original message with a warning prefixed**
   - **Reject the message as if it was a virus**
8. Click **Apply**.



Configuring the HTTP proxy server

If the computer with Kerio Connect is behind a firewall, you can use a proxy server to check for virus database updates.

1. Go to **Configuration** → **Advanced Options** → **HTTP Proxy**.
2. Select the option **Use HTTP proxy for antivirus updates,...**
3. Type the address and port of the proxy server.
4. If the proxy server requires authentications, select **Proxy server requires authentication**.
5. Type the user name and password.
6. Click **Apply**.

Go to **Configuration** → **Content Filter** → **Antivirus** and click **Update Now** to check the connection.

Filtering message attachments

For information on scanning message attachments, read Filtering message attachments in Kerio Connect.

Troubleshooting

To view the statistics for Kerio Connect antivirus control, go to **Status** → **Statistics**. This section displays the number of messages checked, viruses detected, and prohibited attachments.

You can also consult the following logs:

- Security: For information on virus database updates, check the Security log.
- Debug — Right-click the Debug log area and enable **Messages** → **Antivirus Checking**

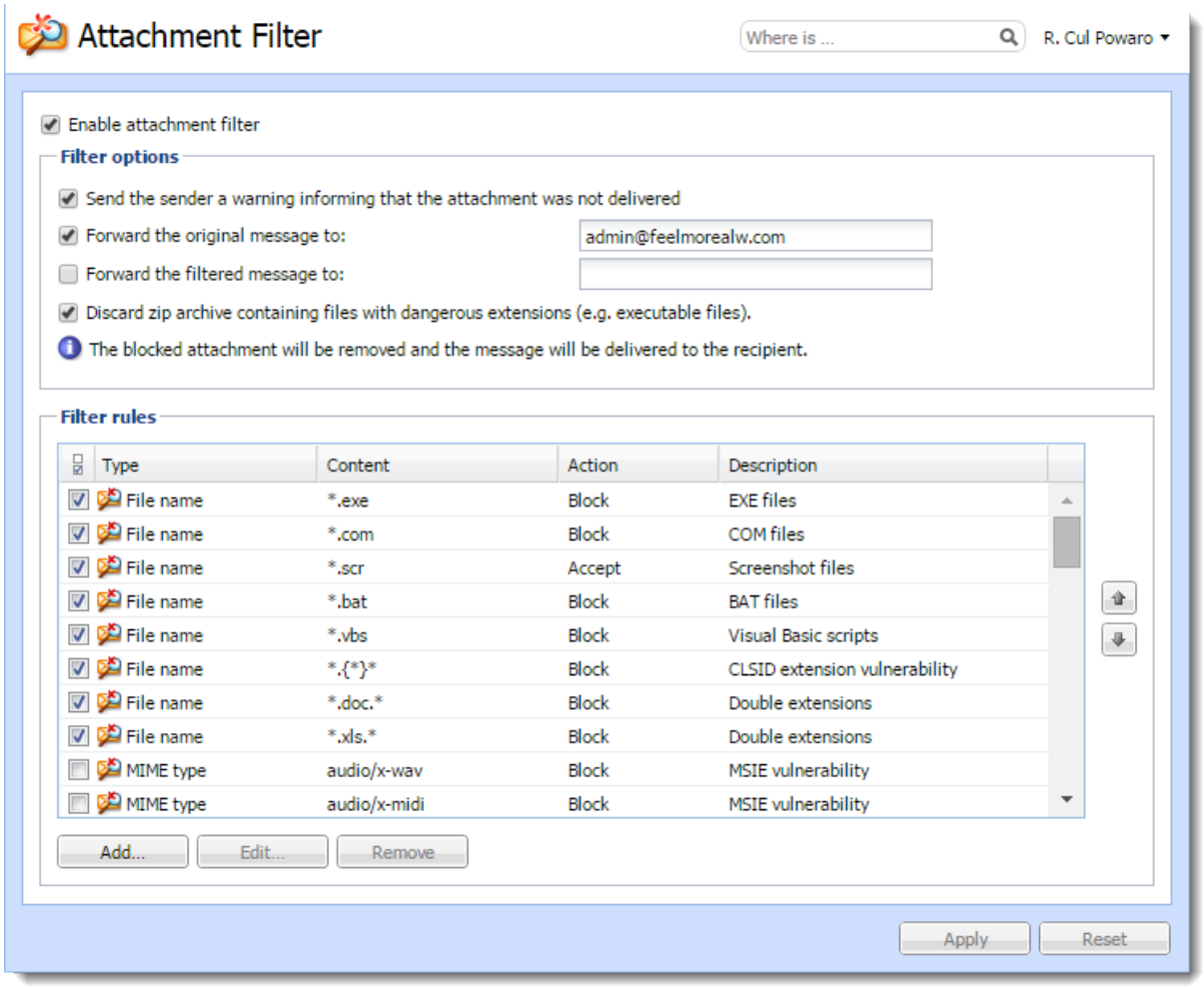
If the time from the last update is several times greater than the interval set, update the database manually and check the Error and Security logs.

Filtering message attachments in Kerio Connect

Overview

Many viruses are hidden as email message attachments. As part of its antivirus control, Kerio Connect can filter email attachments according to your settings.

If Kerio Connect detects a problematic attachment, it removes the attachment and delivers the message without it.



Configuring the attachment filter

To configure attachment filtering:

1. In the administration interface, go to **Configuration** → **Content Filter** → **Attachment Filter**.
2. Select the option **Enable attachment filter**.
3. If you want Kerio Connect to notify the sender that their attachment was not delivered, select the option **Send the sender a warning**.
4. To have Kerio Connect send the original messages to a different email address, select the option **Forward the original messages to** and type the address.
5. To have Kerio Connect send the filtered messages to a different email address, select the option **Forward the filtered messages to** and type the address.
6.

   New in Kerio Connect 8.5!

   To discard the `ZIP` attachments with dangerous files, select the **Discard zip archive containing files with dangerous extensions...** option.
7. Select any of the predefined filter rules.

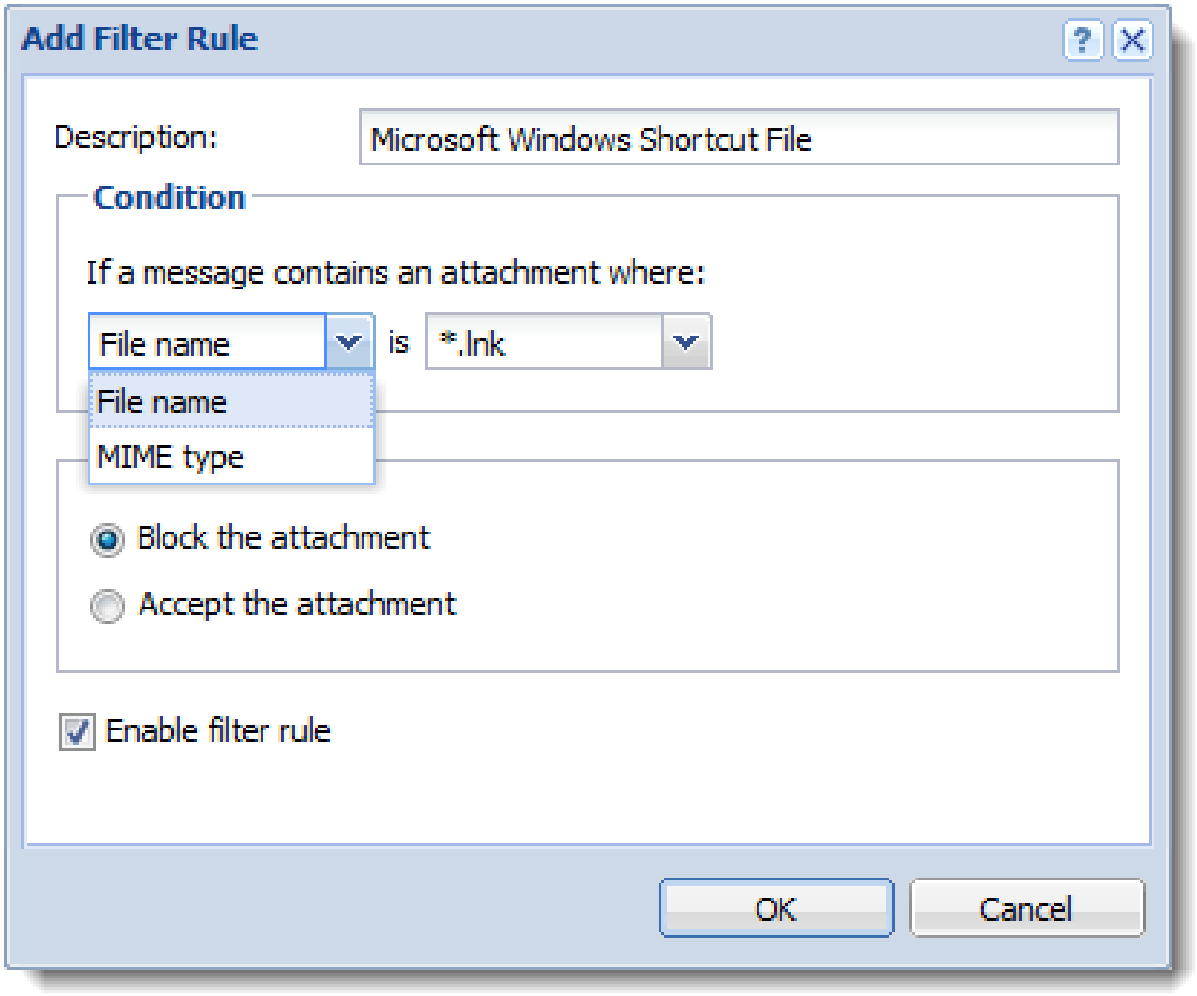
   Each rule can allow or block one specific type of attachment.
8. Click **Apply**.

Now when a problematic attachment is detected, Kerio Connect removes it and delivers the message without the attachment.

Creating custom attachment filter rules

To customize your filter rules:

1. In the section **Configuration** → **Content Filter** → **Attachment Filter**, click **Add**.
2. Type a description for the new rule.
3. Define the condition for the attachments.
4. Select whether Kerio Connect blocks or accepts messages with this type of attachment.
5. Click **OK**.



Troubleshooting

For details on attachment filtering in your Kerio Connect, consult the Security log.

Using external antivirus with Kerio products

Antivirus SDK for Kerio products

Kerio Connect and Kerio Control feature only the integrated Sophos antivirus.

However, Kerio Technologies has issued an **Antivirus SDK for Kerio Connect and Kerio Control**. The Antivirus SDK includes a public API that can be used to write plugins for third-party antivirus solutions.

Get the SDK and read our blog to get detailed information.

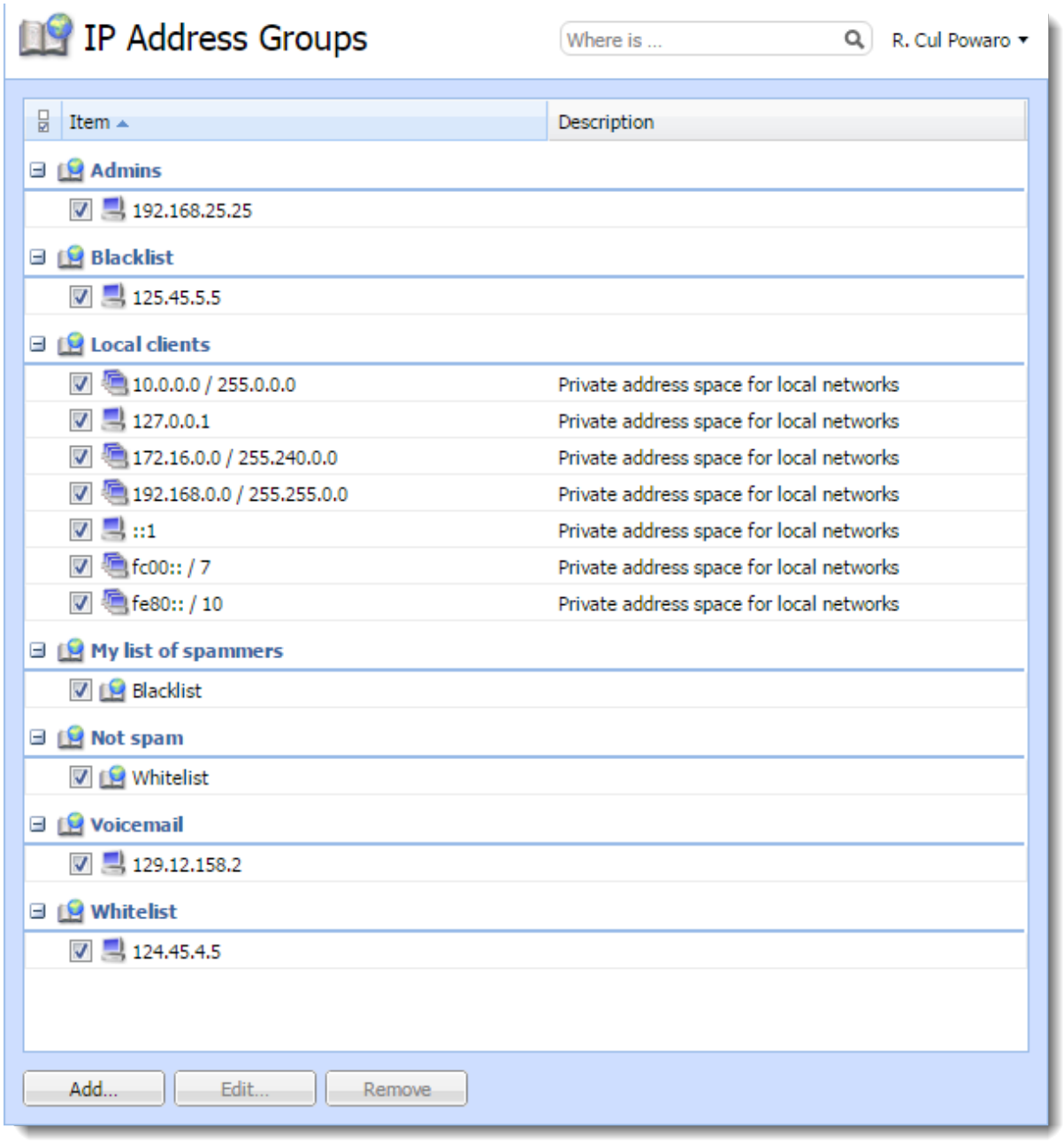
Configuring IP address groups

Overview

 Kerio Connect 9 and newer supports **IPv6**!

IP address groups help easily define who has access, for example, to:

- Remote administration
- Kerio Connect services
- Spam (creating whitelist, blacklists, and so on)



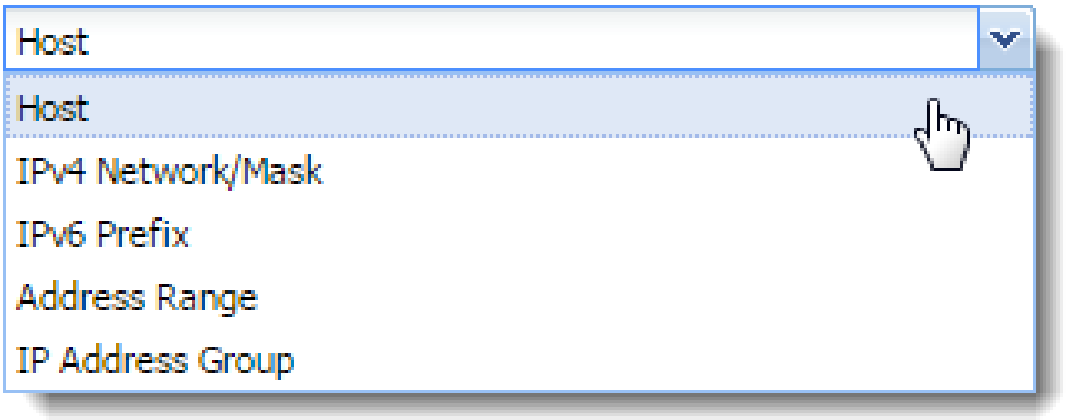
You can use IP address groups in many settings in Kerio Connect. Whenever a section in the administration interface allows IP groups, you can configure them directly from this section.

Configuring IP address group

Kerio Connect automatically creates a default group of local IP addresses. You can edit and remove this group anytime.

1. In the administration interface, go to the **Configuration** → **Definitions** → **IP Address Groups** section.
2. Click**Add**
3. To create a new IP address group, select **Create new**.

   To add IP addresses to an existing group, select the IP address group in **Select existing**.
4. Select the type and specify the IP address.



5. Add a description for better reference.
6. Click **OK**.

Creating time ranges in Kerio Connect

What are time ranges

All scheduled tasks in Kerio Connect can be restricted to certain time ranges.

A time range may consist of multiple intervals with different settings.

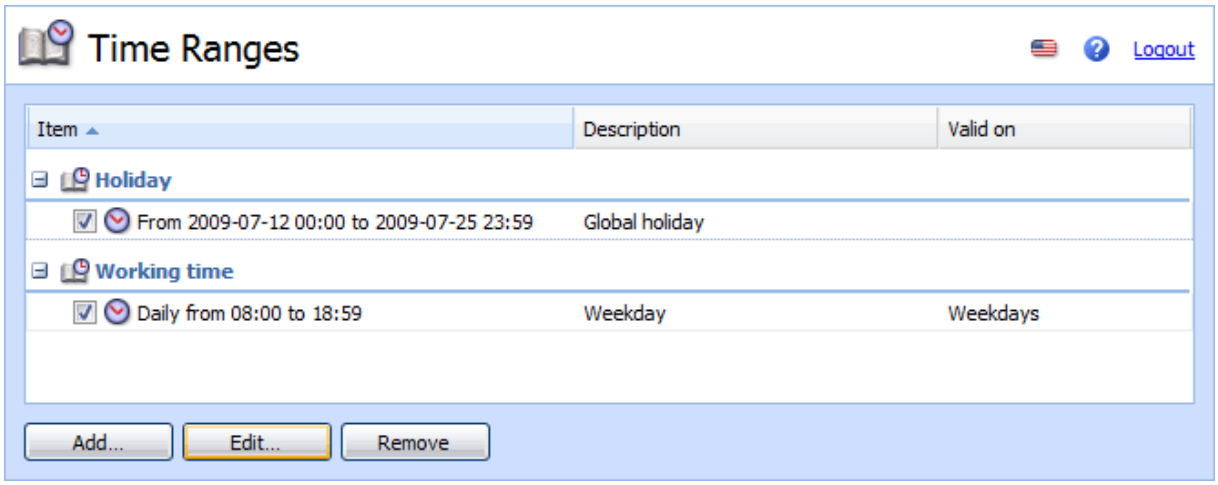


Figure 1 Time ranges

Creating time ranges

1. In the administration interface, go to section **Configuration** → **Definitions** → **Time Ranges**.
2. Click **Add** and
   - create a new group of time intervals, or
   - create an interval in an existing group
3. Add a description for better reference.
4. Configure the **Time settings** — frequency, time interval and days if applicable.
5. Confirm.

Filtering messages on the server

Overview

New in Kerio Connect 9!

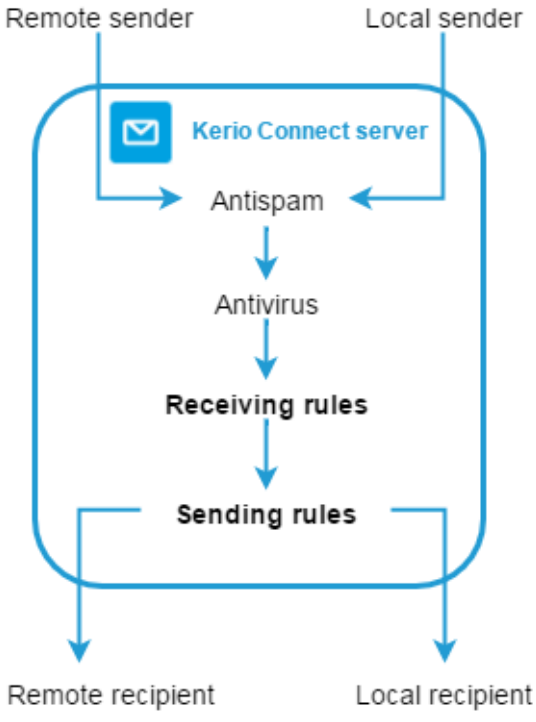
Users can filter messages in their mailbox with Kerio Connect Client filters. Administrators can apply message filters directly on the Kerio Connect server.

For example, you can:

- Forward messages sent to a former employee to another mailbox
- Send an auto-reply to messages sent to a particular email address or even a domain
- Add recipients to specific messages
- Reject messages with large attachments

Kerio Connect applies **Receiving rules** to all recipients in the message. In the **Sending rules**, messages are considered separately for each recipient.

You can see the order how Kerio Connect processes the rules:



You can find specific examples below.

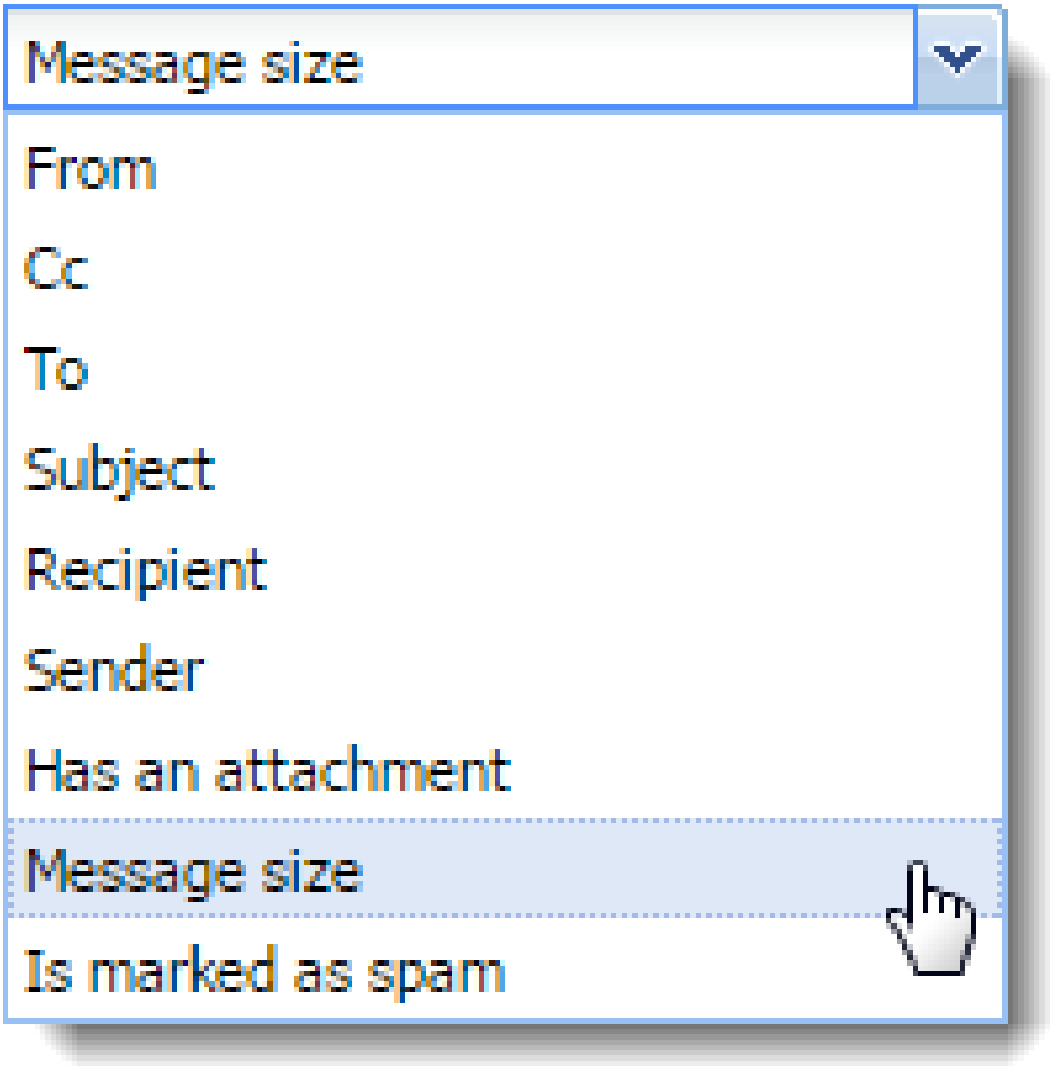
Creating receiving rules

Kerio Connect applies receiving rules to all messages that come to the server from local or remote senders.

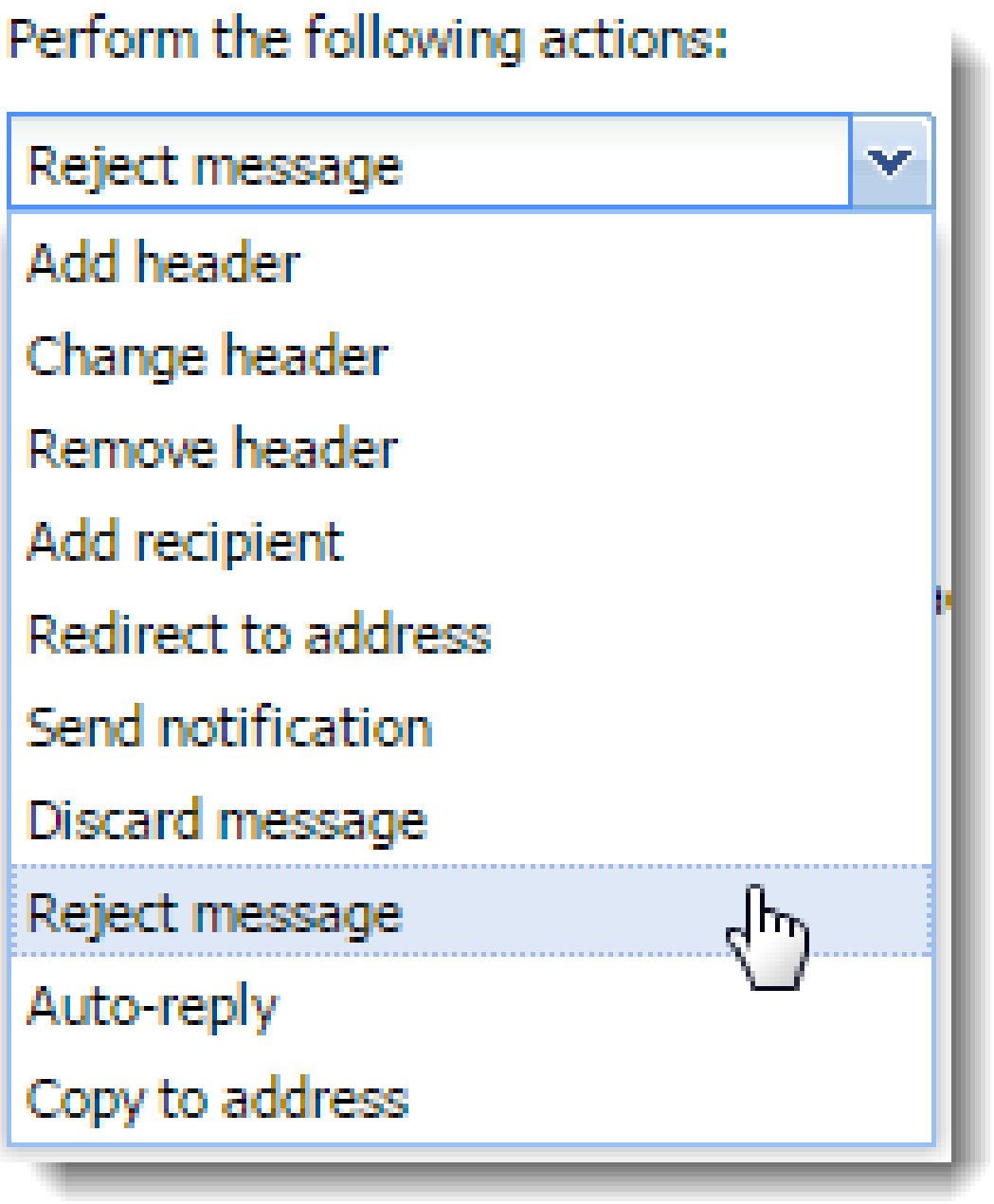
These rules are applied before the outgoing rules and before the user filters in Kerio Connect Client.

1. In the administration interface, go to **Configuration** → **Content Filter** → **Message Filters**.
2. In the **Receiving rules** section, click **Add**.
3. In the description field, type a name for the filter.
4. Specify the conditions for the filter.

   Use a comma (,), or a semi-colon (;) to separate multiple items. Regular expressions and the ? / * placeholders are not supported.



5. Specify the actions.

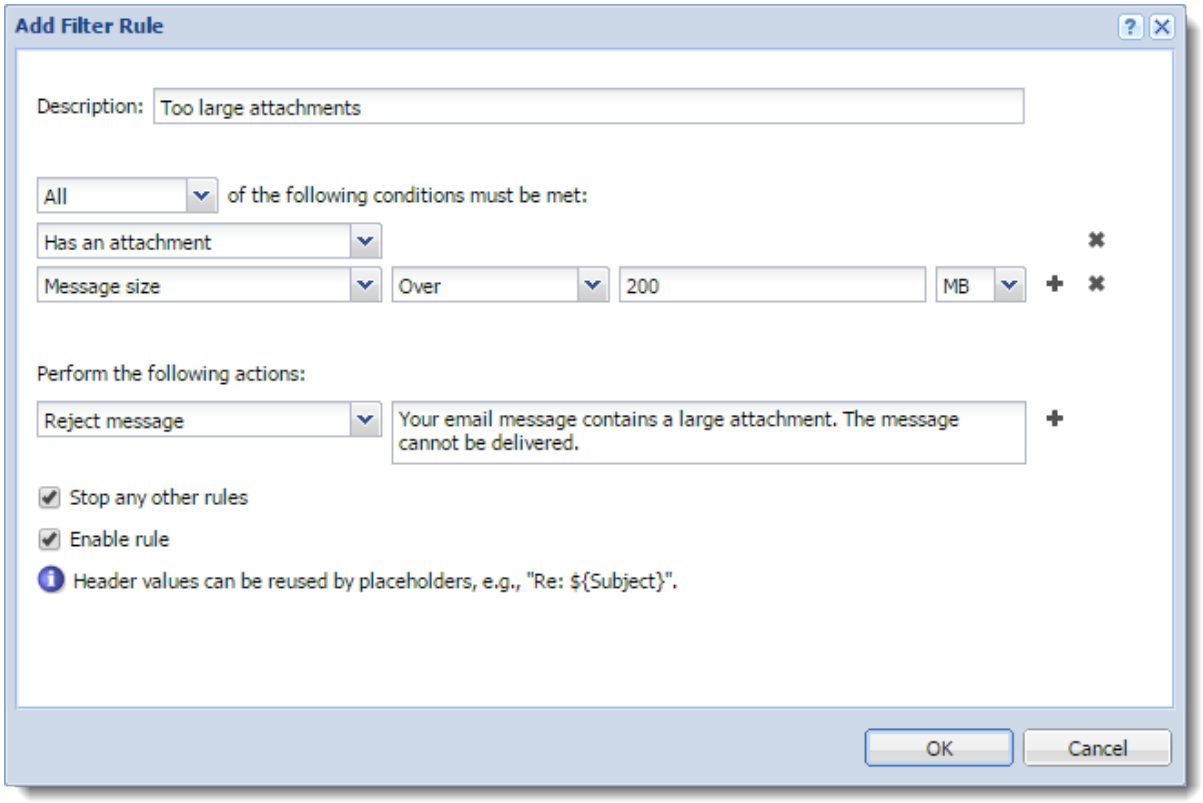


6. (Optional) Select the **Stop any other rules** option.

   The rules are processed from the top. If the message matches the rule, no other rules are processed.

7. Click **OK**.

8. Click **Apply**.



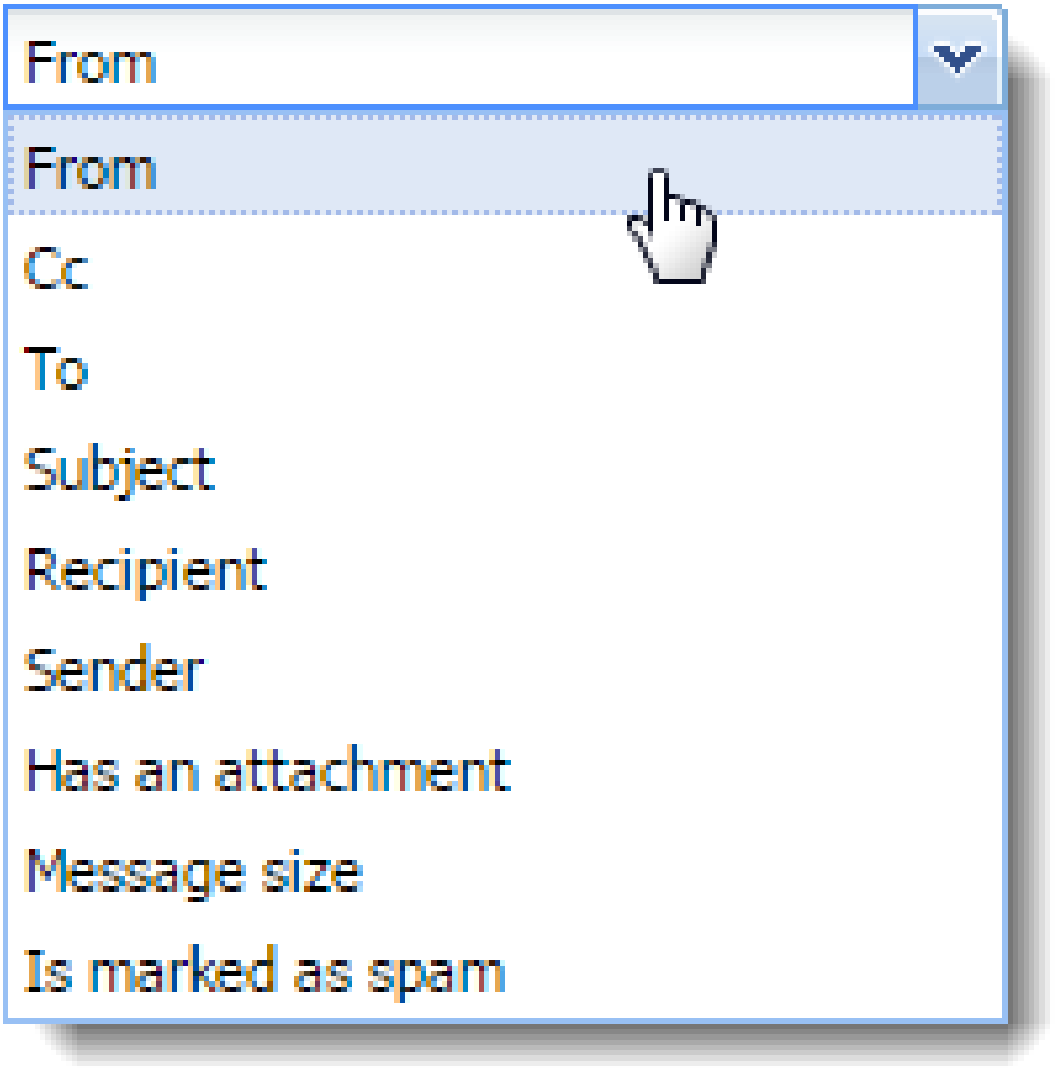
Creating outgoing rules

Kerio Connect applies outgoing rules to all messages that leave the server and are sent to local or remote recipients.

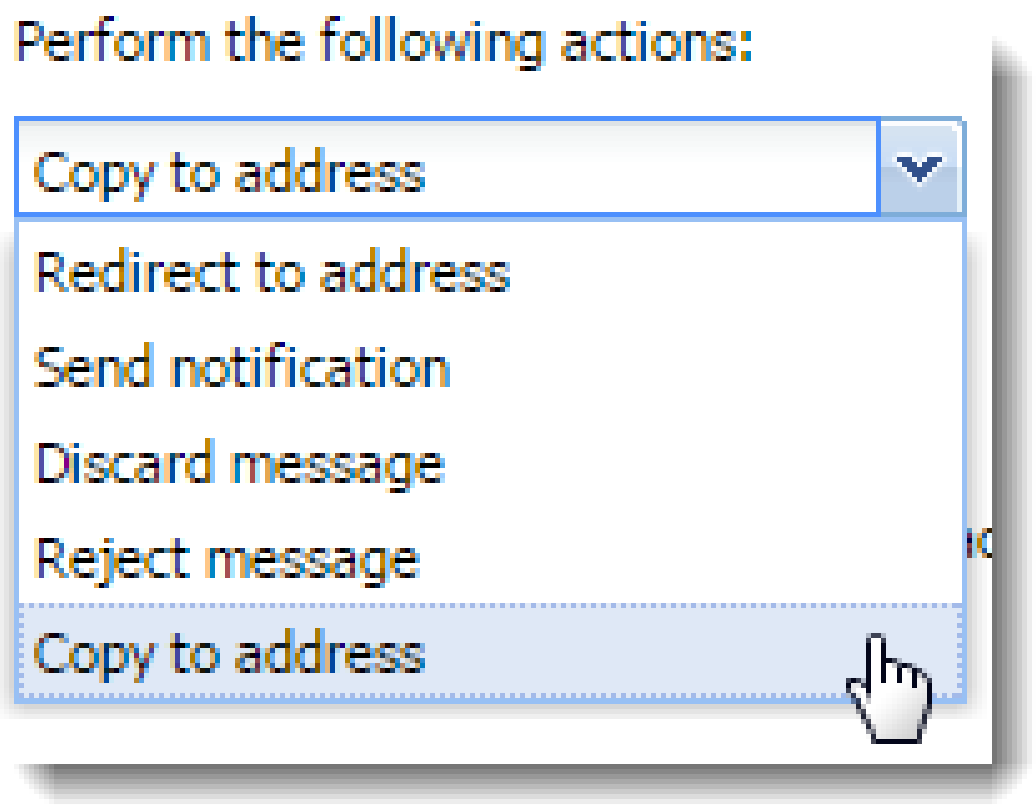
These rules are applied after the receiving rules and before the user filters in Kerio Connect Client.

1. In the administration interface, go to **Configuration** → **Content Filter** → **Message Filters**.
2. In the **Sending rules** section, click **Add**.
3. In the description field, type a name for the filter.
4. Specify the conditions for the filter.

   Use a comma (,), or a semi-colon (;) to separate multiple items. Regular expressions and the ? / * placeholders are not supported.



5. Specify the actions.

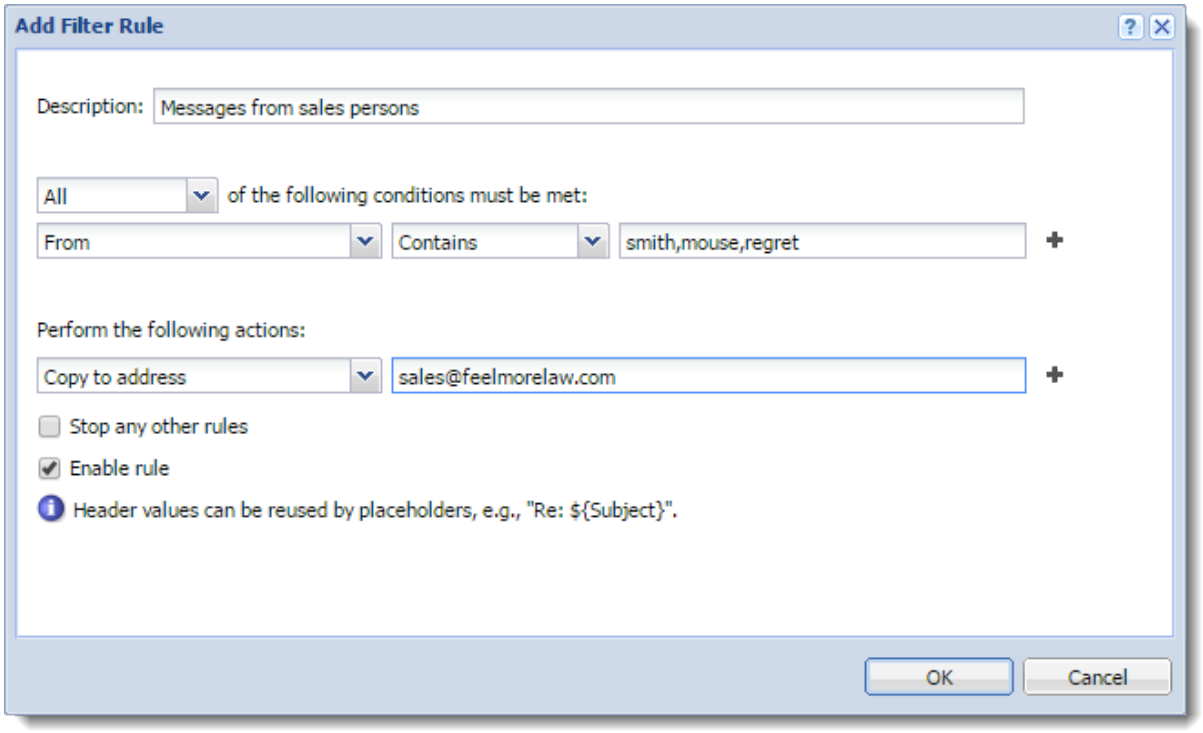


6. (Optional) Select the **Stop any other rules** option.

   The rules are processed from the top. If the message matches the rule, no other rules are processed.

7. Click **OK**.

8. Click **Apply**.



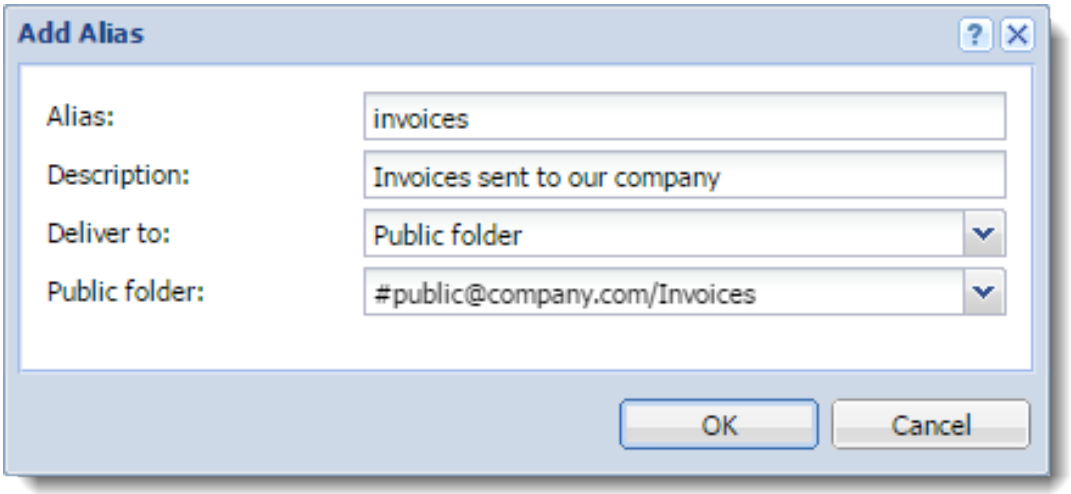
Example 1 - Forwarding messages to public folders

To forward messages to public folders, you must create:

- An alias email address for the public folder
- Server rule for forwarding the messages

You want all messages sent to `accounting@company.com` that include invoices as attachments to be sent to a public folder **Invoices**.

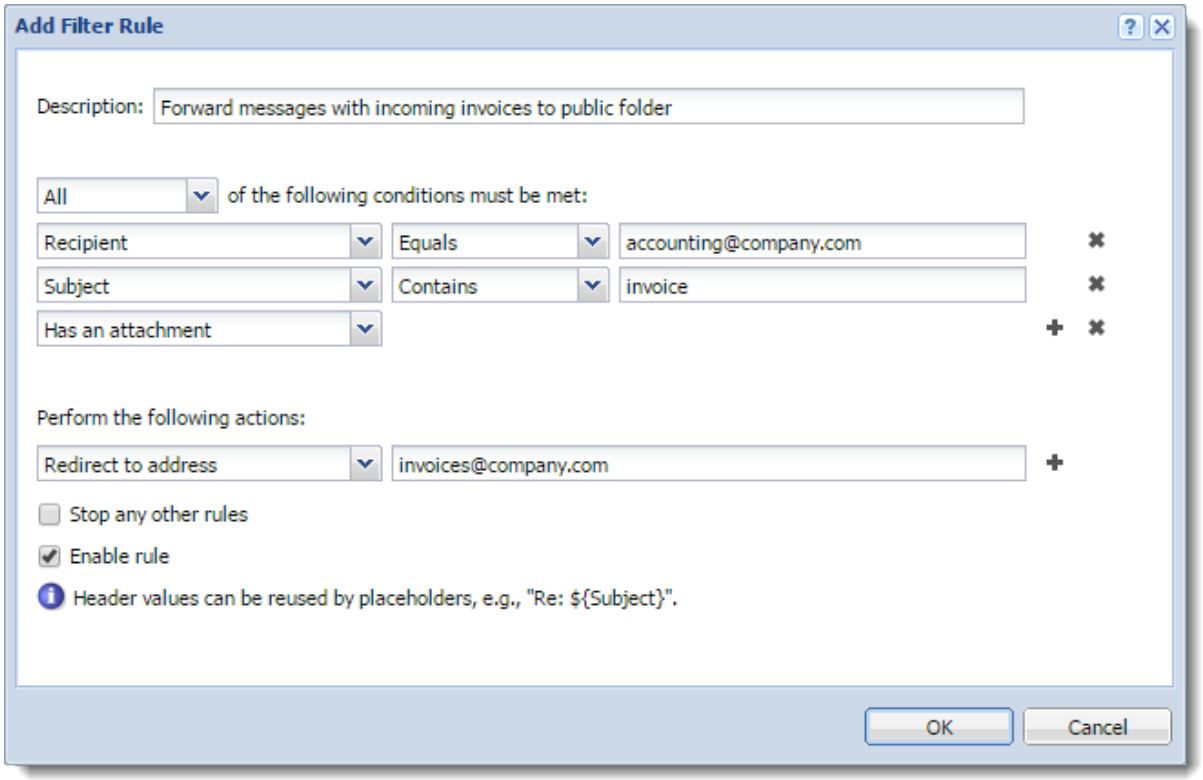
1. In the **Accounts** → **Aliases** section, create an alias that points to a public folder.



2. Go to the **Configuration** → **Content Filter** → **Message Filters** section.
3. In the **Receiving rules** section, click **Add**.
4. Set the condition to **Recipient** → **Equals** → **accounting@company.com**.
5. Click the plus sign to add another condition.
6. Set the condition to **Subject** → **Contains** → **invoice**.
7. Click the plus sign to add another condition.
8. Set the condition to **Has an attachment**.
9. Set the action to **Redirect to address** and type the alias email address of the public folder.

   If you use **Add recipient** or **Copy to address**, Kerio Connect delivers the message to other recipients as well.

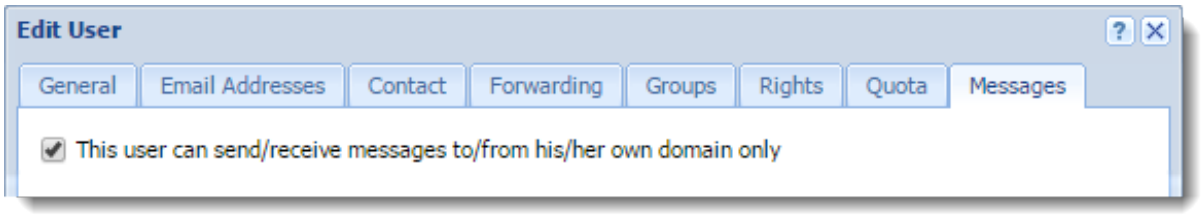
10. Click **OK** and **Apply**.



If you use **Redirect to address**, the message is not delivered to the original recipients, however, the sender receives their delivery receipt if required.

Example 2 - Prohibiting sending messages to remote recipients for individual users

In the settings of each user, you can disable the user to send and receive messages outside their own domain.



With a special server rule you can limit this either to sending or receiving.

You want to disable John Smith (`jsmith@company.com`) to send messages outside his domain (`company.com`). However, he can receive messages from other domains.

1. Verify that the **This user can send/receive messages...** option in the user settings is disabled.
2. Go to the **Configuration** → **Content Filter** → **Message Filters** section.
3. In the **Sending rules** section, click **Add**.
4. Set the condition to **Sender** → **Equals** → **jsmith@company.com**.
5. Click the plus sign to add another condition.
6. Set the condition to **Recipient** → **Does not contain** → **company.com**.
7. Set the action to **Reject message** and type the reason for rejecting that the user receives.
8. Select **Stop any other rules**.
9. Click **OK** and **Apply**.

If the message has multiple recipients and some of them are from the user's domain, Kerio Connect:

- Delivers the message to the recipients from the user's domain
- Rejects to deliver to message to recipients outside the user's domain
  If you create the same rule in the **Receiving rules** section, neither remote nor local recipients get the message.

Example 3 - Sending a copy of a message to another email address

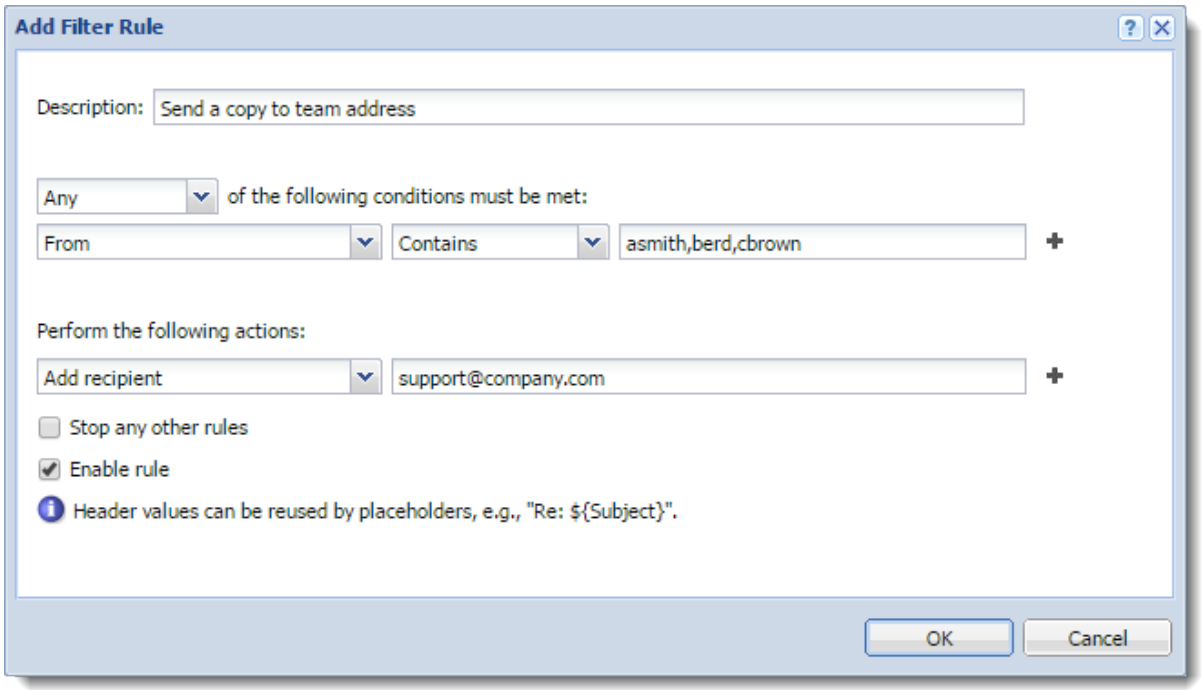
A team of support technicians help customers solve their problems. They communicate via their email addresses:

- `asmith@company.com`
- `berd@company.com`
- `cbrown@company.com`

They also have a team address `support@company.com`.

You want to send a copy of all messages, which they send, to their team address so that the other team members are aware of the current issues

1. In the **Receiving rules** section, click **Add**.
2. Set the condition to **From** → **Contains** → **asmith,berd,cbrown**
3. Set the action to **Add recipient** → **support@company.com**
4. Click **OK** and **Apply**.



You can also use **Copy to address**. Both **Add recipient** and **Copy to address** send a blind copy to the specified address. However, if the message cannot be delivered to that address, the sender gets notification only if you use **Add recipient**.

Example 4 - Rejecting messages with large attachments

You want to prevent your Kerio Connect to be overloaded with large attachments.

You can limit the size of messages with attachments that go through your server:

1. In the **Receiving rules** section, click **Add**.

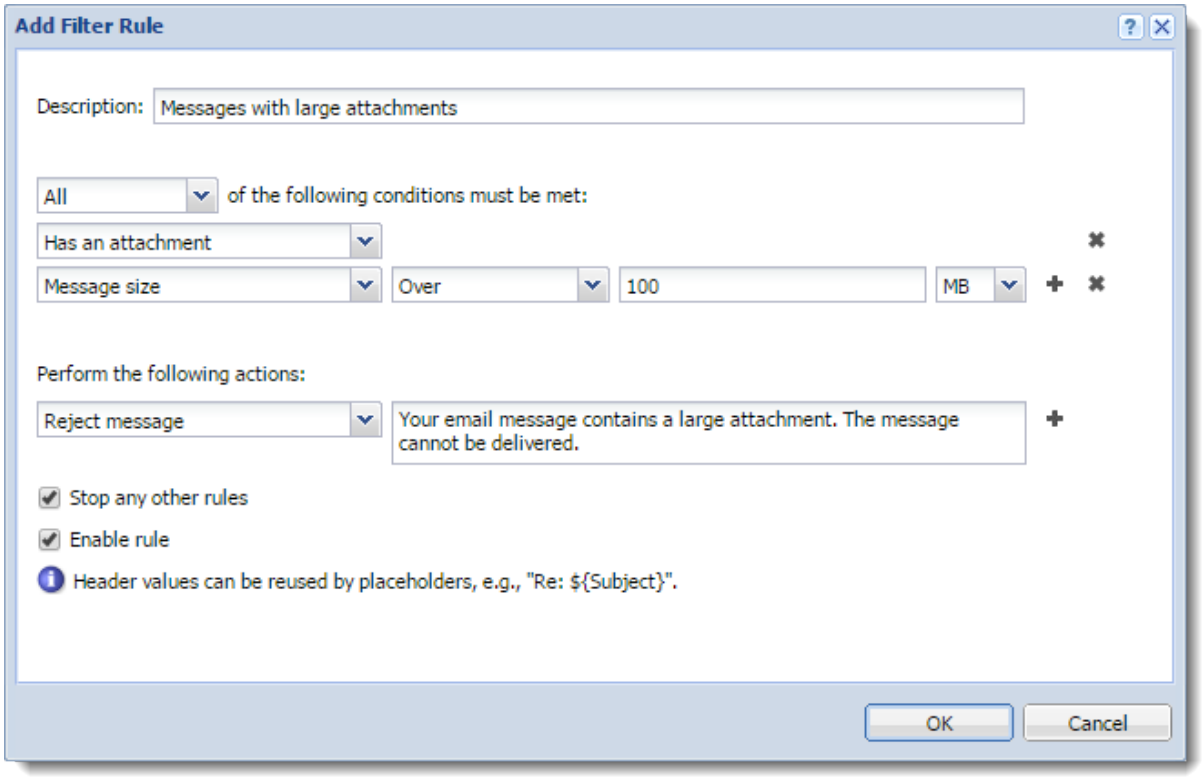
   If you create this rule in **Sending rules**, the Kerio Connect server may get overloaded if the message has many recipients.

2. Select **All** in the drop-down list.
3. Set the condition to **Has an attachment**.
4. Click the plus sign to add another condition.
5. Set the condition to **Message size** → **Over** → **100MB**.
6. Set the action to **Reject message** and type the reason for rejecting that the sender receives.

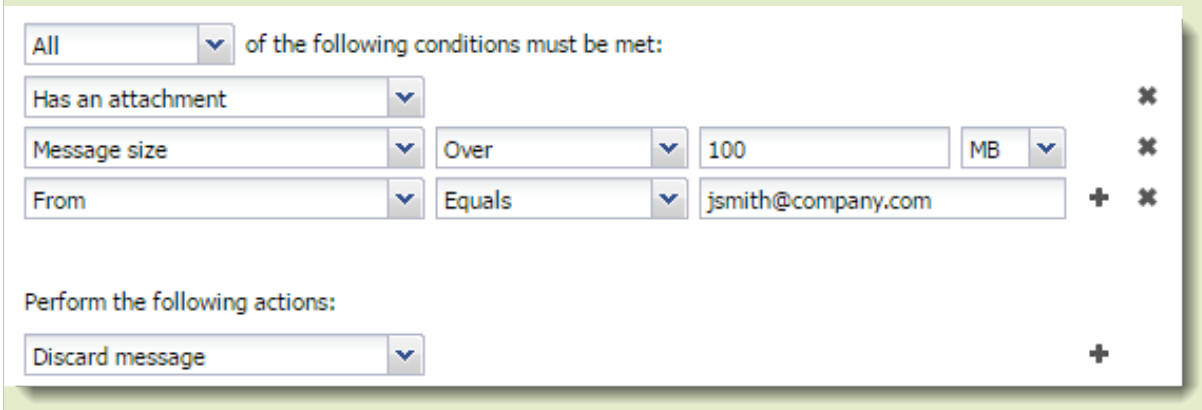
   

   If you select **Discard message**, the sender is not notified.

7. Select **Stop any other rules**.
8. Click **OK** and **Apply**.



To limit large attachments only for specific users, create this rule in the **Sending rules** section and specify recipients.



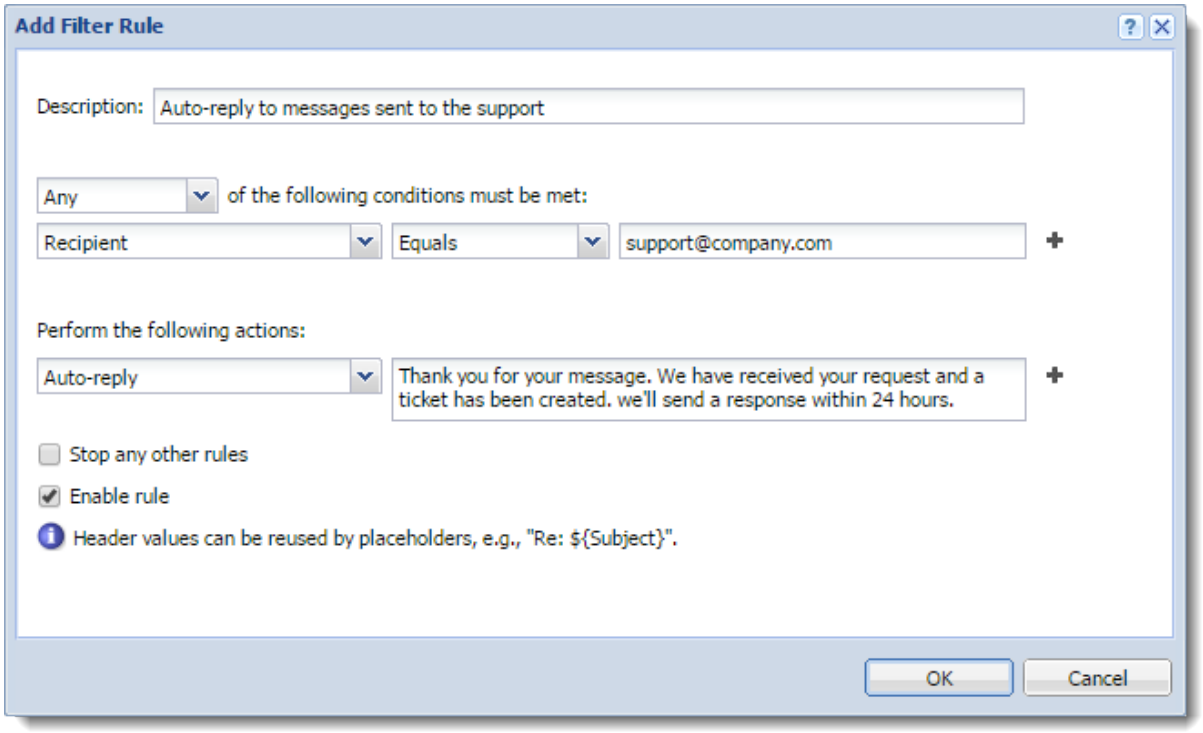
Examples 5 - Sending an auto-reply message

You want to send an automatic reply to each message that Kerio Connect delivers to your support team address.

1. In the **Receiving rules** section, click **Add**.
2. Set the condition to **Recipient** → **Equals** → **support@company.com**.

3. Set the action to **Auto-reply** and type the text.

4. Click **OK** and **Apply**.



Public folders in Kerio Connect

Overview

Public folders are folders available to all users in a domain or the whole server. You can create public folders of these types:

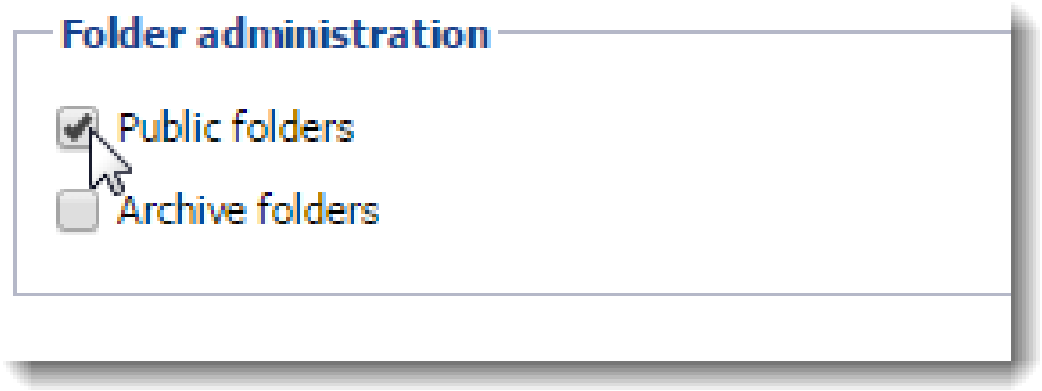
- Mail
- Calendar
- Contacts
- Tasks
- Notes

You can create public folders in Kerio Connect Client or Microsoft Outlook.

Only users with appropriate rights can create and edit public folders (see below).

Assigning administrator rights to manage public folders

1. In the administration interface, go to **Accounts** → **Users**.
2. Double-click a user and go to the**Rights** tab.
3. Select the **Public folders** option.



4. Save the settings.

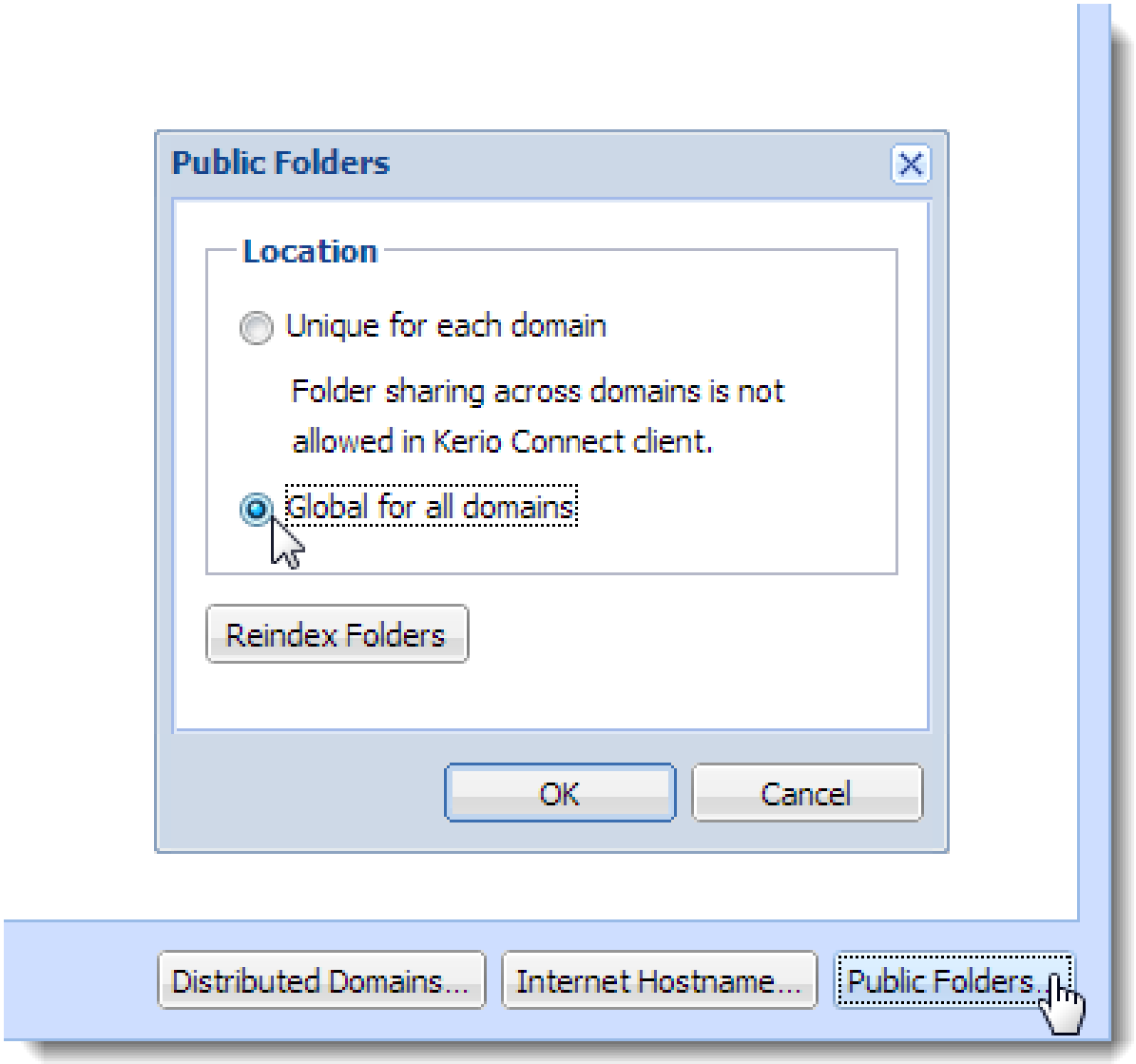
Global vs. domain public folders

In Kerio Connect, public folders can be:

- Different for each domain
- Global for all domains

To select the type of public folders:

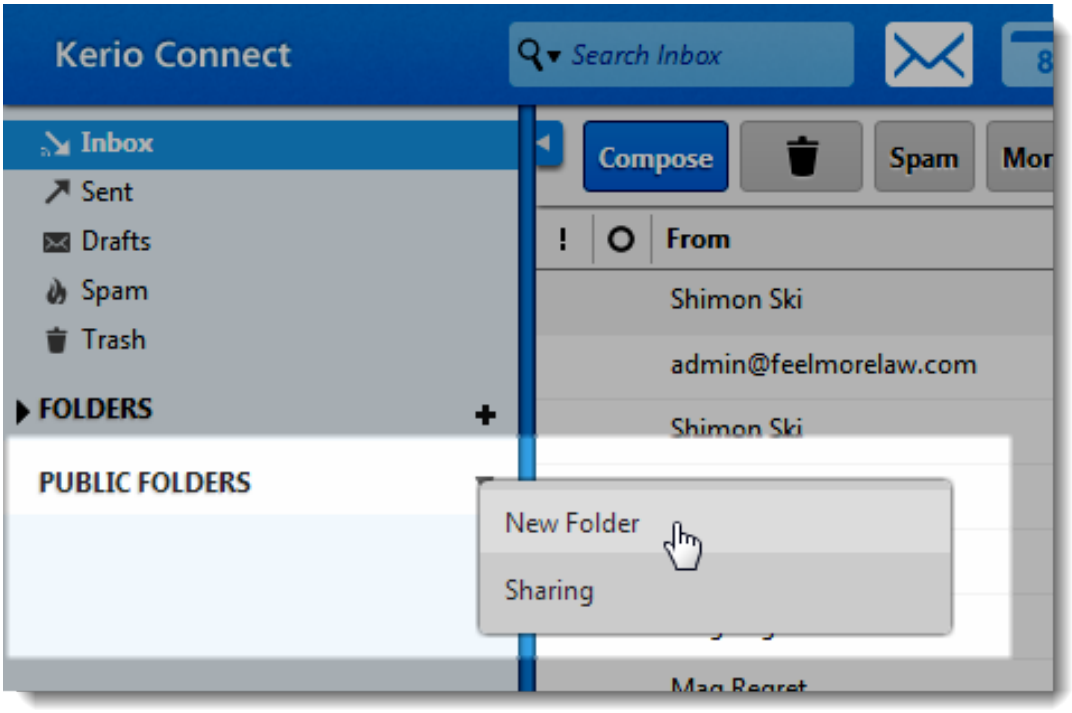
1. Go to the administration interface to the **Configuration** → **Domains** domains.
2. Click the **Public Folders** button in the right bottom corner and select your option.
3. Save your settings.



If you switch the public folder type after public folders has already been created, you must create new public folders — users will not be able to see the old ones.
Read How to change from individual public folders to global public folders and keep your existing public folder data for additional information.

Creating public folders in Kerio Connect Client

1. Go to your Kerio Connect Client.
2. In the left folder tree, right-click **Public folders** and select **New Folder**.



3. Type a name for the public folder.

By default, all users from the domain can view public folders. To change the sharing rights, read article Sharing in Kerio Connect Client.

Microsoft Outlook has a similar procedure.

Viewing public folders

All public folders are automatically displayed in Kerio Connect Client and other clients.

See the following table for detailed information:

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 Connect Client	YES	YES	YES	YES	YES
Microsoft Outlook for Mac 2011	YES	YES	YES	YES	YES
Exchange account in Apple Mail	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

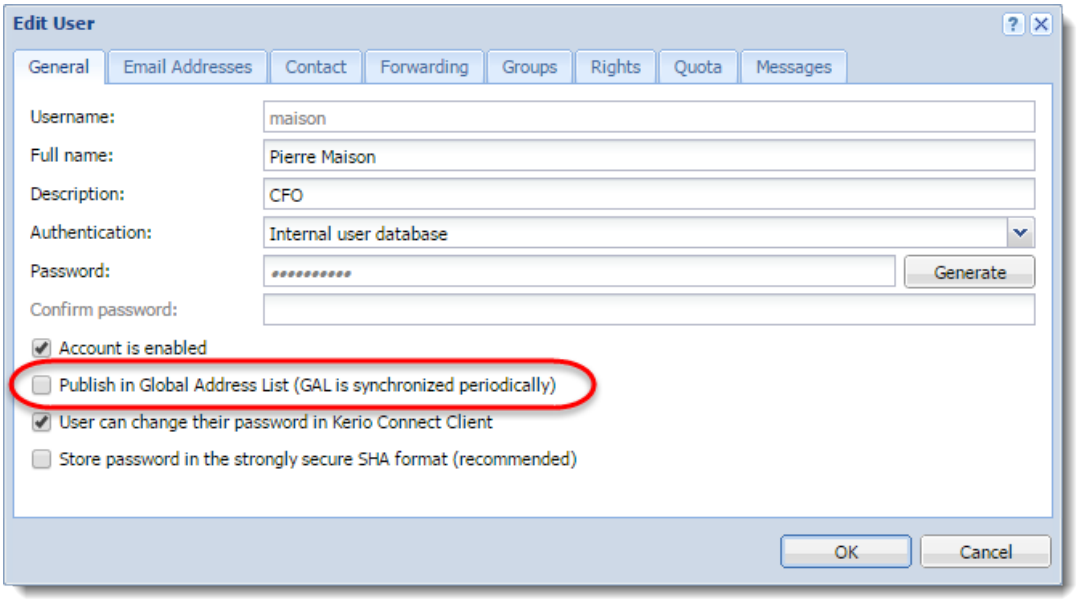
Table 1 Viewing public folders in individual account types

Global Address List

Kerio Connect can automatically add users to a public contacts folder which is used as an internal source of company contacts.

By default, this option is enabled. To disable it for individual users:

1. In the administration interface, go to the **Accounts** → **Users** section.
2. Double-click a user and clear the checkbox for the **Publish in Global Address List** option on the **General** tab.



If users are mapped from Active Directory or Apple Open Directory, the entire LDAP database synchronizes every hour automatically.

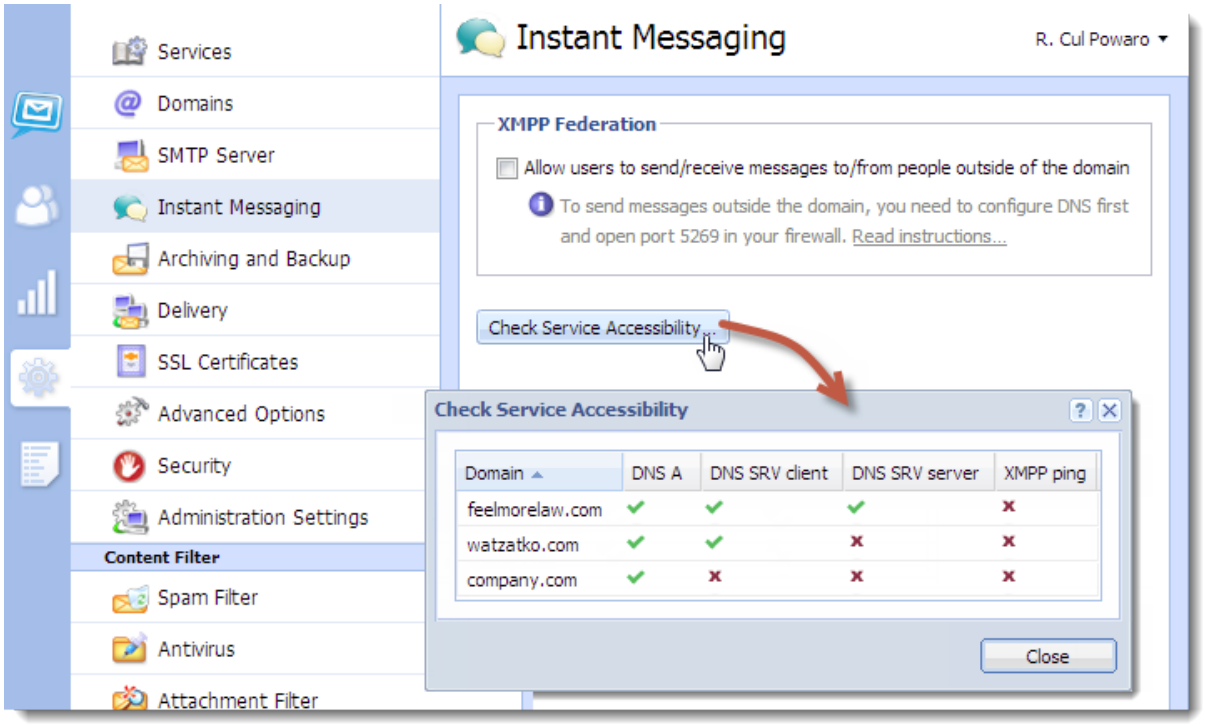
Configuring instant messaging in Kerio Connect

About instant messaging

Kerio instant messaging service is based on XMPP, an open technology for real-time communication.

The instant messaging (IM) service is running in Kerio Connect automatically.

To check if the instant messaging is accessible, click on **Check Service Accessibility** in the administration interface in section **Configuration** → **Instant Messaging**.



Make sure to open the following ports on your firewall (both directions):

- 5222 (IM service)
- 5223 (secured IM service)
- 5269 (if sending outside of your domain is allowed)

DNS records must be configured for your domain. Read article Configuring DNS for instant messaging for more information.

Sending messages outside of your domain

By default, users can send messages only to members of the same domain.

To enable sending/receiving instant messages to/from other domains (either within the Kerio Connect server or outside), follow these steps:

1. In the administration interface, go to section **Configuration** → **Instant Messaging**.
2. Check option **Allow users to send/receive messages to/from people outside of the domain**.
3. Save the settings.
4. **Check Service Accessibility**.

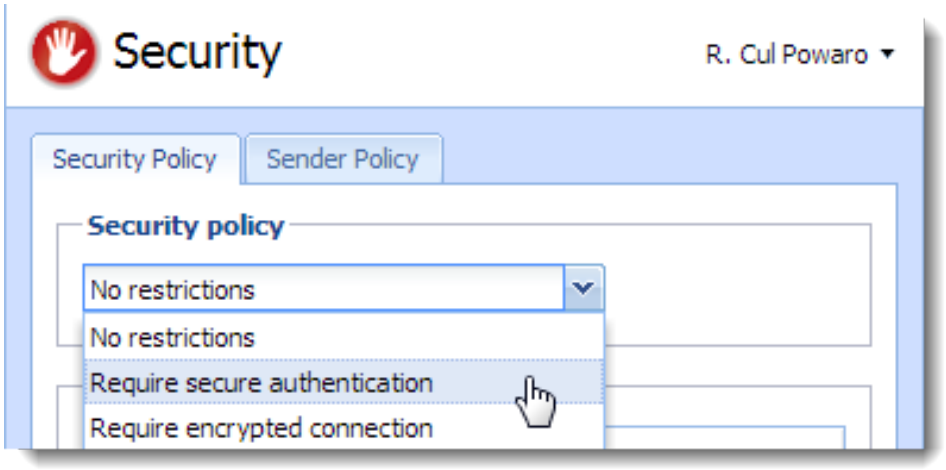
These settings are valid for all domains on the server. You can override them by individual user settings (on tab **Messages**) or group settings (tab **Rights**).

Remember to configure DNS for instant messaging.

Securing instant messaging

We recommend to secure instant messaging by using TLS:

- set security policy to require encrypted connection or secure authentication in section **Configuration** → **Security** → **tab Security Policy** (**Configuration** → **Advanced Options** → **tab Security Policy** for Kerio Connect 8.1 and older)



- use unsecured instant messaging service (port 5222)

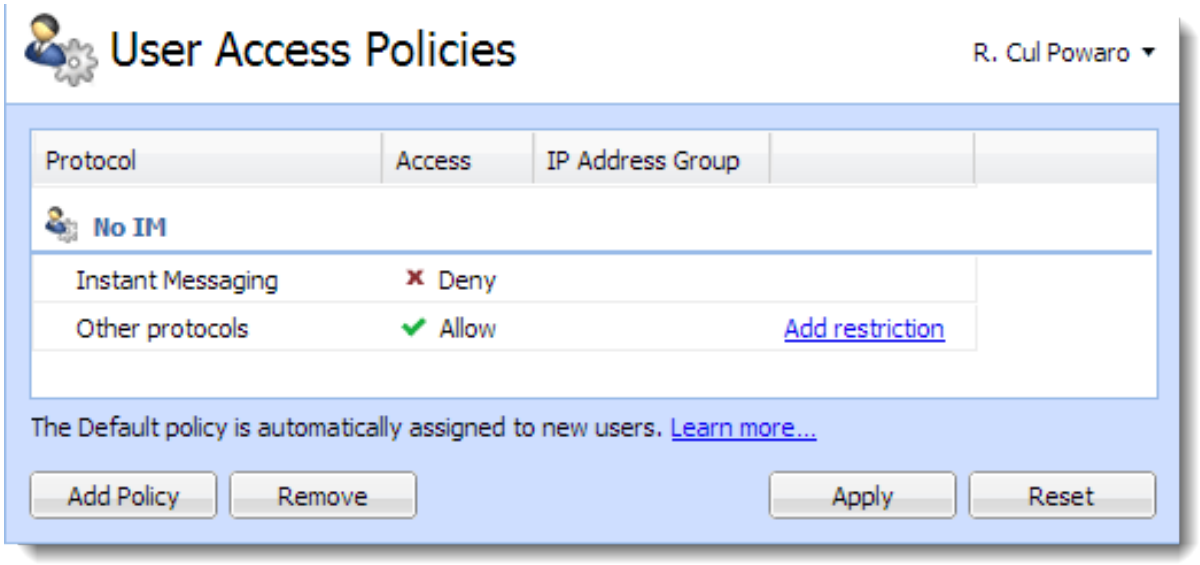
You can also enable only the secure instant messaging service (port 5223) and use SSL.

Security policy is applied to all services in your Kerio Connect.

Limiting access to instant messaging

If you need to restrict access to any users, you can define User Access Policies to:

- disable access to IM
- restrict access IM to specific addresses



To display which users are connected to the IM server, go to section Active Connections in the administration interface.

Disabling instant messaging

You can disable instant messaging by stopping the instant messaging services (see article Services in Kerio Connect).

Archiving instant messages

For information about archiving instant messages, read article Archiving instant messaging.

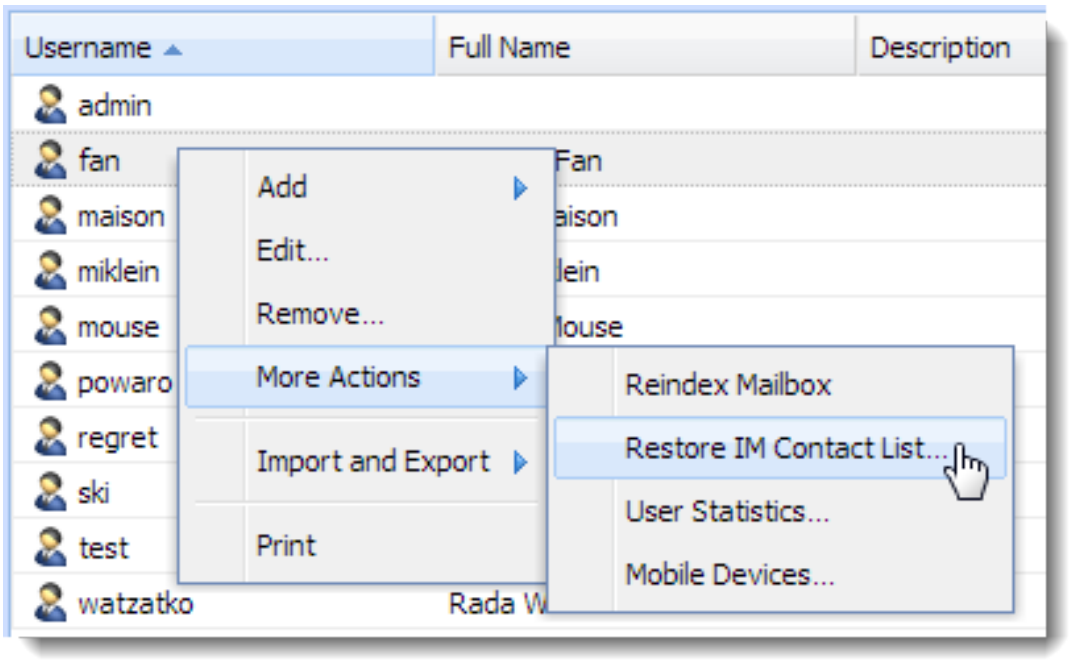
Automatic contact list

Kerio Connect automatically creates contact lists of all domain users who are published in the global address list.

Once users login to an IM client, their account will display list of contacts of users from their domain (**Colleagues**).

If a user is having problems with their contact list (e.g. if they delete any users), you can restore their contact list:

1. In the administration interface, go to section **Accounts** → **Users**.
2. Right-click the user and select **More Actions** → **Restore IM Contact List**.
3. Confirm.



Restoring contact lists discards any changes the user has made to their **Colleagues** list. Added contacts will remain preserved.

Maximum size of the automatic contact list

Maximum number of users in the automatic contact list is set to 300. The users who exceed this number are not included in the **Colleagues** contact list and also their contact list is empty.

To change the maximum size of the contact list:

1. Stop the Kerio Connect engine.
2. Open the `mailserver.cfg` file.
3. Edit the following line:

   ```
   <variable name="RosterMaximum">300</variable>
   ```

   To disable the automatic contact list completely, set the `MaximumRoster` value to 0 (zero).
4. Save the file.
5. Start the Kerio Connect engine.

Kerio Connect saves the information about exceeding the maximum number of users in the Warning log.

The size of the contact list affects the performance of the server. We recommend the following RAM size for the different contact list sizes:

- 0-100 users — 256 MB
- 100-200 users — 384 MB
- 200-500 users — 768 MB
- 500+ users — 2048 MB

Configuring IM clients

For recommended clients and their configuration, read article Configuring clients for instant messaging.

Troubleshooting

If any problem regarding instant messaging occurs, consult the Debug log (right-click the Debug log area and enable **Messages** → **Instant Messaging Server**).

If you rename a domain, users must re-configure their IM clients. All previous changes to their contact list will be lost.

Configuring DNS for instant messaging

About SRV records

SRV (service) records are entries in your DNS which specify the location of service servers. You must configure SRV records to make instant messaging in Kerio Connect accessible from other servers.

There are two types of SRV records:

- xmpp-server — necessary if you enable sending messages outside of your domain
- xmpp-client

Go to the Kerio Connect administration (**Configuration** → **Instant Messaging**) to check if the SRV records for your domain are configured (for detailed information, read article Configuring instant messaging in Kerio Connect).

You must add SRV records on your DNS server or use the management interface of your DNS registrar to add the records.

Visit XMPP wiki or Wikipedia for more information on SRV records.

Configuring DNS records for server to server communication

Follow this example to add a server SRV record to your DNS:

```
_xmpp-server._tcp.feelmorelaw.com. 18000 IN SRV 0 5 5269 connect.feelmorelaw.com.
```

The following items can be changed:

`feelmorelaw.com` — domain

`connect.feelmorelaw.com` — instant messaging server (Kerio Connect)

18000 — TTL

0 — record priority

5 — record weight

Do not change the port number (`5269`).

Configuring DNS records for client auto-configuration

If the name of your domain differs from the name of the instant messaging server, you can add a client SRV record to your DNS.

This record will allow auto-configuration of instant messaging clients. Without the client SRV record, users must manually specify the server and port in their client configuration.

Follow this example to add a client SRV record to your DNS:

```
_xmpp-client._tcp.feelmorelaw.com. 18000 IN SRV 0 5 5222 connect.feelmorelaw.com.
```

The following items can be changed:

`feelmorelaw.com` — domain

`connect.feelmorelaw.com` — instant messaging server (Kerio Connect)

`18000` — TTL

`0` — record priority

`5` — record weight

`5222` — port of the service

Archiving instant messaging

Overview

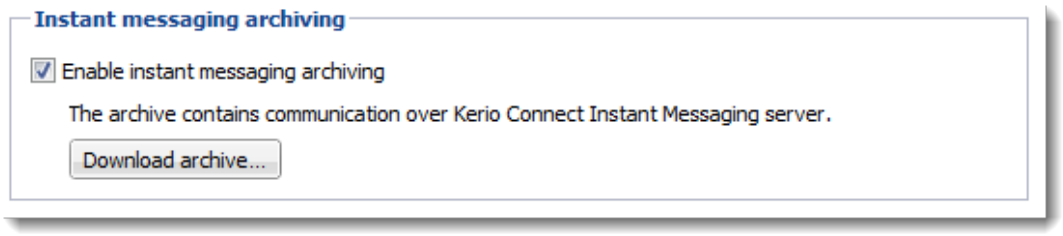
If you want to look at any instant message later, Kerio Connect can archive all instant messages sent to or from your users.

The archived data include:

- local messages and messages sent to and received from outside of their domain
- group chats
- file name and size of all files transferred over instant messaging

Configuring instant messaging archiving

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → **tab Archiving**.
2. Select **Enable instant messaging archiving**.



3. Save the settings.

Archive files

There are three types of archive files — `*.txt` (current archive files), `*.zip` (files which have reached the default file size), `*.part` (temporary archive files).

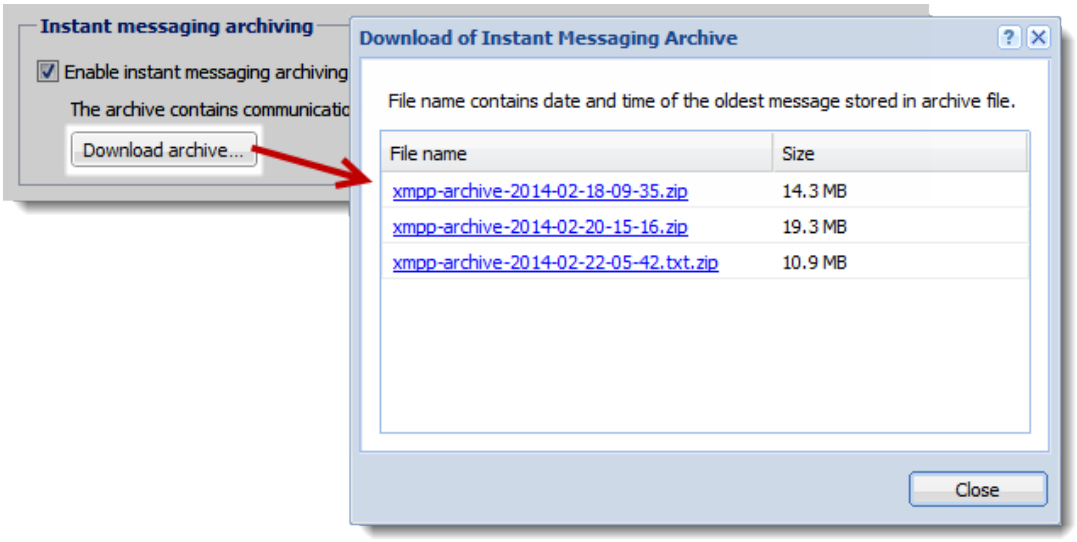
The default maximum size of the archive files is 50 MB. Once the archive file reaches 50 MB, a new file is created.

You can adjust the archive file size in the `mailserver.cfg` file in the installation folder of Kerio Connect (variable = `ArchiveFileSize` .

Accessing the instant messaging archives

To download the instant messaging archive files from the administration interface:

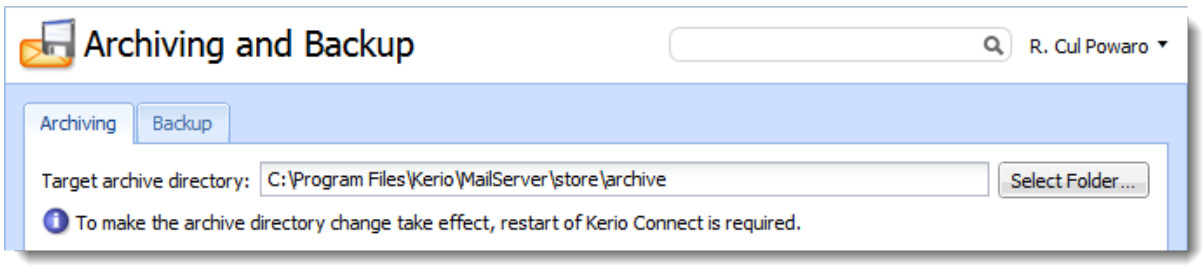
1. Go to **Configuration** → **Archiving and Backup** → **tab Archiving**.
2. In **Instant messaging archiving**, click **Download archive**.



   This opens the list of available archive files. The file name contains the date and time of the first message saved in this file.

3. Click any file name and save the file.

The instant messaging archives are stored in the target archive directory specified in **Configuration** → **Archiving and Backup** → **tab Archiving** in the `xmpp` folder .



Customizing Kerio Connect

About customization

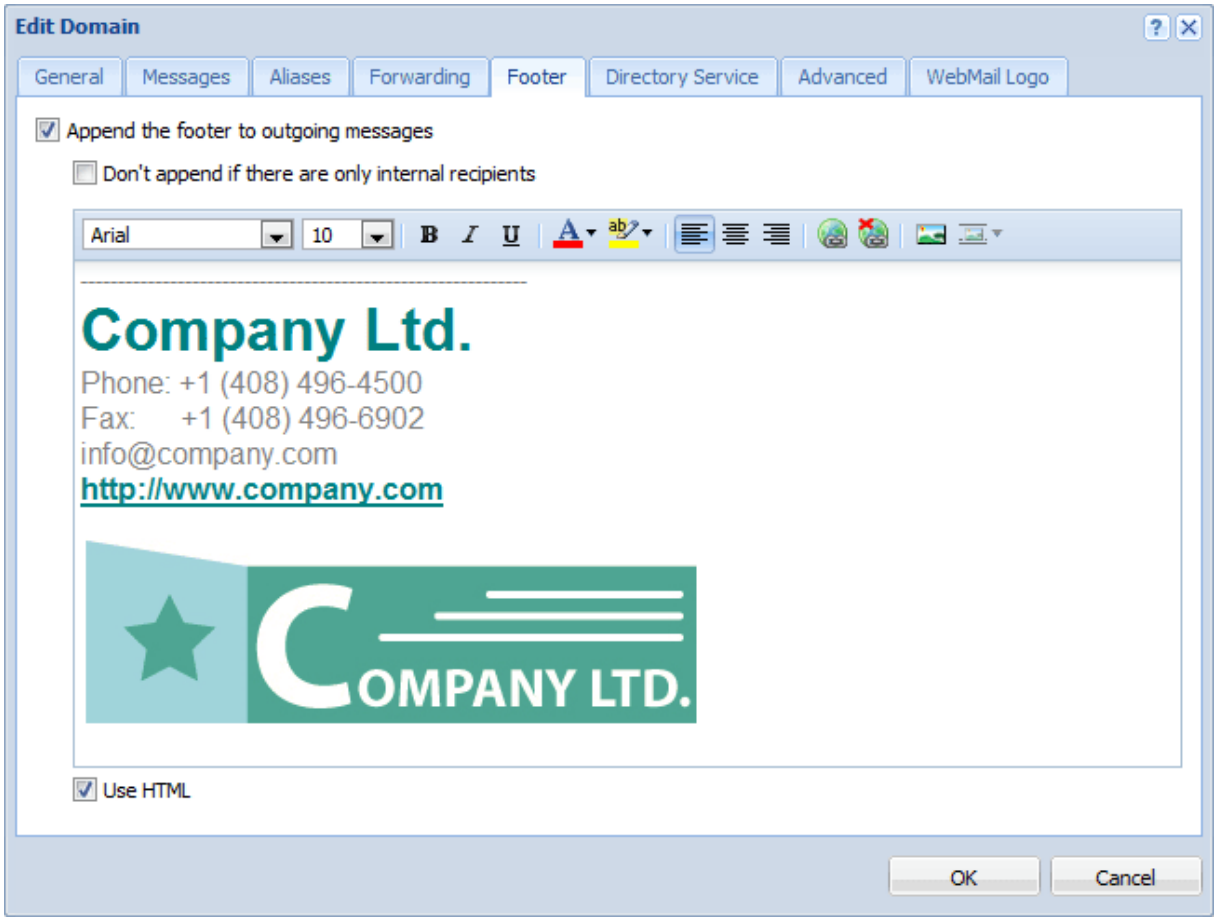
In Kerio Connect, you can:

- Define custom email footers
- Translate the interfaces into another language
- Create a custom page for Kerio Connect Client (read Customizing the Kerio Connect Client login page)
- Add a custom logo to Kerio Connect Client

Defining custom email footers

For each domain, you can customize email footers that are automatically added to all messages sent from this domain.

1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Double-click the domain and go to the **Footer** tab.
3. Enable the **Append the footer to outgoing messages** option.
4. Create the footer (in plain text or HTML).
5. If you do not want to append footers to messages for internal recipients, select the **Don't append if...** option.
6. Click **OK**.



If user defines their own email signature, this domain footer is displayed below the user's signature.

When a user replies to a message, Kerio Connect places the domain footer below the whole conversation and the user's signature below the individual replies.

If users send digitally signed or encrypted messages, Kerio Connect does not append any footers to the message.

Adding automatic user and company details to domain footers

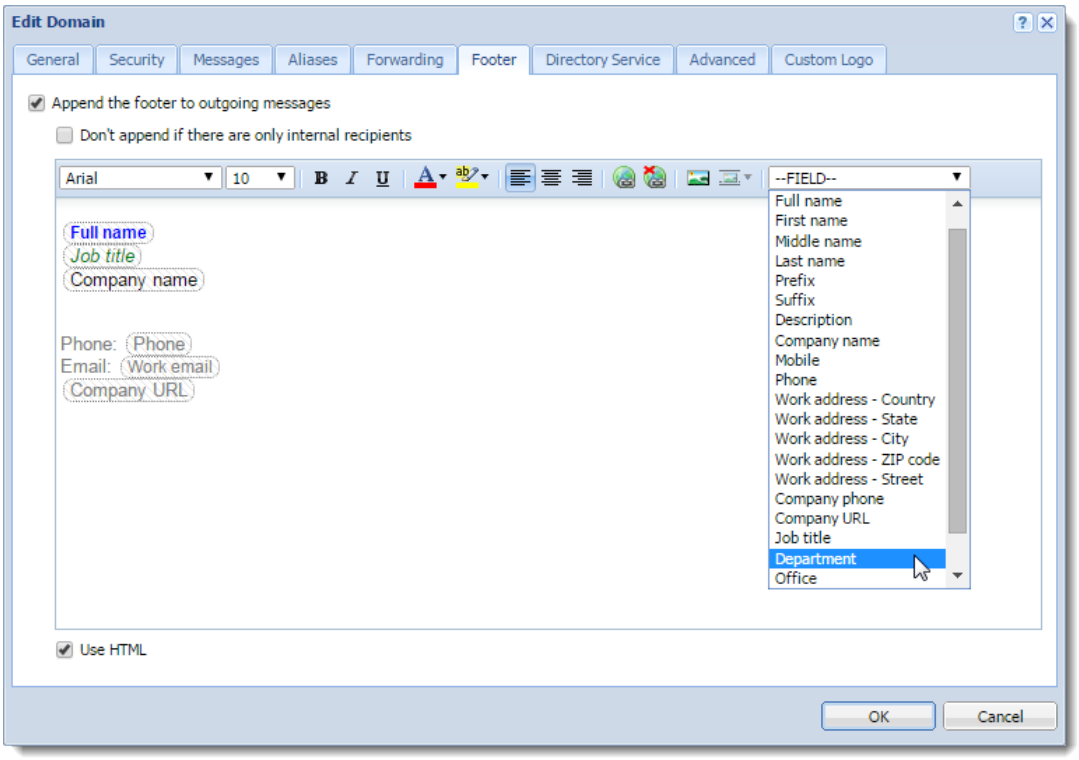
You can use special field identifiers to add user and/or company details to the footer:

1. Fill in the information in the users' account details.
2. Create company locations.
3. In the administration interface, go to the **Configurations** → **Domains** section.

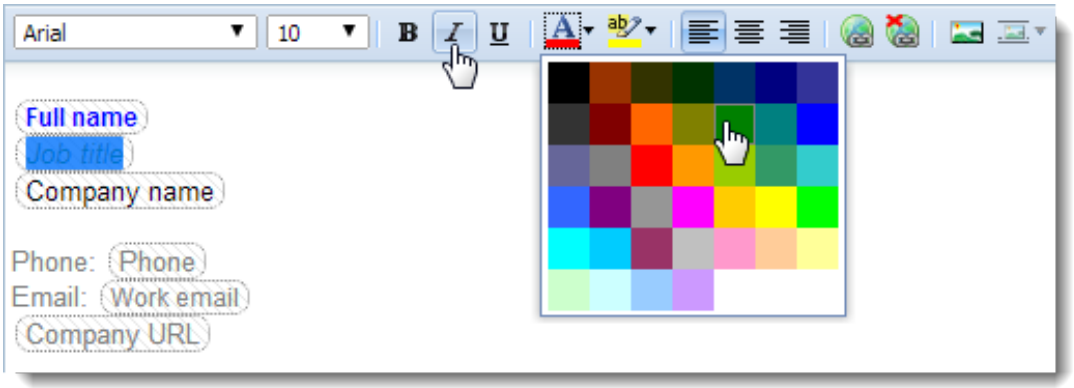
4. Select a domain and click **Edit**.

5. Click the **Footer** tab.

6. Define the footer using items in the **Field** drop-down list.

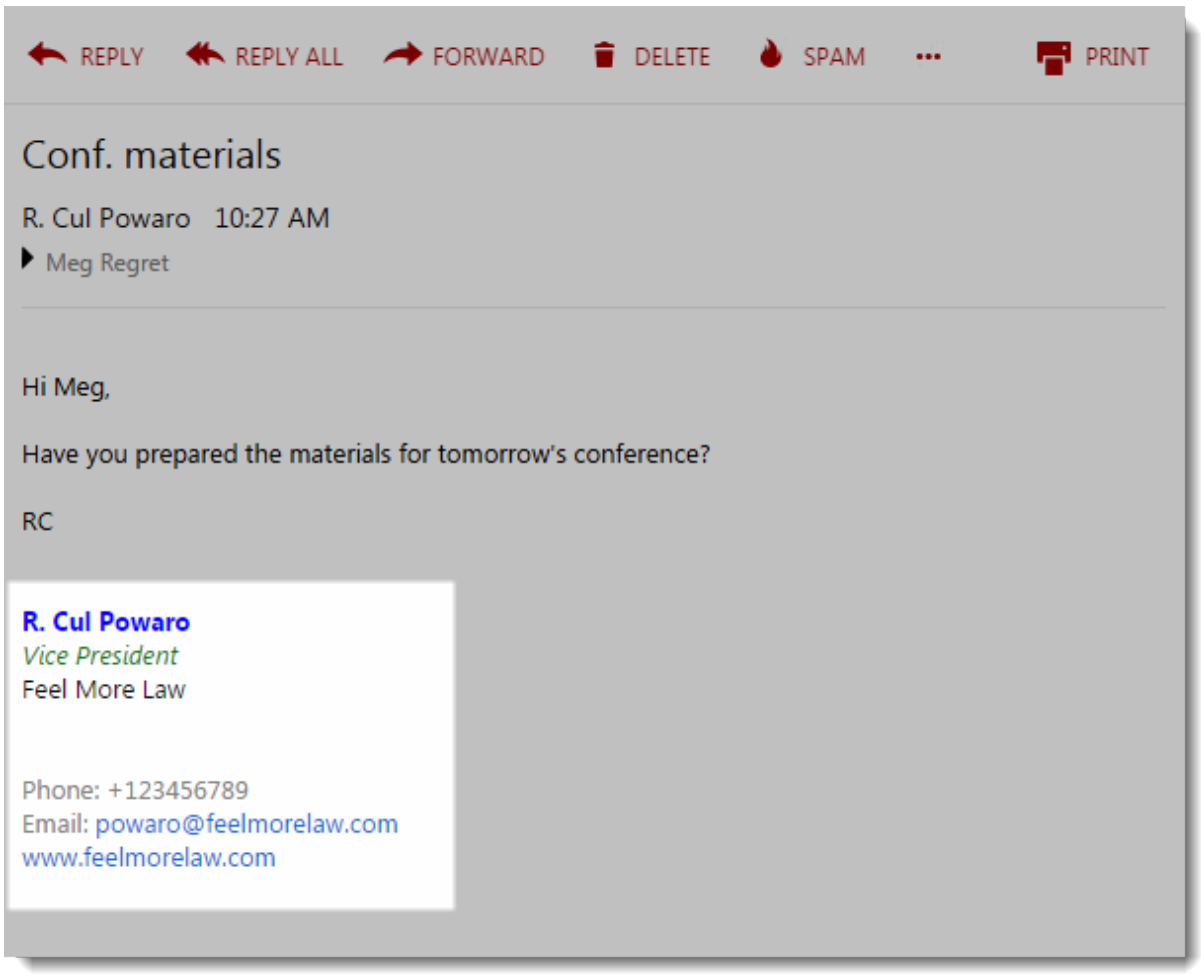


7. If you select the **Use HTML** option, you can format the fields: select the field and apply formatting attributes.



8. Click **OK**.

The final footer might look like this:



If users send digitally signed or encrypted messages, Kerio Connect does not append any footers to the message.

Adding a custom logo to Kerio Connect Client

Kerio Connect Client displays a default logo in the top left corner.

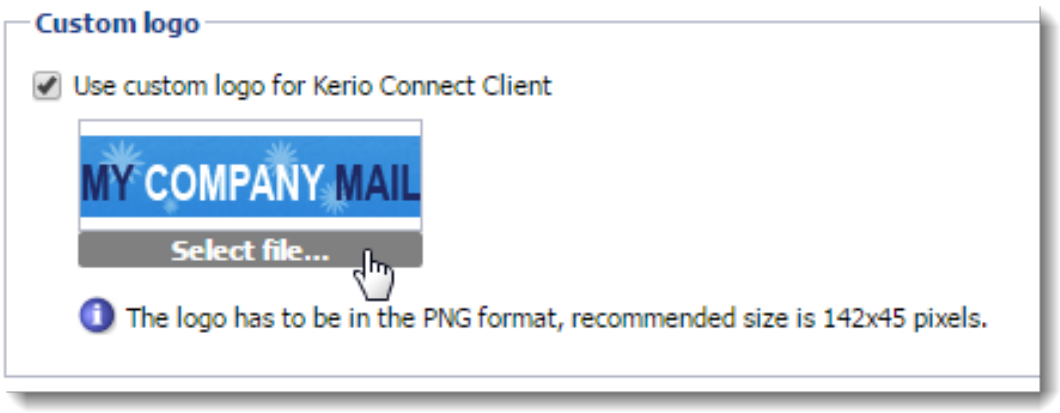
For version 8.5 and newer, you can change the logo:

- Globally for all domains
- For each domain separately

If you set both logos, Kerio Connect Client displays the logo configured for a particular domain.

Changing the logo for all domains

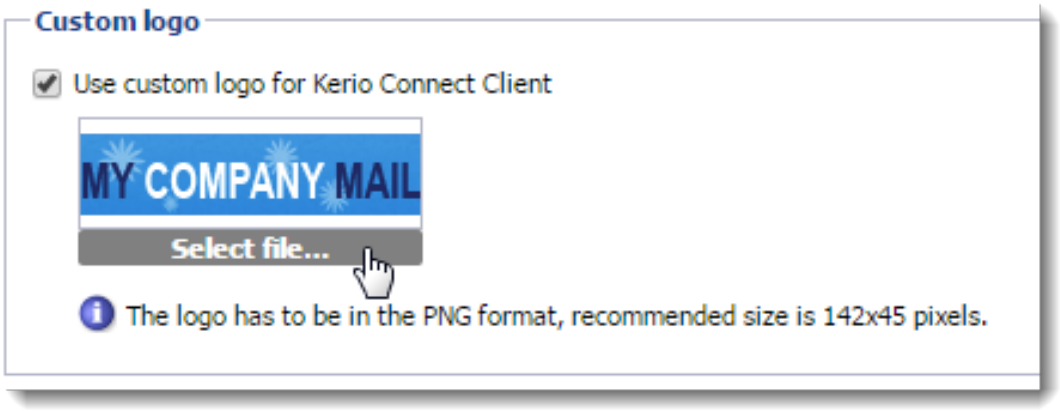
1. In the administration interface, go to **Configuration** → **Advanced Options** → **Kerio Connect Client**.
2. In the **Custom logo** section, select **Use custom logo for Kerio Connect Client**.
3. Click **Select file** and locate your image.



4. Click **Apply**.

Changing the logo for individual domains

1. In the administration interface, go to **Configuration** → **Domains**.
2. Double-click a domain and go to the **Custom Logo** tab.
3. Select the **Use custom logo for Kerio Connect Client** option.
4. Click **Select file** and locate your image.



5. Click **OK**.

Localizing the user interface

Kerio Connect Client 8.1 and later

For detailed information on how to localize Kerio Connect Client, read Translating Kerio Connect Client into a new language.

Kerio Connect Client 8.0

You cannot add new translations to Kerio Connect Client 8.0.However, you can overwrite one of the existing translations:

1. Go to the installation directory of Kerio Connect.
2. Open the `web\webmail\translations` folder.
3. Select a language file to overwrite and open it in a text editor.

   The file contains both the source language (English) and the target language.
4. Translate into the target language.
5. Save the file and restart Kerio Connect.

The text in the language files must be coded in UTF-8.

Translating Kerio Connect Client to a new language

Translating Kerio Connect Client

This article describes Kerio Connect 8.1 and newer. For information on translating Kerio Connect Client in version 8.0, read the Customizing Kerio Connect article.

Translations of Kerio Connect Client are saved in several files in the installation directory of Kerio Connect.

To add a new language for Kerio Connect Client, follow these steps:

1. Go to the Kerio Connect installation directory to folder `web/webmail/translations`.

   Files with localizations are named using 2-letter language codes.

2. Copy all files of one language (except English) and rename them according to the target language code.

3. In file `xx_definitions.xml`, rewrite the code and name of the new language.

4. In files `xx.js` and `xx_login.js`, translate all strings to the new language.

   Do not change the structure of any file.

5. Restart Kerio Connect.

The new language is now available in Kerio Connect Client.

Upgrading Kerio Connect

Kerio Connect upgrades may contain new or modified sentences. These will not be included in your own translations and will be displayed in English.

We recommend to use the original files (which you used as a template for the new language) and compare them with the same language files after the upgrade. You can then translate new sentences into your language.

Configuring data store in Kerio Connect

How to set path to data store directory

You configure the path to the data store during the installation process.

To change the data store folder:

1. Create a new folder for the data store.

   Do not use diacritics and make sure there is enough free space for the data store.

    The folder must be on a local disk. If you're using a virtual machine, define the disk as local.

2. In the administration interface, go to **Configuration** → **Advanced Options** → **Store Directory**.

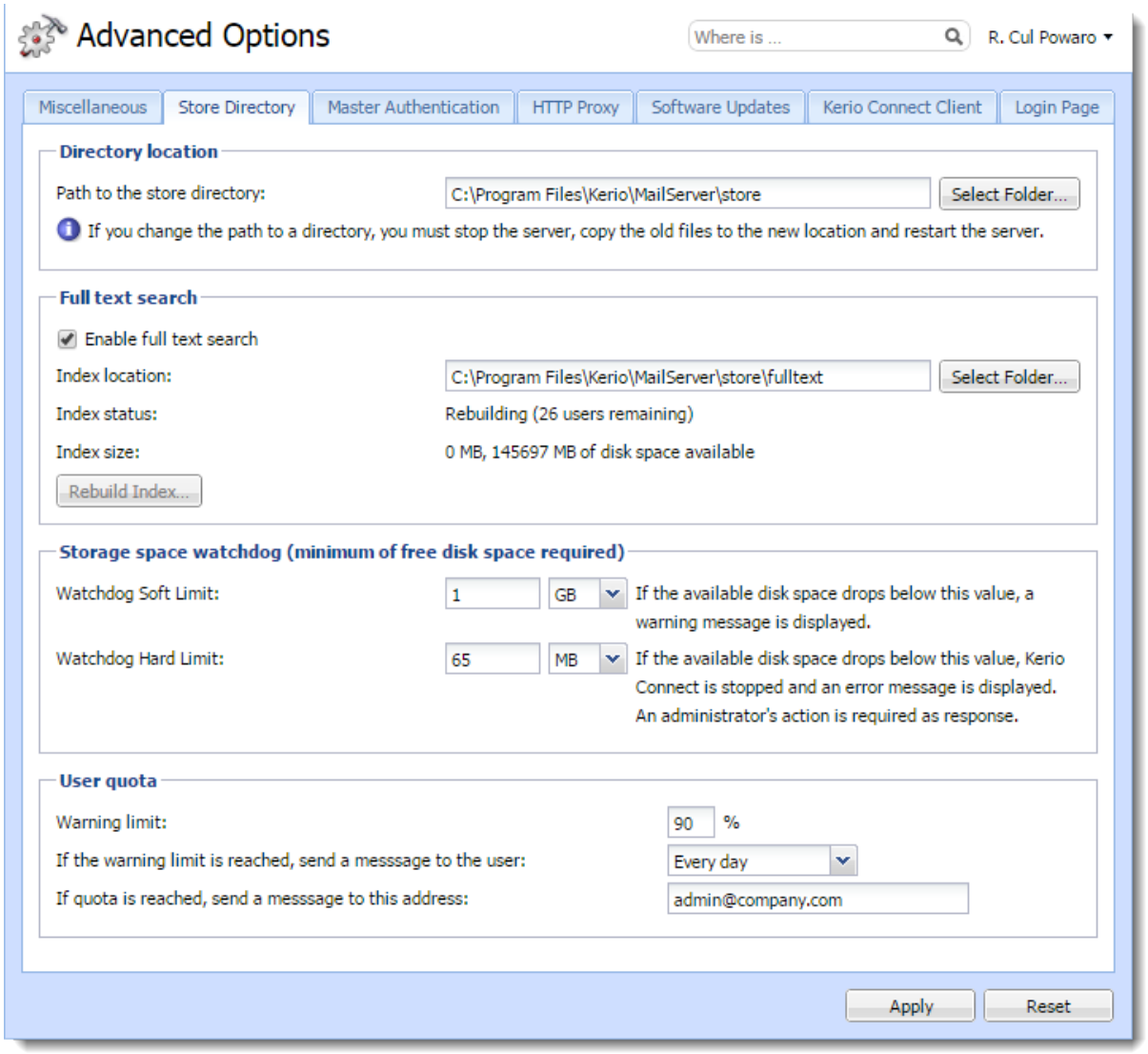
3. Select the new folder and confirm the settings.

    Do not use a UNC path.

4. Stop Kerio Connect.

5. Copy all files from the old store directory to the new one.

6. Run Kerio Connect.



Configuring full text search

In Kerio Connect, users can search their items using the full text search feature.

To enable this option:

1. In the administration interface, go to **Configuration** → **Advanced Options** → **Store Directory**.
2. Select the **Enable full text search** option.
3. Specify a folder for storing the fulltext search index.

Do not use a UNC path.

4. To create a new index, click **Rebuild Index**.
5. Select who to rebuild the index for and click **Start**.

   You can rebuild the index for:

   - Whole server
   - Single domain
   - Single user
6. Save your settings.

If you have many users with large mailboxes, the full text search can affect the performance of your server.

Setting the data store notification limits

Kerio Connect can notify you when the free space in your data store folder has dramatically decreased.

Set the limits in the administration interface in section **Configuration** → **Advanced Options** → **Store Directory**.

Watchdog Soft Limit
: If the free space on disk with the data store drops below this value, Kerio Connect displays a message in the administration interface.

Watchdog Hard Limit
: If the free space on disk with the data store drops below this value, Kerio Connect stops and displays a message in the administration interface.

Information about reached limits is logged in the Error log.

Archiving in Kerio Connect

About archiving

Kerio Connect can store copies of email messages. If you need a particular or deleted message, you can recover them by using email recovery.

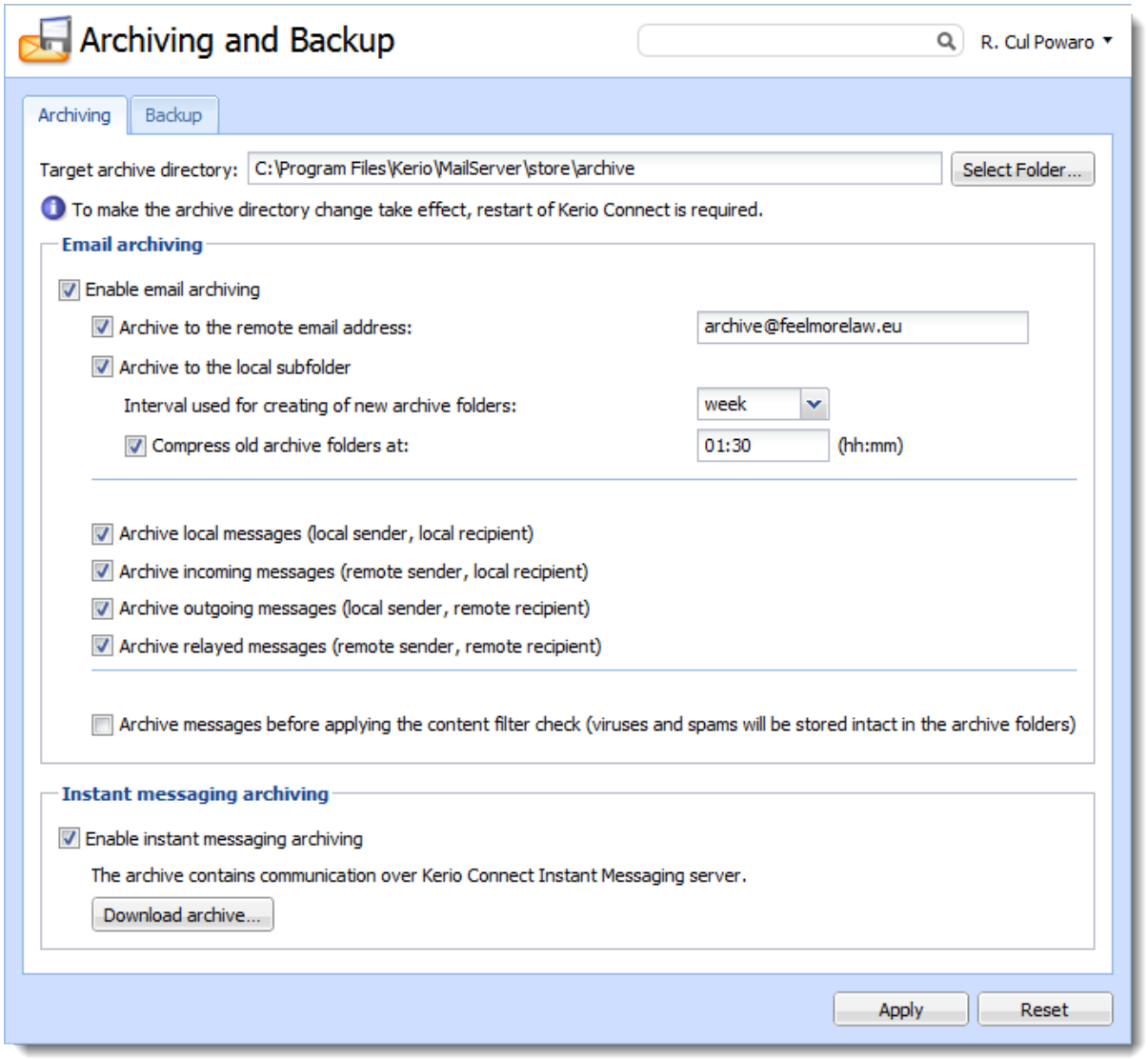
You can archive:

- Local messages — with local sender and local recipient
- Incoming messages — with remote sender and local recipient
- Outgoing messages — with local sender and remote recipient
- Relayed messages — with remote sender and remote recipient

Archiving saves messages which users send/receive after the archiving is enabled. If you want to save older messages, use the backup feature.
Also use backups to store additional data (e.g. configuration, licenses, SSL certificates, etc.).
For archiving of mailing lists, read this article.
For archiving instant messaging, read article Archiving instant messaging.

Configuring archiving

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → **the Archiving tab**.
2. Click **Select folder** and define where Kerio Connect will store the archived files.
3. Select the **Enable email archiving** option.
4. Kerio Connect can also send the archive files to an email address. Enable the **Archive to the remote email address** option and specify the address.
5. To archive messages also to the Kerio Connect installation directory, select the **Archive to the local subfolder** option and select the archiving interval.
6. Select the types of messages you want to archive (see above).
7. To avoid the antispam and antivirus check before archiving, select the **Archive messages before applying the content filter check** option.
8. Click **Apply** to save your settings.



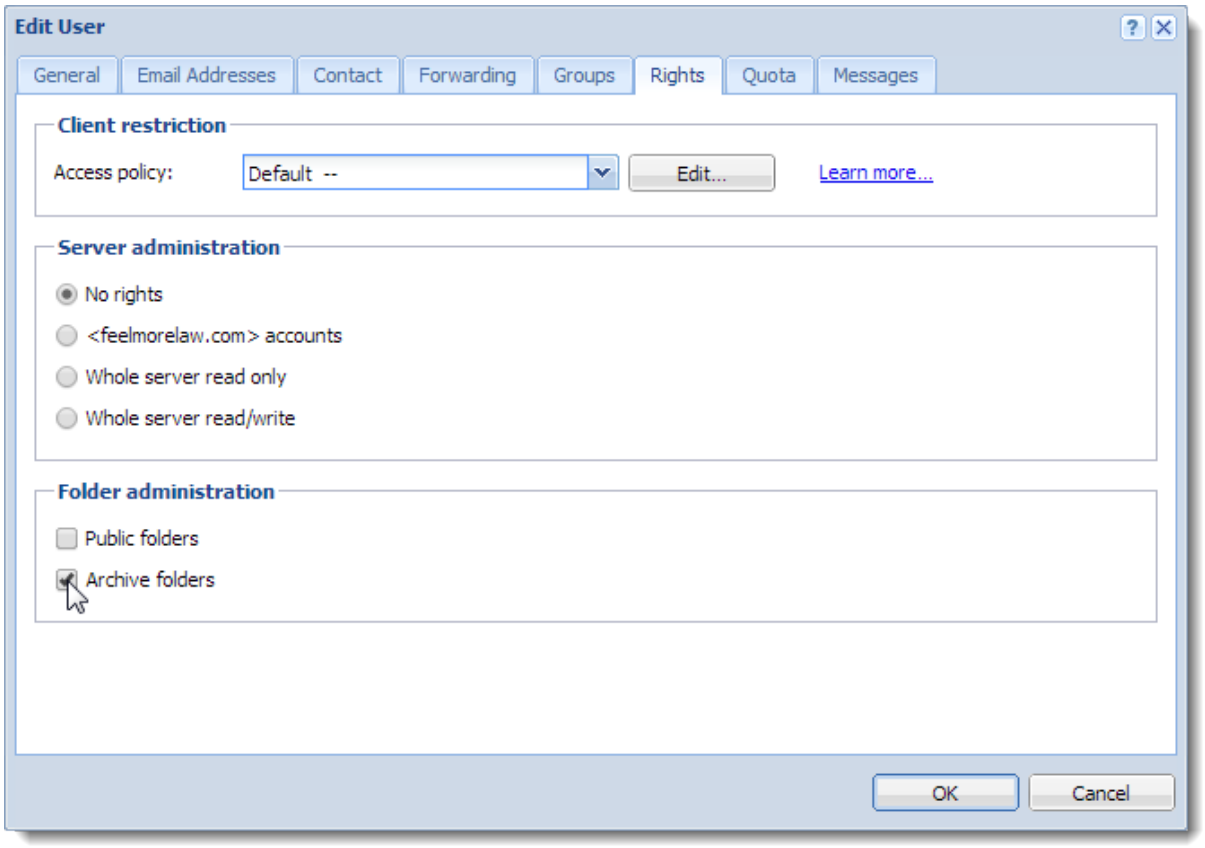
Viewing archive folders

By default, only the administrator of the primary domain can view archive folders. They can also assign the rights to other users.

Because messages of all users are archived, only a confidential administrators should have access to the archive folders.

1. In the administration interface, go to the **Accounts** → **Users** section.
2. Double-click the user and go to the **Rights** tab.
3. Select the **Archive folders** options.
4. Click **OK**.

Whenever an archive folder is available for viewing, it is automatically displayed in Kerio Connect Client of users with appropriate access rights..



Configuring backup in Kerio Connect

Overview

Kerio Connect can backup the following items:

- User mailboxes
- Public folders
- Mailing lists
- configuration files
- Licenses
- SSL certificates
- SpamAssassin database
- Contact lists in instant messaging

For backups, use any removable or network disk.

You can configure backups in section **Configuration** → **Archiving and Backup**.

Temporarily disabled users are not included in the backups.

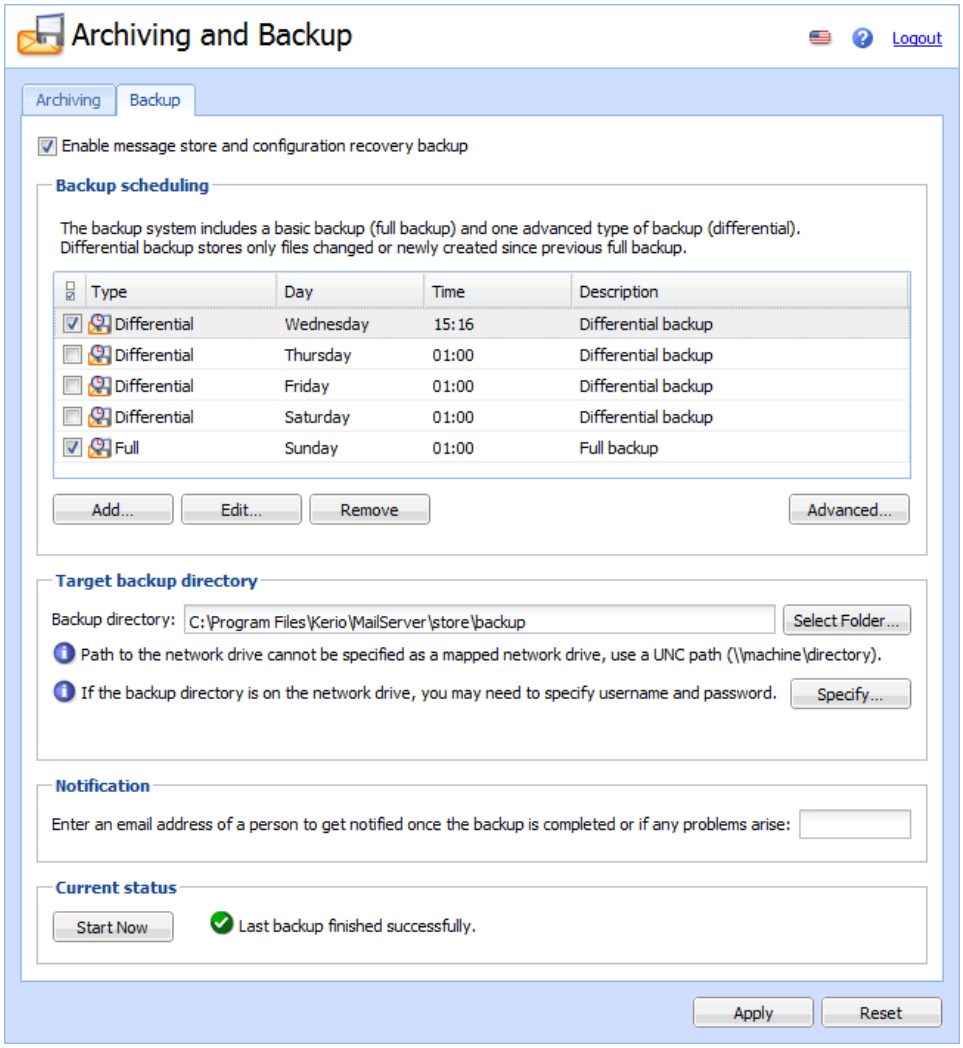
Types of backups

In Kerio Connect, there are two types of backups — **full** backups and **differential** backups.

- **Full backup** stores all files and items.
- **Differential backup** stores files that have been added or changed since the last full backup.

You can schedule any number of full and differential backups. You may consider the:

- Size of the data store. This influences the time each backup takes and its size.
- Importance of data which might be lost. When email communication and storing messages is important for your company, schedule more frequent backups.



If you perform backups frequently, minimum of data is lost if server fails.

Configuring backups

To configure backups, you must have the full access rights to administration or you can use the built-in administrator account. For more information on access rights, read the Accessing Kerio Connect administration.

To configure the backup schedule:

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → **Backup**.
2. Select the **Enable message store and configuration recovery backup** option.
3. Click **Add**. Select the type and time for the backup and click **OK**.
4. Click the **Advanced** button to specify the maximum size and number of backups.

5. Define the folder where to store all backups (**Target backup directory**).

   If required, **Specify** the username and password for accessing a network drive (on Microsoft Windows only).

   No special characters allowed in the folder name.

6. Type an email address where Kerio Connect can send messages about backups.

7. Save your settings.

If you want to make an immediate full backup which is independent of your other backups, click the **Start Now** button.

Recovering data from backups

To get instructions for data recovery, read Data recovery in Kerio Connect.

Data recovery examples

To read through some examples of data recovery, see Examples of data recovery in Kerio Connect.

Troubleshooting

If any problem with backups occurs, consult the Debug log (right-click the Debug log area and enable **Store Backup**).

Examples of data recovery in Kerio Connect

Data recovery in Kerio Connect

The following sections contain examples of recovery of backed up data in Kerio Connect.

Examples for Microsoft Windows

Full backup recovery

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 directory

   `D:\store`

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

   `E:\backup`

Solution:

The command must be run from the directory where Kerio Connect is installed. In this case, it is directory

`C:\Program Files\Kerio\MailServer`

Now, two scenarios are possible:

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 Connect's configuration file and uses it.

 If the parameter contains a space in a directory name, it must be closed in quotes. For example:
`kmsrecover "E:\backup 2"`

Recovery of a single user's mailbox

- The directory with the backup is stored on an external disk E,
- we need to get a single user's mailbox from the backup,
- the entire mailbox and its content will be saved out of the Kerio Connect's store (folder `\tmp`).

`kmsrecover -d company.com -u smith -s D:\tmp E:\backup` (for recovery from the latest complete backup, i.e. combination of the latest full and differential backup)

or

`kmsrecover -d company.com -u smith -s D:\tmp E:\backup\F20051009T220008Z.zip` (for recovery from a particular backup)

Recovery of a single folder of a user

- The directory with the backup is stored on an external disk E,
- one specific folder of the user mailbox must be gained from the backup (`Sent Items` in this case),
- the command is run in the verbose mode (parameter `-v`) which allows to monitor the recovery process.

`kmsrecover -v -d company.com -u smith -f "Sent Items" E:\backup` (for recovery from the latest complete backup, i.e. combination of the latest full and differential backup)

or

`kmsrecover -v -d company.com -u smith -f "Sent Items" E:\backup\F20051009T220008Z.zip` (for recovery from a particular backup)

Recovery of public folders of a particular domain

- The directory with the backup is stored on an external disk E,

- it is now necessary to recover the domain's public folders (the `public` mask will be used here),
- and the original public folders will be kept at the same time (status before using Kerio Connect Recover). This will be done simply by using the `-b` parameter.

```
kmsrecover -b -d company -m public E:\backup
```

Examples for Mac OS X

Full backup recovery

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

   `/Volumes/backup`

Solution:

The command must be run from the directory where Kerio Connect 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 Connect directory is included in the path variable or not. If the path is not set there, the command will be as follows:

```
./kmsrecover /Volumes/backup
```

Otherwise, it will be like this:

```
kmsrecover /Volumes/backup
```

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

Recovery of a single user's mailbox

- The directory with the backup is stored on an external disk,
- we need to get a single user's mailbox from the backup,
- the entire mailbox and its content will be saved out of the Kerio Connect's store (folder `/Temp`).

```
./kmsrecover -d company.com -u wsmith -s /Volumes/Temp
/Volumes/backup/F20051009T220008Z.zip
```

Recovery of a single folder of a user

- The directory with the backup is stored on an external disk,
- one specific folder of the user mailbox must be gained from the backup (`Sent Items` in this case),
- the command is run in the verbose mode (parameter `-v`) which allows to monitor the recovery process.

```
./kmsrecover -v -d company.com -u wsmith -f "Sent Items"
/Volumes/backup/F20051009T220008Z.zip
```

Recovery of public folders of a particular domain

- The directory with the backup is stored on an external disk,
- it is now necessary to recover the domain's public folders (the `public` mask will be used here),
- and the original public folders will be kept at the same time (status before using Kerio Connect Recover). This will be done simply by using the `-b` parameter.

```
./kmsrecover -b -d company.com -m public /Volumes/backup
```

Data recovery in Kerio Connect

Recovering data from backup

To recover backup data, use a special tool, **Kerio Connect Recover**. The tool extracts the back-up and saves the data in their original location in the Kerio Connect hierarchy.

To launch Kerio Connect Recover, run the `kmsrecover` command from the directory where Kerio Connect is installed:

```
kmsrecover [options] <directory_name>|<file_name>
```

On Mac OS X and Linux, enter a command in the following format (if it has not already been introduced in the file of the path system variable):

```
./kmsrecover [options] <directory_name>|<file_name>
```

To see details and examples of individual attributes run commands:

`kmsrecover -h` or `kmsrecover --help`

 If differential backup is used, use the last full and differential backups for the recovery.

- Stop the Kerio Connect Engine prior to the recovery.
- Launch kmsrecover from the computer where Kerio Connect is installed.
- If Kerio Connect Recover is run without advanced parameters, all items in the Kerio Connect's data store, such as configuration files, licenses, mailing lists and data, will be overwritten.

Advanced options of Kerio Connect Recover

Abbreviation	Full option	Mask	Description
`-d`	`--domain`		Recovers (or lists with parameter `-l`) all backed-up data for the specified domain..
`-u`	`--user`		Recovers (or lists with parameter `-l`) data of the specified user.
`-f`	`--folder`		This option recovers the specified folder of the user (this option requires setting of the `-d` and `-u` options).
`-s`	`--store`		This option sets where SpamAssassin databases, mailing lists and emails (including events, notes, contacts, etc.) would be unpacked and stored. By default, the `store` on the Kerio Connect from which `kmsrecover` was launched is used.
`-c`	`--cfgdir`		This option sets a directory where configuration files, SSL certificates and licenses would be stored. By default, the current folder from which the `kmsrecover` command was started is used.
`-m`	`--mask`		This option allows to set which parts of the back up would be recovered. It requires setting of mask with `-m <value>` or`--mask=<value>`.The `<value>` value stands for any combination mentioned below. Example: `-m cfg,license,sslca,sslcert` — this command recovers license, SSL certificates and configuration files.
		`cfg`	This argument recovers only configuration files mailserver.cfg and users.cfg where server configurations are defined.

Abbreviation	Full option	Mask	Description
		`mail`	This recovers only the `\store\mail` directory.
		`lists`	This argument recovers only configuration of mailing lists (`\store\lists`).
		`spamassassin`	This argument recovers only the SpamAssassin database.
		`license`	This argument recovers the Kerio Connect license.
		`sslca`	This argument recovers certificates issued by certification authorities.
		`sslcert`	This argument recovers the Kerio Connect certificates.
		`public`	This argument recovers public folders.
`-b`	`--backup`		This option performs an additional back-up before the recovery is started. The original directory will have the BAK extension. If such a file already exists, it will be replaced by the new version. However, bear in mind that backup of the current status doubles the store size. It is therefore not desirable to use this option if there is not enough free disk space available.
`-g`	`--noprogress`		This option hides information about the recovery progress. It is useful especially if the recovery is recorded in the log. Information of how much time is left to the completion of the recovery process is irrelevant in that case.
`-l`	`--listing`		This option lists the backup store content. It is also possible to use additional parameters (such as `-d` and `-u` which lists only contents of the mailbox of the specific user).
`-q`	`--quiet`		Recovery progress information will not be provided in the command line.
`-v`	`--verbose`		Recovery progress information will be provided in the command line.
`-h`	`--help`		This option prints out the help file.

Backup files

File names

Each archive name consists of backup type and date when it was created:

Full backup

`F20120118T220007Z.zip`
F — full backup
2012 — year
01 — month
18 — day
T220007Z — GMT timestamp (22:00:07); it always starts with T and ends with Z.

Differential backup

`D20120106T220006Z.zip`
D — differential backup
2012 — year
01 — month
06 — day
T220006Z — GMT timestamp (22:00:06); it always starts with T and ends with Z.

Backup copy (manual backup)

`C20120117T084217Z.zip`
2012 — year
01 — month
17 — day
T084217Z — GMT timestamp (08:42:17); it always starts with T and ends with Z.

File content

Each backup includes the following files and directories:

- `.version.txt` — the file is created at the start of the backup creation process and it includes the following information:
  - `started` — date of the start of the backup creation in pattern `YYYY-MM-DD hh:mm:ss`.
  - `version` — version of the backup tool.
  - `hostname` — DNS name of the Kerio Connect host which the backup was created for.
- `@backup` — the main directory of the backup. This directory includes the following items.

    - `license` — license backup
    - `sslca` — backup of certification authorities' certificates.
    - `sslcert` — backup of Kerio Connect's SSL certificates.
    - `store` — backup of the data store
- `mailserver.cfg` — a file with the Kerio Connect configuration. All settings done in the administration interface are saved in `mailserver.cfg`.
- `users.cfg` — a file with user configuration. It involves all users and their parameters set in the Kerio Connect's administration interface.
- `.summary.txt` — the file is created at the end of the backup creation process and it includes the following information:
    - `started` — date of the start of the backup creation in pattern `YYYY-MM-DD hh:mm:ss`.
    - `finished` — date of the backup completion in pattern `YYYY-MM-DD hh:mm:ss`.
    - `count_files` — number of backed-up files.
    - `total_size` — total size of the files (in bytes) which are backed-up in the interval between creation of files `.version.txt` and `.summary.txt`.
    - `duration` — total time of the backup creation process in pattern `hh:mm:ss:msms`

Data recovery examples

To read through some examples of data recovery, see this article.

Troubleshooting

If any problem regarding backups occur, consult the Debug log (right-click the Debug log area and enable **Store Backup**).

Configuring SSL certificates in Kerio Connect

About SSL certificates

You need a SSL certificate if you wish to secure Kerio Connect by SSL/TLS encryption. SSL certificates are used to authenticate an identity on a server.

Kerio Connect creates the first self-signed certificate during the installation. Upon their first login, users will have to confirm they want to go to a page which is not trustworthy. To avoid this, generate a new certificate request in Kerio Connect and send it to a certification authority for authentication.

To make the communication as secure as possible, you can:

- disable all unsecured services or
- set an appropriate security policy

Certificates can be created in section **Configuration** → **SSL Certificates**.

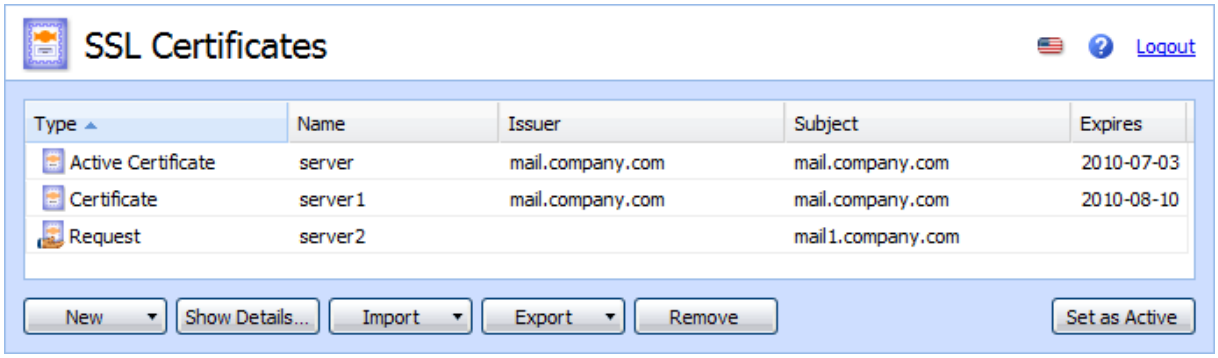


Figure 1 SSL certificates

Kerio Connect supports certificates in the following formats:

- Certificate (public key) — X.509 Base64 in text format (PEM). The file has suffix `.crt`.
- Private key — the file is in RSA format and it has suffix `.key` with 4KB max.

Creating self-signed certificates

To create a self-signed certificate, follow these steps:

1. Go to section **Configuration** → **SSL Certificates**.
2. Click on **New** → **New Certificate**.
3. Fill in the information and save.

To enable the server to use this certificate, select the certificate and click on the **Set as Active** button.

Creating certificates signed by certification authority

To use a certificate signed by a trustworthy certification authority, you must first generate a certificate request, send it to a certification authority and import a signed certificate upon receiving it.

1. Open section **Configuration** → **SSL Certificates** and click on **New** → **New Certificate Request**.
2. Fill in the information and save.
3. Select the certificate and click on the **Export** → **Export Request** button.
4. Save the certificate to your disk and send it to a certification authority.

Once you obtain your certificate signed by a certification authority:, and click on **Import** → **Import Signed Certificate from CA**.

1. Go to section **Configuration** → **SSL Certificates**.
2. Click on **Import** → **Import Signed Certificate from CA**.
3. To enable the server to use this certificate, select the certificate and click on the **Set as Active** button.

Intermediate certificates

Kerio Connect allows authentication by **intermediate** certificates. To make authentication by these certificates work, follow these steps to add the certificates to Kerio Connect:

1. In a text editor, open the server certificate and the intermediate certificate.
2. Copy the intermediate certificate below the server certificate into the server certificate file (`*.crt`) and save.

   The file may look like this:

```
-----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+E6o3tiUEDywrgrVX6OCjbW1+y0CdMaq7dlpszRB
t14EmBxKYw==
-----END CERTIFICATE-----
```

3. In the administration interface, go to section **Configuration** → **SSL Certificates**.
4. Import the modified server certificate by clicking on **Import** → **Import New Certificate**.
5. Save the settings.

 If you have multiple intermediate certificates, add them one by one to the server certificate file.

Configuring SSL/TLS in Kerio Connect

Overview

New in Kerio Connect 8.5!

Kerio Connect 8.5 introduces various security improvements. The configuration file now allows you to enable or disable specific security protocols and ciphersets manually.

You might need to adjust the security settings when a flaw in a security protocol is found or to get a good security rating for your server. (You can test your server, for example, at Qualys SSLlabs test site).

Changing the SSL/TLS configuration

Kerio Connect uses different variables for the SSL/TLS protocols configuration. To change the configuration:

1. Stop the Kerio Connect engine.
2. Open the configuration file `mailserver.cfg` for editing

   See Configuration files for the default location.
3. Change the settings in the `Security` section.

   See the list of variables below.
4. Save the file.
5. Start Kerio Connect.

Resetting the SSL/TLS configuration

To reset the SSL/TLS configuration in the configuration file:

1. Stop the Kerio Connect engine.
2. Open the configuration file `mailserver.cfg` for editing.

   See Configuration files for the default location.
3. Delete any variable in the `Security` section.

4. Save the file.

5. Start Kerio Connect.

Kerio Connect sets the default values of all the SSL/TLS variables.

List of variables

Kerio Connect uses eight variables for the SSL/TLS protocols configuration.

DisableEphemeralDH

Changed in Kerio Connect 9!

The default value, **1**, disables the use of DHE (Ephemeral Diffie-Hellman) for key exchange.

If enabled, the server generates a random ephemeral public key for each session so that attackers cannot decipher past sessions (this is also called “forward secrecy”).

This variable replaces **AllowEphemeralDH**. In Kerio Connect 8.5, set the value of `AllowEphemeralDH` to **0** to disable the use of DHE.

EphemeralDHParamSize

New in Kerio Connect 9!

The default value, **0**, sets the size of DHE to 2048. Make sure the **DisableEphemeralDH** is enabled.

You can change the default value to **1024**, **2048**, or **4096**

AllowEphemeralECDH

The default value, **1**, enables ECDHE for key exchange.

The server generates a random ephemeral public key for each session so that attackers cannot decipher past sessions. ECDHE is more efficient than DHE and uses shorter keys.

SSLDontInsertEmptyFragments

The default value, **1**, disables the OpenSSL workaround for the CVE-2011-3389 vulnerability.

If you set the variable to **0**, some older implementations of SSL may not connect to Kerio Connect servers.

ServerTlsProtocols

In this variable, you can change the SSL/TLS protocols used by Kerio Connect.

Leave the variable empty to use a default set of SSL/TLS protocols: `TLSv1,TLSv1.1,TLSv1.2`

To use a custom set of protocols, list the protocol names, separated by commas, in the variable. For example: `<variable name="ServerTlsProtocols">SSLv3,TLSv1,TLSv1.1,TLSv1.2</variable>`

ServerTlsCiphers

In this variable, you can change the cipher list used by Kerio Connect.

Leave the variable empty to use a default cipher list: `AESGCM:HIGH:+EDH-RSA-DES-CBC3-SHA:+EDH-DSS-DES-CBC3-SHA:+DES-CBC3-SHA`

To use a custom cipher list, type the cipher list in the variable.

For the full syntax of cipher lists, see the OpenSSL website.

ClientTlsProtocols

In this variable, you can change the SSL/TLS protocols used when Kerio Connect acts as a client, for example, when sending messages via the SMTP protocol.

Leave the variable empty to use a default set of SSL/TLS protocols: `TLSv1,TLSv1.1`

To use a custom set of protocols, list the protocol names, separated by commas, in the variable. For example: `<variable name="ClientTlsProtocols">SSLv3,TLSv1,TLSv1.1,TLSv1.2</variable>`

ClientTlsCiphers

In this variable, you can change the client cipher list.

Leave the variable empty to use a default cipher list.

To use a custom cipher list, type the cipher list in the variable.

For the full syntax of cipher lists, see the OpenSSL website.

PreferServerCipherOrder

The default value, **1**, allows Kerio Connect decide which cipherset to use regardless of the client preferences.

Adding trusted root certificates to the server

Overview

If you want to send or receive messages signed by root authorities and these authorities are not installed on the server, you must add a trusted root certificate manually.

Use the following steps to add or remove trusted root certificates to/from a server.

Mac OS X

Add

Use command:

```
sudo security add-trusted-cert -d -r trustRoot -k
/Library/Keychains/System.keychain ~/new-root-certificate.crt
```

Remove

Use command:

```
sudo security delete-certificate -c "<name of existing certificate>"
```

Windows

Add

Use command:

```
certutil -addstore -f "ROOT" new-root-certificate.crt
```

Remove

Use command:

```
certutil -delstore "ROOT" serial-number-hex
```

Linux (Ubuntu, Debian)

Add

1. Copy your CA to `dir /usr/local/share/ca-certificates/`
2. Use command:
   ```
   sudo cp foo.crt /usr/local/share/ca-certificates/foo.crt
   ```
3. Update the CA store:
   ```
   sudo update-ca-certificates
   ```

Remove

1. Remove your CA.
2. Update the CA store:
   `sudo update-ca-certificates --fresh`

Restart Kerio Connect to reload the certificates in the 32-bit versions or Debian 7.

Linux (CentOs 6)

Add

1. Install the ca-certificates package:
   `yum install ca-certificates`
2. Enable the dynamic CA configuration feature:
   `update-ca-trust enable`
3. Add it as a new file to /etc/pki/ca-trust/source/anchors/:
   `cp foo.crt /etc/pki/ca-trust/source/anchors/`
4. Use command:
   `update-ca-trust extract`

Restart Kerio Connect to reload the certificates in the 32-bit version.

Linux (CentOs 5)

Add

Append your trusted certificate to file /etc/pki/tls/certs/ca-bundle.crt
`cat foo.crt >> /etc/pki/tls/certs/ca-bundle.crt`

Restart Kerio Connect to reload the certificates in the 32-bit version.

Managing logs in Kerio Connect

About Kerio Connect logs

Logs are files where Kerio Connect records information about certain events, for example, error and warning reports and debugging information. Each item represents one row starting with a timestamp (date and time of the event).

Messages in logs are displayed in English for every language version of Kerio Connect.

See the section Types of logs for detailed information about each log.

Configuring logs

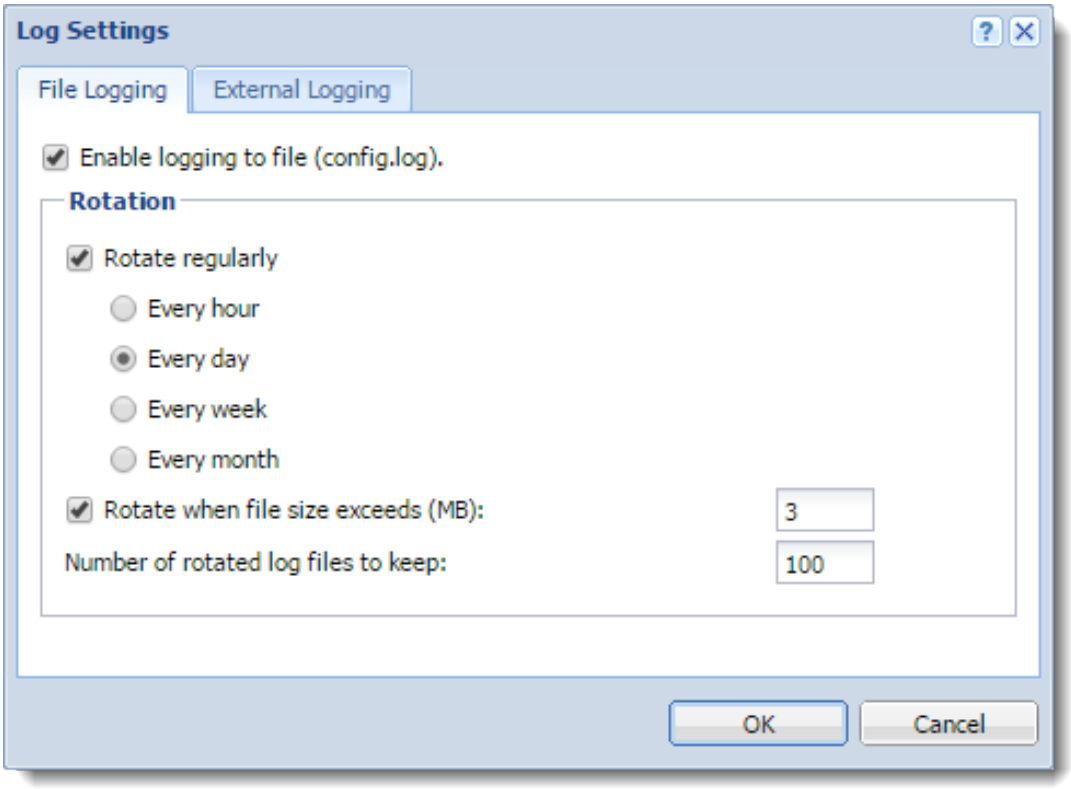
Logs are available in the Kerio Connect administration interface in the section **Logs**.

When you right-click in a log area, you can configure the following settings (available in all logs):

Save log
: You can save whole logs or a selected part in a `txt` or `HTML` format.

Highlighting
: You can highlight any part of text in logs for better reference. Specify a substring or regular expression and all rows containing such text will be highlighted.

Log Settings
: You can configure regular saves of individual logs, specifying the size and number of saved files.
You can also enable external logging to a Syslog server.



Information about log settings are recorded in the **Config** log.

The default location of the log files varies by platform:

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

Types of logs

Config log

The **Config** log keeps complete history of configuration changes. It tells you which user performed individual administration tasks and when.

Debug log

The **Debug** log monitors various kinds of information and is used for problem-solving.

You can select which information it displays.

1. Right-click in the log window and click **Messages**.
2. Select any option you want to monitor.
3. Click **OK**.


Too much information can be confusing and slows Kerio Connect's performance. Switch off the logging if you solve your problem.

Mail log

The **Mail** log contains information about individual messages processed by Kerio Connect.

Security log

The **Security** log contains information related to Kerio Connect's security. It also contains records about all messages that failed to be delivered.

Warning log

The **Warning** log displays warning messages about errors of little significance. Events causing display of warning messages in this log do not greatly affect Kerio Connect's operation. However, they can , indicate certain (or possible) problems.

For example, the Warning log can help if a users complain that certain services are not working.

Operations log

The **Operations** log gathers information about removed and moved items (folders, messages, contacts, events, tasks and notes) in user mailboxes. It is helpful especially if a user cannot find a particular message in their mailbox.

Error log

The **Error** log displays errors of great significance that usually affect the mailserver's operation (in contrast to the Warning log).

Typical error messages displayed in the Error log concern service initiation (usually due to port conflicts), disk space allocation, antivirus check initialization, improper authentication of users, and so on.

Spam log

The **Spam** log displays information about all spam emails stored (or marked) in Kerio Connect.

Audit log

New in Kerio Connect 9!

The **Audit** log displays information about all successful authentication attempts to Kerio Connect accounts, including Kerio Connect Administration, Kerio Connect Client, Microsoft Outlook with KOFF, etc.

Integrating Kerio Connect with Kerio Operator

Overview

If you have both Kerio Connect and Kerio Operator, you can use the **Click to Call** feature to place calls through Kerio Connect Client.

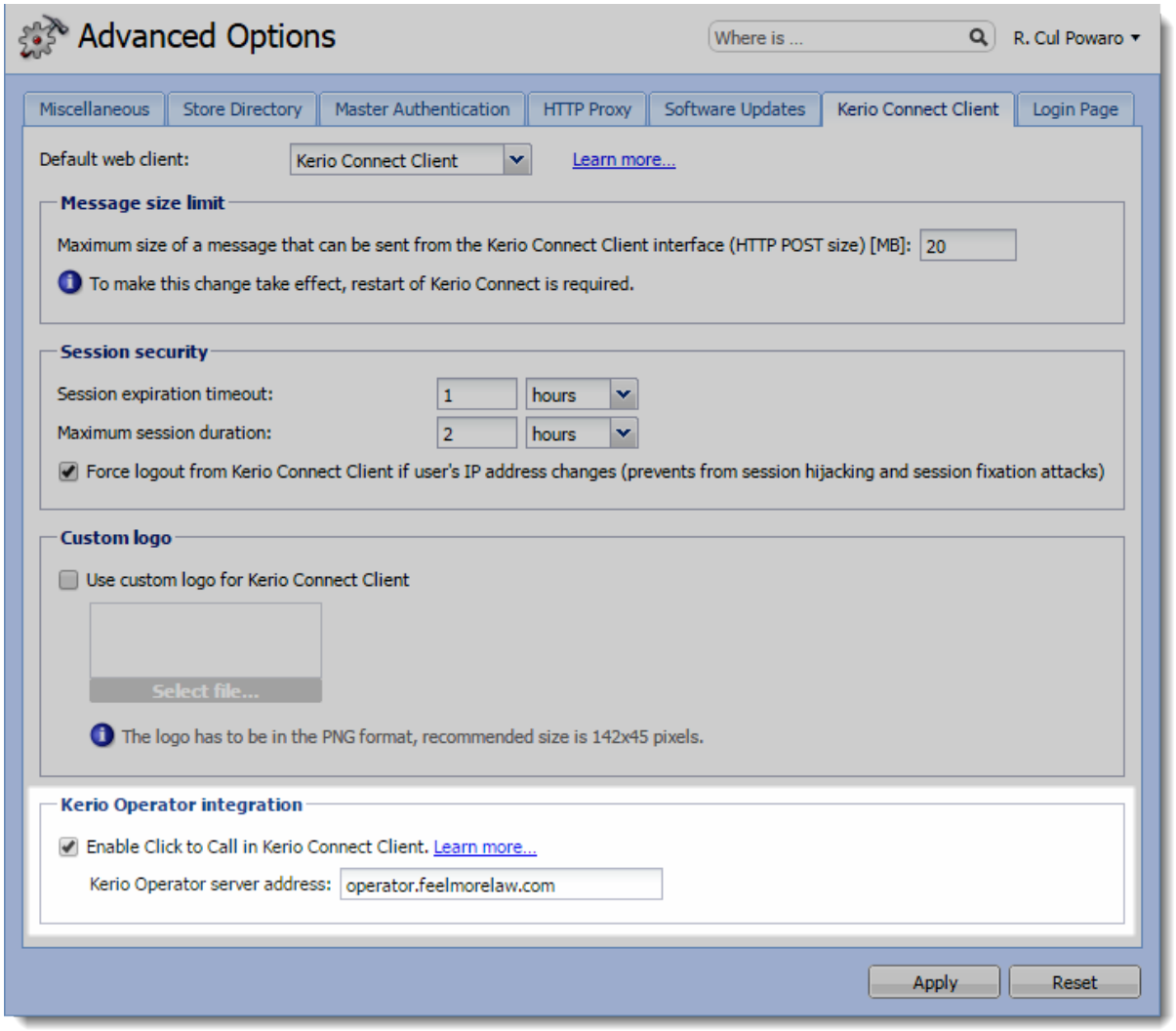
With **Click to Call**, users can dial numbers from their Kerio Connect Client using Kerio Operator.

Configuring Kerio Connect

An administrator with full access rights must connect Kerio Connect to Kerio Operator.

 Users must have identical usernames in both Kerio Connect and Kerio Operator to use the **Click to Call** feature.

1. Login to Kerio Connect Administration.
2. Go to the **Configuration** → **Advanced Options** section.
3. On the **Kerio Connect Client** tab, type the name of the Kerio Operator server.



Configuring Kerio Operator

No special configuration is necessary in Kerio Operator. If you use an outgoing prefix in your environment, you must add a number transformation rule to Kerio Operator.

See Making calls from Kerio Connect Client for more information on using Click to Call.

Kerio Active Directory Extension

How to use Kerio Active Directory Extension

You install Kerio Active Directory Extension into the Microsoft Active Directory and items containing specific Kerio Connect information are added to Active Directory.

User account will be managed in one place — in Microsoft Active Directory.

Kerio Active Directory Extension is available only in English.

How to install Kerio Active Directory Extension

Download Kerio Active Directory Extension at the Kerio Connect product pages.

It can be installed on supported operating systems using a standard installation wizard.

After the installation a new tab for creating a Kerio Connect account will be added to the dialog window for creating new users in Microsoft Active Directory.

 Depending on the version of your Microsoft Internet Explorer, you may be asked to install *Microsoft XML Parser*. Allow the installation — without it, the installation of Kerio Active Directory extension will not be completed!

How to create users and groups Kerio Connect in Active Directory

You can create user accounts and groups in Microsoft Active Directory (using, for example, **Active Directory Users And Computers**) in a usual way — the standard wizard contains a new tab for Kerio Connect.

Once you create users, map them to Kerio Connect.

 Usernames must be in ASCII or users will not be able to login to their accounts.

Troubleshooting

If you encounter any problems during KADE installation, view/save the log during the installation process (View Log/Save Log File).

Kerio Open Directory Extension

How to use Kerio Open Directory Extension

You install Kerio Open Directory Extension into the Apple Open Directory and items containing specific Kerio Connect information are added to Open Directory.

User account will be managed in one place — in Apple Open Directory.

How to install Kerio Open Directory Extension

Download Kerio Open Directory Extension at the Kerio Connect product pages.

It can be installed on supported operating systems using a standard installation wizard.

 When using configurations of Mac OS X servers of `Master/Replica` type, Kerio Open Directory Extension must be installed to the "master" server, as well as to all "replica" servers, otherwise the account mapping will not work.
If the configuration is as follows:

- you use Kerio Open Directory Extension 6.6 and newer,
- servers run on OS X 10.5.3 and newer,
- `Replica` servers were created after installation of Kerio Open Directory Extension on the "master" server,

then "replica" servers download the extension automatically from the "master" server during the creation process.
If you install Kerio Open Directory Extension on "replica" servers by hand, the configuration will not be affected.

Setting user account mapping in Kerio Connect

In Mac OS X Server, no other settings than Kerio Open Directory Extension installation are usually necessary.

 The usernames must be in ASCII. If the username includes special characters or symbols, it might happen that the user cannot log in.

In Kerio Connect the following settings must be specified:

- Enable user mapping in domain settings.
- Set user authentication via Kerberos in domain settings.
- Set user authentication via Kerberos in user settings.

Troubleshooting

If you encounter any problems during KODE installation, view/save the log during the installation process (View Log/Save Log File).

Managing user mobile devices

Managing mobile devices in Kerio Connect

Each user can synchronize their Kerio Connect account with an unlimited number of mobile devices which support Exchange ActiveSync 2.5-14.1.

 You can disable Exchange ActiveSync 14 for older devices. Read Setting a compatible Exchange ActiveSync version for specific mobile devices for more details.

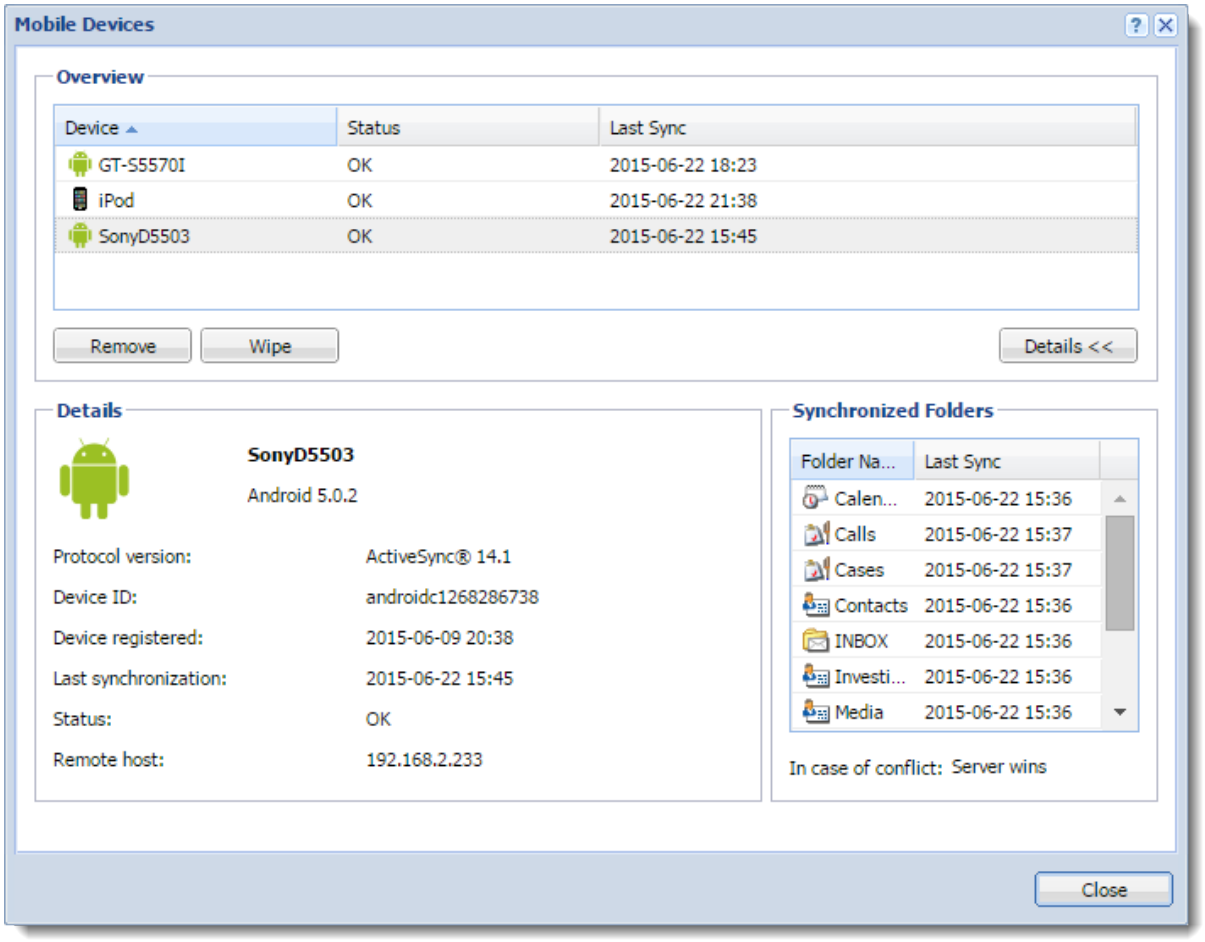
 In Kerio Connect 8.4 and older, you must select the **Allow synchronization of unsupported Exchange ActiveSync devices** option in **Configuration** → **Advanced Options** → **Miscellaneous** to allow synchronization of all devices.

Viewing users devices

In the administration interface, you can view information about all devices connected to user accounts.

1. Go to **Accounts** → **Users**.
2. Select a user and click **More Actions** → **Mobile Devices**.

   This displays a list of user's devices.
3. Select a device and
   - Click **Details** to view information about the device
   - Click **Remove** to delete unused devices from the list
   - Click Wipe to delete data from the device



Remotely deleting data from users' device

If users lose their devices, you can delete all the account data from the devices.

1. In the administration interface, go to **Accounts** → **Users**.
2. Select a user and click **More Actions** → **Mobile Devices**.
3. Select a device and click **Wipe**.

Once the device connects to the Kerio Connect server, Kerio Connect removes all the account data from the device.

Based on the device type and its operating system, you reset the device completely or you only clear out the account. If the device stores email attachments on a memory card, Kerio Connect deletes the attachments as well.

You can cancel the wipe before the device connects to the Kerio Connect server (click **Cancel Wipe**).

You can find details of the wipe process in the Security log.

Users can also wipe their own devices from their Kerio Connect Client.

User confirmation of the wipe action - windows mobile

On Windows Mobile operating systems, users must agree that the administrator performs the wipe action. They must confirm a dialog during the first data synchronization between the device and Kerio Connect. If they don't confirm, it is not possible to complete the synchronization process.

Setting a compatible Exchange ActiveSync version for specific mobile devices

Overview

New in Kerio Connect 8.5.1!

Kerio Connect supports Exchange ActiveSync 14. Some older mobile devices may experience problems with this version of Exchange ActiveSync (EAS) — for example, duplicated messages in their mailboxes, empty message folders, and so on.

If users have such problems, you can disable EAS 14 for individual devices in the configuration file. These devices then work with earlier versions of EAS and they do not:

- Synchronize notes
- Synchronize read/forward flags
- Show free/busy information

Editing the configuration file

1. Stop the Kerio Connect server.
2. Open the `mailserver.cfg` file.

   The default location is:

   - **Windows**: C:\Program Files\Kerio\MailServer
   - **Mac**: /usr/local/kerio/mailserver
   - **Linux**: /opt/kerio/mailserver
3. In the **LegacyDevices** list, add the devices for which you want to disable EAS 14 in the following format:

   ```
   <variable name="UserAgent">[device UserAgent string]</variable>
   ```

   Example for Android 4.1.1 and iPod devices:

```
<list name="LegacyDevices">
  <listitem>
    <variable name="UserAgent">Android/4.1.1-EAS-1.3</variable>
  </listitem>
  <listitem>
    <variable name="UserAgent">Apple-iPod/705.18</variable>
  </listitem>
</list>
```

You can find the device **UserAgent** string in the Debug log.
To start logging information about Exchange ActiveSync devices, right-click in the log area and select **Messages** → **ActiveSync Synchronization**.
The line to search for may look like this (you find the string at the end of the line):

```
[22/Jun/2015 21:38:58][4892] {activesync} Receiving request from 192.168.0.113:4916
Version: 12.1, Command: Ping, Device Id: Appl9C8303NA14N, Policy
Key: 1, Device Type: iPod, User: powaro, User Agent: Apple-iPod/705.18
```

To avoid low performance of your server, disable ActiveSync Synchronization logging after you acquire the UserAgent strings.

Some devices may have identical **UserAgent** strings. If you disable such string, you disable Exchange ActiveSync 14 and newer for all such devices.

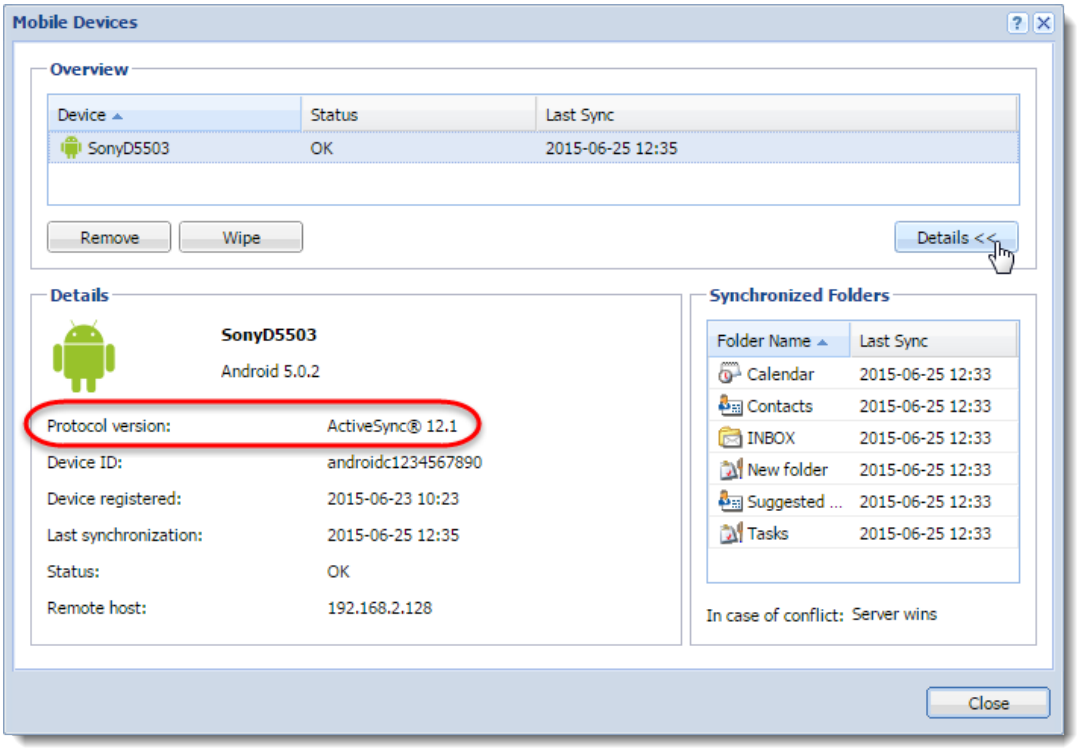
4. Save the file.
5. Start the Kerio Connect server.
6. Recreate the Kerio Connect account on the user's device.

Now the listed devices do not use Exchange ActiveSync version 14 and newer; they use any previous version available for them.

To verify the device uses a lower version of EAS:

1. In the administration interface, go to the **Accounts** → **Users**.
2. Select the users and click **More Actions** → **Mobile Devices**.
3. Select the device and click **Details**.

   The details show the protocol version the devices uses.


Mobile Devices
Overview
Device
Status
Last Sync
SonyD5503
OK
2015-06-25 12:35
Remove
Wipe
Details <<
Details
SonyD5503
Android 5.0.2
Protocol version:
ActiveSync® 12.1
Device ID:
androidc1234567890
Device registered:
2015-06-23 10:23
Last synchronization:
2015-06-25 12:35
Status:
OK
Remote host:
192.168.2.128
Synchronized Folders
Folder Name
Last Sync
Calendar
2015-06-25 12:33
Contacts
2015-06-25 12:33
INBOX
2015-06-25 12:33
New folder
2015-06-25 12:33
Suggested ...
2015-06-25 12:33
Tasks
2015-06-25 12:33
In case of conflict: Server wins
Close

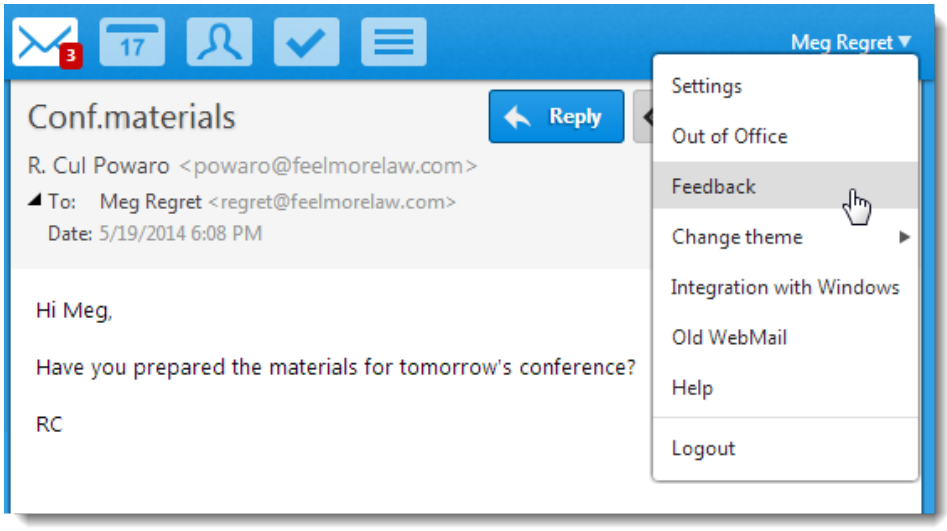
Providing feedback for Kerio products

Giving feedback through Kerio Connect Client

To give an opinion about Kerio Connect Client:

- In Kerio Connect 8.5 and newer — click your name, select **About** and **Send a suggestion**.

- In Kerio Connect 8.4 and older, click your name in Kerio Connect Client and select **Feedback**.



The feedback forum is displayed. It provides the same features as the admin forum (see the image above).

Kerio Connect — Legal notices

Trademarks and registered trademarks

Microsoft®, Windows®, Windows NT®, Windows Vista®, Internet Explorer®, Active Directory®, Outlook®, ActiveSync®, Entourage® and Windows Mobile® are registered trademarks of Microsoft Corporation.

Apple®, iCal®, Mac OS®, OS X ®, Safari™, Tiger™, Panther®, Open Directory logo™, Leopard®, Snow Leopard® and Lion® are registered trademarks or trademarks of Apple, Inc.

Palm®, Treo™, Pre™ and VersaMail® are registered trademarks or trademarks of Palm, Inc.

Red Hat® and Fedora™ are registered trademarks or trademarks of Red Hat, Inc.

SUSE®, openSUSE® and the openSUSE logo are registered trademarks or trademarks 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).

avast!® is registered trademark of AVAST Software.

eTrust™ is trademark of Computer Associates International, Inc.

ClamAV™ is trademark of Tomasz Kojm.

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.

AVG® is registered trademark of AVG Technologies.

IOS® is registered trademark of Cisco Systems, Inc.

NotifyLink® is registered trademark of Notify Technology Corporation.

BlackBerry® is registered trademark of Research In Motion Limited (RIM).

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.

Android™ and Nexus One™ are trademarks of Google Inc. This trademark can be used only in accord with Google Permissions.

DROID™ is trademark of Lucasfilm Ltd. and affiliated companies.

Motorola® is registered trademark of Motorola, Inc.

Used open source software

This product contains the following open-source libraries:

Appliance OS sources - Debian

Kerio Connect appliance is based on Debian GNU/Linux - Linux distribution composed of open source software from various sources.
Please refer to /usr/share/doc/*/copyright files installed inside the appliance for exact licensing terms of each package the appliance is built from.
The source package itself can be downloaded from http://kerio.com/...

Berkeley DB

Berkeley DB (BDB) is a computer software library that provides a "high-performance" embedded database, with bindings in C, C++, Java, Perl, Python, Ruby, Tcl, Smalltalk, and many other programming languages.
The Regents of the University of California. All rights reserved.

bindlib

DNS resolver library, linked by PHP on Windows.
Copyright © 1983, 1993 The Regents of the University of California. All rights reserved.
Portions Copyright © 1993 by Digital Equipment Corporation.

bluff

Bluff is a JavaScript port of the Gruff graphing library for Ruby. The Gruff library is written in Ruby.
Copyright © 2008-2009 James Coglan.
Original Ruby version © 2005-2009 Topfunky Corporation.

cfgwizard

Tool for initial configuration of Kerio Mailserver for Linux.
Distributed and licensed under GNU General Public License version 3.
Copyright © Kerio Technologies s.r.o.
Homepage: http://kerio.com/
Complete source code of the executable is available from http://kerio.com/...

CppSQLite

A C++ wrapper around the SQLite embedded database library .
Copyright ©2004 Rob Groves. All Rights Reserved.

excanvas

The ExplorerCanvas library allows 2D command-based drawing operations in Internet Explorer.

Copyright © 2006 Google Inc.

Firebird 2

This software embeds modified version of Firebird database engine distributed under terms of IPL and IDPL licenses.

All copyright © retained by individual contributors — original code Copyright © 2000 Inprise Corporation.

Modified source code is available from http:/kerio.com/

gettext

Gettext is a software translation toolkit. It is distributed under GNU General Public License version 3. Its libintl subpart is distributed under GNU Lesser General Public License version 2.1 or newer.

Copyright © 1984, 1989, 1990, 1991, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010 Free Software Foundation, Inc.

Complete source code is available at: http:/kerio.com/...

glib

GLib is a cross-platform software utility library. It is distributed under GNU Lesser General Public License version 2 or later.

Copyright © 2006-2010 Red Hat, Inc., Kerio Technologies s.r.o. and others.

Copyright © 1998-2010 Tim Janik, Red Hat, Inc., Kerio Technologies s.r.o. and others

Copyright © 1995-2010 Peter Mattis, Spencer Kimball, Josh MacDonald, Sebastian Wilhelmi, Kerio Technologies s.r.o. and others.

Complete source code is available at: http:/kerio.com/...

gmime

GMime is a C/C++ library which may be used for the creation and parsing of MIME messages. It is distributed under GNU Lesser General Public License version 2.1 or later.

Copyright © 2000-2009 Jeffrey Stedfast and Michael Zucchi

Complete source code is available at: http:/kerio.com/...

Heimdal Kerberos

Heimdal Kerberos is used only in Linux-oriented Kerio Connect versions.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Copyright ©1995-1997 Eric Young. 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.

ICU — International Components for Unicode (C/C++)

ICU is a mature, widely used set of C/C++ and Java libraries providing Unicode and Globalization support for software applications.
Copyright © 1995-2009 International Business Machines Corporation and others

intl — windows

libintl for Windows is a software library for native language support. It is released under LGPL license version 2 or later.
Copyright © 2008 Tor Lillqvist
The source code is available at: http:/kerio.com/...

JSColor

JSColor is a simple and user-friendly color picker for your HTML forms. It extends all desired <input> fields of a color selection dialog.
Jan Odvarko, http://odvarko.cz

libcurl

Libcurl is a free and easy-to-use client-side URL transfer library. This library supports the following protocols: FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP.
Copyright ©1996-2008, Daniel Stenberg.

libiconv

Libiconv converts from one character encoding to another through Unicode conversion. This product contains customized version of this library which is distributed and licensed under GNU Lesser General Public License version 3.
Copyright © 1999-2003 Free Software Foundation, Inc.
Author: Bruno Haible
Homepage: http://www.gnu.org/software/libiconv/
Complete source code is available at: http:/kerio.com/...

libIDL

LibIDL is a front-end for CORBA 2.2 IDL and Netscape's XPIDL.
Copyright © 1998, 1999 Andrew T. Veliath.

libdkim++

libdkim++ is a lightweight and portable DKIM (RFC4871) library for *NIX, supporting both signing and SDID/ADSP verification sponsored by Halon Security. libdkim++ has extensive unit test coverage and aims to fully comply with the current RFC.
Copyright © 2009,2010,2011 Halon Security <support@halon.se>

libmbfl

libmbfl is a streamable multibyte character code filter and converter library. The libmbfl library is distributed under LGPL license version 2.
Copyright ©1998-2002 HappySize, Inc. All rights reserved.
The library is available for download at: http://download.kerio.com/archive/

libMemcached

libMemcached is an open source C/C++ client library and tools for the memcached server. It has been designed to be light on memory usage, thread safe, and provide full access to server side methods.

libnewt

Newt is a programming library for color text mode, widget-based user interfaces. It is distributed and licensed under GNU Lesser General Public License.

Complete source code is available at: http:/kerio.com/...

libslang

S-lang is a C-like programming language, designed to be embedded in programs. It is distributed and licensed under GNU General Public License.

Homepage: http://www.s-lang.org

Complete source code is available at: http:/kerio.com/...

libspf2

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/).

libstdc++

C++ Standard Library is a collection of classes and functions, which are written in the core language and part of the C++ ISO Standard itself.

libtiff

Libtiff is a library for reading and writing Tagged Image File Format files.

Copyright © 1985, 1986 The Regents of the University of California
Copyright © 1990 by Sun Microsystems, Inc.
Copyright © 1996 Pixar
Copyright © 1999, Frank Warmerdam
Copyright © 2002, Andrey Kiselev
Copyright © 2003 Ross Finlayson
Copyright © 2009 Frank Warmerdam
Copyright © Copyright 1990 by Digital Equipment Corporation, Maynard, Massachusetts.
Copyright © 2004 Free Software Foundation, Inc.
Copyright © 1994 X Consortium
Copyright © 2003 Ross Finlayson
Copyright © 1996 BancTec AB
Copyright © 1996 Mike Johnson

libxml2

XML parser and toolkit.
Copyright ©1998-2003 Daniel Veillard. All Rights Reserved.
Copyright ©2000 Bjorn Reese and Daniel Veillard.
Copyright ©2000 Gary Pennington and Daniel Veillard
Copyright ©1998 Bjorn Reese and Daniel Stenberg.

myspell

Spellcheck library.
Copyright 2002 Kevin B. Hendricks, Stratford, Ontario, Canada And Contributors. All rights reserved.

MariaDB Connector/C

MariaDB Connector/C is used to connect applications developed in C/C++ to MariaDB and MySQL databases.
Copyright © 2010 Michael Bell <michael.bell@web.de>
Copyright © 2000 MySQL AB & MySQL Finland AB & TCX DataKonsult AB
Copyright © 1989, 90, 91, 92, 93, 94 Free Software Foundation, Inc.
Copyright © 2000 MySQL AB
Copyright © 2010 - 2012 Sergei Golubchik and Monty Program Ab
Copyright © 2013 by MontyProgram AB
Copyright © 2012 Monty Program AB
Copyright © 2011, Monty Program Ab
Copyright © 2011,2013 Monty Program Ab;
Copyright © 2010 Sergei Golubchik and Monty Program Ab
Copyright Abandoned 1996, 1999, 2001 MySQL AB
Copyright © 2006-2011 The PHP Group
Copyright © 2000, 2011 MySQL AB & MySQL Finland AB & TCX DataKonsult AB
Copyright © 2011, Oleksandr Byelkin
Copyright © 2011,2012 Oleksandr Byelkin
Copyright © 1995-2003, 2010 Jean-loup Gailly.

Copyright © 1995-2005 Jean-loup Gailly.
Copyright © 1995-2006 Jean-loup Gailly.
Copyright © 1995-2010 Jean-loup Gailly
Copyright © 1995-2010 Jean-loup Gailly and Mark Adler
Copyright © 1995-2003, 2010 Mark Adler
Copyright © 1995-2005, 2010 Mark Adler
Copyright © 1995-2006, 2010 Mark Adler
Copyright © 1995-2007 Mark Adler
Copyright © 1995-2003, 2010 Mark Adler
Copyright © 1995-2009 Mark Adler
Copyright © 1995-2010 Mark Adler
Copyright © 2004, 2005, 2010 Mark Adler
Copyright © 2004, 2010 Mark Adler
Copyright © 2006-2011 The PHP Group

Nginx

nginx [engine x] is an HTTP and reverse proxy server, as well as a mail proxy server, written by Igor Sysoev.
Copyright © 2002-2014 Igor Sysoev
Copyright © 2011-2014 Nginx, Inc.
Copyright © Maxim Dounin
Copyright © Unbit S.a.s. 2009-2010
Copyright © 2008 Manlio Perillo (manlio.perillo@gmail.com)
Copyright © Austin Appleby
Copyright © Roman Arutyunyan
Copyright © Unbit S.a.s. 2009-2010
Copyright © Valentin V. Bartenev
Copyright © Yichun Zhang (agentzh)
Copyright © 2009-2014, Yichun "agentzh" Zhang <agentzh@gmail.com>, CloudFlare Inc.
Copyright © 2010-2013, Bernd Dorn.

OpenLDAP

Freely distributable LDAP (Lightweight Directory Access Protocol) implementation.
Copyright © 1998-2007 The OpenLDAP Foundation
Copyright ©1999, Juan C. Gomez, All rights reserved
Copyright ©2001 Computing Research Labs, New Mexico State University
Portions Copyright©1999, 2000 Novell, Inc. All Rights Reserved
Portions Copyright ©PADL Software Pty Ltd. 1999
Portions Copyright ©1990, 1991, 1993, 1994, 1995, 1996 Regents of the University of Michigan
Portions Copyright ©The Internet Society (1997)
Portions Copyright ©1998-2003 Kurt D. Zeilenga
Portions Copyright ©1998 A. Hartgers
Portions Copyright ©1999 Lars Uffmann

Portions Copyright ©2003 IBM Corporation
Portions Copyright ©2004 Hewlett-Packard Company
Portions Copyright ©2004 Howard Chu, Symas Corp.

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/).
This product includes cryptographic software written by Eric Young.
This product includes cryptographic software written by Tim Hudson.

PHP

PHP is a widely-used scripting language that is especially suited for Web development and can be embedded into HTML.
Copyright ©1999-2006 The PHP Group. All rights reserved.
This product includes PHP software, freely available from http://www.php.net/software/

proxy-libintl

proxy-libintl is a small static library. It acts as a proxy for the the DLL from gettext.
Tor Lillqvist <tml@iki.fi>, July 2008
Complete source code is available at: http:/kerio.com/...

sdbm

This product includes software developed by the Apache Software Foundation (http://www.apache.org/)

slf4j

slf4j is a simple logging facade for Java.
Copyright ©2004-2010 QOS.CH
Copyright ©2004-2005 SLF4J.ORG
Copyright ©2005 - 2010, James Auldridge
Copyright ©1999-2005 The Apache Software Foundation.

Tigase

The Tigase Jabber/XMPP Server is Open Source and Free (GPLv3) {Java} based server.
Copyright ©2004 Tigase.org. <http://www.tigase.org/>
Copyright ©2001-2006 Tigase Developers Team. All rights Reserved.
Copyright ©2004-2011 "Artur Hefczyc" <artur.hefczyc@tigase.org>
Copyright ©2009 "Tomasz Sterna" <tomek@xiaoka.com>
Copyright ©2001-2008 Julien Ponge, All Rights Reserved.
Copyright© 2008 "Bartosz M. Małkowski" <bartosz.malkowski@tigase.org>

zlib

General-purpose library for data compressing and decompressing.
Copyright ©1995-2005 Jean-Loup Gailly and Mark Adler.