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 this article 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. Kerio Connect is installed using the standard installation wizard. The initial configuration is performed (see section Configuration wizard).

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

Kerio Connect Engine is started (immediately or after restart). It runs as a service.

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. Kerio Connect is installed using the standard installation wizard into folder `/usr/local/kerio/mailserver`. The initial configuration is performed (see section Configuration wizard)

4. The Kerio Connect service starts automatically upon the computer system startup. To run or restart the service, run **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 (for *Mac OS X 10.5 Leopard* or newer):

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
```

If possible, it is recommended to stop/start the service in **System Preferences** → **Others** → **Kerio Connect Monitor**

⚠ Do not delete the Kerio Connect installation package — it includes Kerio Connect Uninstaller.

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. Kerio Connect is installed into folder `/opt/kerio/mailserver`.

4. Run the configuration wizard (see section Configuration wizard).

New installation

Start the installation using this command:

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

Example:

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

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

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

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

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

⚠ The Kerio Connect Engine must be stopped while the configuration wizard is running.

Starting and stopping the server

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

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

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

Kerio Connect must be run under the user `root`.

If your distribution has `systemd` available, use the following command to start/stop Kerio Connect:

```
systemctl start kerio-connect.service
systemctl stop 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. Kerio Connect is installed into folder `/opt/kerio/mailserver`.

4. Run the configuration wizard (see section Configuration wizard).

New installation

To install either of the installation packages, double-click on its icon or use for example the following command in the terminal:

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

Example:

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

It is recommended to read carefully the DEBIAN-README file immediately upon the installation. The file can be found in the installation directory in folder doc.

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

```
cd /opt/kerio/mailserver
dpkg-reconfigure kerio-connect
```

Starting and stopping the server

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

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

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

Kerio Connect must run under user root.

When installing on Debian with a graphical user interface, open the installation package with the gdebi installer (right-click the file and **Open with**).

Configuration Wizard

The configuration wizard helps to set the basic parameters for Kerio Connect. These include:

- primary domain
- administrator's account
- data store

It also creates special files where the server configuration is saved.

If you do not use the configuration wizard, it will not be possible to login to the Kerio Connect's administration interface.

On Windows and Mac, the configuration file is run automatically during the installation.

On Linux, use the following commands:

Linux — RPM

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

Linux — DEB

```
cd /opt/kerio/mailserver
dpkg-reconfigure kerio-connect
```

When a corresponding package is installed, user will be informed that the wizard is available. This information is also provided by the daemon if it detects that the wizard has not been used yet.

Kerio Connect must be stopped while settings are changed in the configuration wizard.
After running the wizard, existing configuration files will be deleted.

Configuration files

The wizard creates the following configuration files:

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.

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

Upgrading Kerio Connect

What can be upgraded

Once 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.

You can upgrade:

- Kerio Connect server
- Kerio Outlook Connector
- Kerio Outlook Connector (Offline Edition)
- Kerio Sync Connector

Kerio Connect can automatically check whether there are new versions available:

1. Go to section **Configuration** → **Advanced Options** → **tab Software Updates**.
2. Select option **Automatically check for new versions**.
3. Kerio Connect will checks for updates every 24 hours.
4. For immediate check of new versions, click **Check now**.
5. You can enable automatic updates of Kerio Outlook Connector (Offline Edition) on client stations.

The **Do not install updates** option may come useful whenever the new version of Kerio Outlook Connector (Offline Edition) is released that does not affect the module's correct functionality (this also means that a popup notice is not displayed upon every startup of Microsoft Outlook).

If the new version is critical for correct functioning of the module (the version installed is not compatible with the server version), this information will be displayed in this section.

Once a new version is available, the **Software Updates** tab will display a link to the download page.

⚠ If Kerio Connect is used in production, we do not recommend enabling **Check also for beta versions**.

Configuring HTTP proxy server

If the computer with Kerio Connect installed is behind a firewall, you can connect it to the Internet (for updates) via a proxy server.

1. Go to section **Configuration** → **Advanced Options** → **tab HTTP Proxy**.
2. Check option **Use HTTP proxy for ...**
3. Specify the address and port of the proxy server.
4. If required, enter the authentication data.
5. Confirm the settings.

Microsoft Windows

To upgrade Kerio Connect on Microsoft Windows, simply download and run the installation package. The program will detect the installation directory, stop running components (Kerio Connect engine and Kerio Connect Monitor) and replace files with new ones automatically. All settings and stored messages will be available after upgrade.

If Kerio Connect is upgrade successfully, a backup of the configuration files of the previous version is saved in the directory where Kerio Connect is installed in folder `UpgradeBackups`.

Mac OS X

To upgrade Kerio Connect on Mac OS X, simply download and run the installation package. The program will detect the installation directory, stop running components (Kerio Connect engine and Kerio Connect Monitor) and replace files with new ones automatically. All settings and stored messages will be available after upgrade.

Linux — RPM

To upgrade Kerio Connect on Linux RPM, use the following command:

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

Use this command to fix the current installation:

```
# rpm -U --force <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

For information on upgrading Kerio Connect VMware Virtual Appliance, read this article.

Troubleshooting

If any problems regarding updates occur, check the Debug log — right-click the Debug log area and check **Messages** → **Update Checker Activity**).

Uninstalling Kerio Connect

How to uninstall Kerio Connect

Windows operating system

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

Decide whether you wish to delete also the data store and configuration files of Kerio Connect. The uninstall wizard offers an option to keep them.

Mac OS X operating system

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

Decide whether you wish to delete also the data store and configuration files of Kerio Connect. The uninstall wizard offers an option to keep them.

Linux operating system — RPM

You can uninstall Kerio Connect using the following command:

`# rpm -e kerio-connect` (for standard Kerio Connect)

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

Linux operating system — DEB

You can uninstall Kerio Connect using the following command:

`# apt-get remove kerio-connect` (for standard Kerio Connect)

⚠ During the uninstallation, only file from the original package and unchanged files are deleted. The configuration files, data store and other changed or added files will be 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 command:

`# apt-get remove --purge kerio-connect` (for standard Kerio Connect)

Switching from 64-bit installation of Kerio Connect back to 32-bit installation on Microsoft Windows

Switching from 64-bit installation to 32-bit installation

We recommend to perform full backup of Kerio Connect before proceeding

To switch your Kerio Connect from the 64-bit version back to 32-bit version, follow these steps:

1. Uninstall the 64-bit version of your Kerio Connect.

   ⚠ Do not remove configuration files and data store during the process.

2. Move folder `MailServer` to directory `Program Files (x86)`.

   From location `C:\Program Files\Kerio\MailServer\` to location `C:\Program Files (x86)\Kerio\MailServer\`

3. Open file `mailserver.cfg` (located in `C:\Program Files (x86)\Kerio\MailServer\`) and change all paths from `C:\Program Files\` to `C:\Program Files (x86)\`.

4. Run the 32-bit installation.

   Do not change the destination folder and select option **Keep existing configuration**.

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.

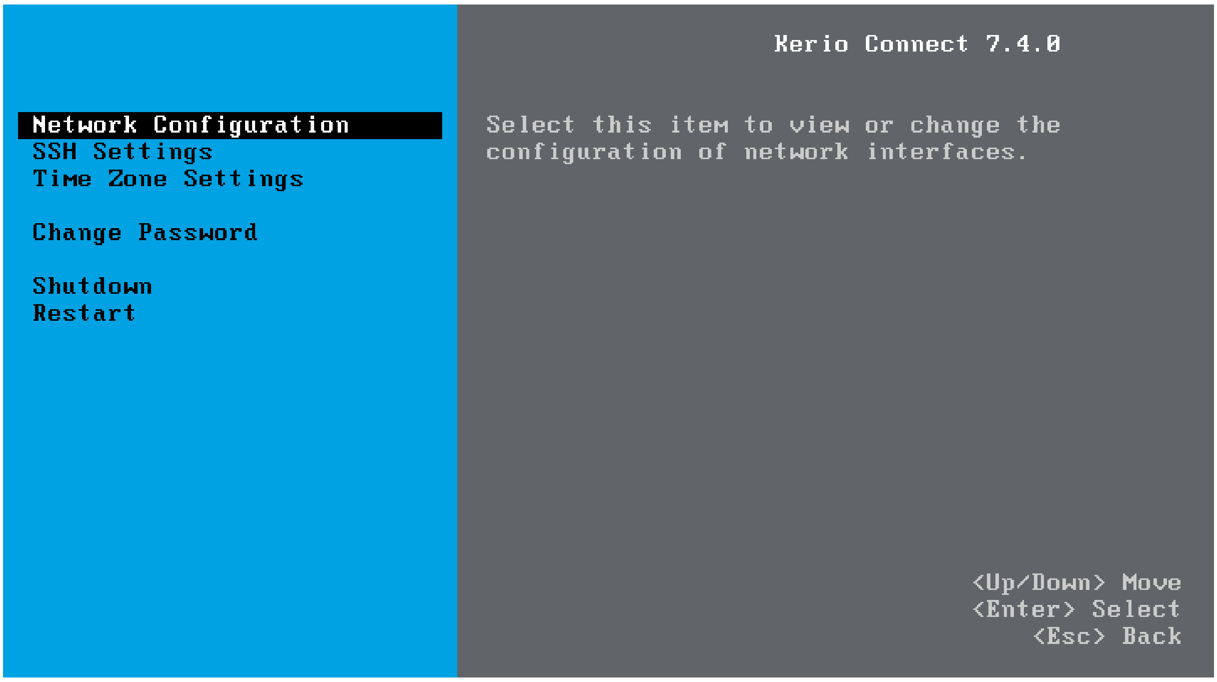
Upon the first startup, configuration wizard gets started where the following entries can be set:

- 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



Kerio Connect 7.4.0

Select this item to view or change the configuration of network interfaces.

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.

Kerio Connect updates:

1. Download the deb package to your computer
2. Use SCP/SSH to move it to VMware Appliance
3. Use command `dpkg` to upgrade

Debian Linux updates: by the standard method using the `apt-get` command.

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 / old WebMail)

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 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:

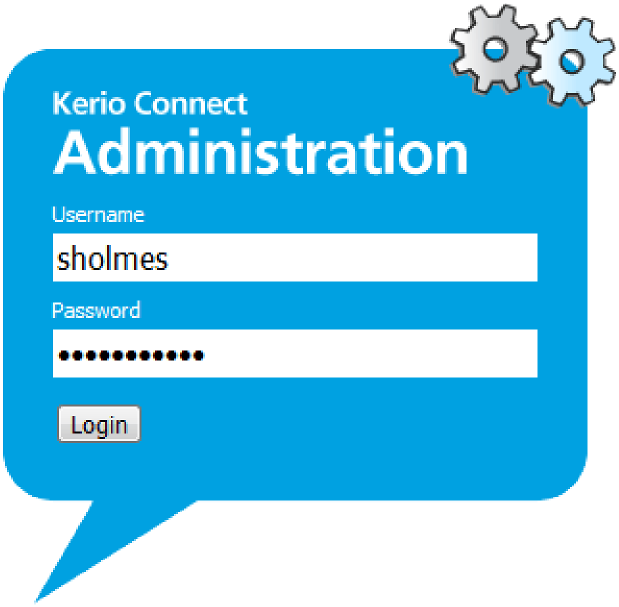
```
kerio.connect.name/admin
```

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.



Kerio Connect Administration

Username: sholmes

Password: ●●●●●●●●●●●

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:

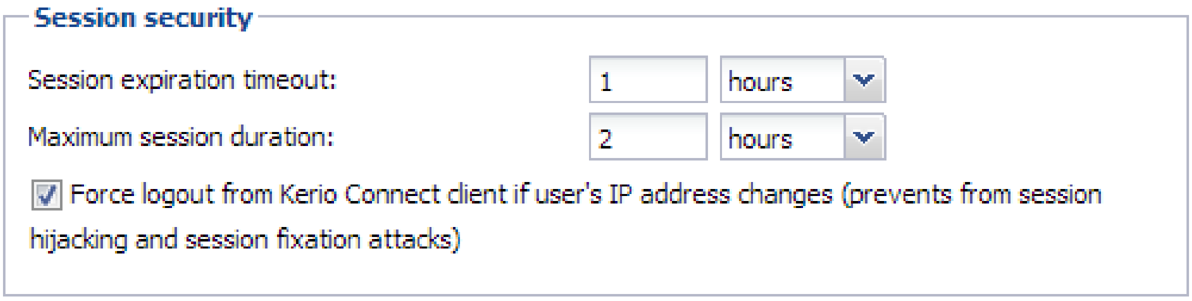
1. In the administration interface, go to section **Configuration** → **Advanced options** → **tab Kerio Connect client**.
2. In the **Session security** section, set the timeout for
   - **session expiration** — Kerio Connect will end the session after the set timeout without any activity in an interface

     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.



Session security

Session expiration timeout: 1 hours

Maximum session duration: 2 hours

☑ Force logout from Kerio Connect client if user's IP address changes (prevents from session hijacking and session fixation attacks)

Figure 2 Session security

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

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, open your browser and enter URL in the following format:

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

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

If the user does not belong to the primary domain, enter also the domain name (e.g. `wsmith@notprimarydomain.com`).

Licenses in Kerio Connect

Licenses in Kerio Connect

Licenses are counted by number of users.

Number of users means the number of mailboxes/accounts:

- created in Kerio Connect
- mapped from a directory service

  When mapped from the LDAP database of a directory service, all users created in this database are counted as individual licenses (all active users).

- imported from a domain

Number of mailing lists, resources, aliases and domains is not limited. The internal administrator account does not count as a license as well.

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

If you wish to extend the number users allowed by your license, visit the Kerio Connect website.

For information on how to register your licence, read this article.

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).

Registering Kerio Connect

Why to register Kerio Connect

Without registration, Kerio Connect behaves as a **trial version**. The limitations of the trial versions are:

- Time — after 30 days from installation, Kerio Connect Engine will be disabled.
- Sophos antivirus engine — the database cannot be updated for unregistered trial versions.
- Exchange ActiveSync — disabled for unregistered trial versions.

If you register a trial version, you will receive technical support during the entire trial period (for more information, visit the Support page at Kerio Technologies site).

It is not necessary to reinstall Kerio Connect after registration.

Registering Kerio Connect in the administration interface

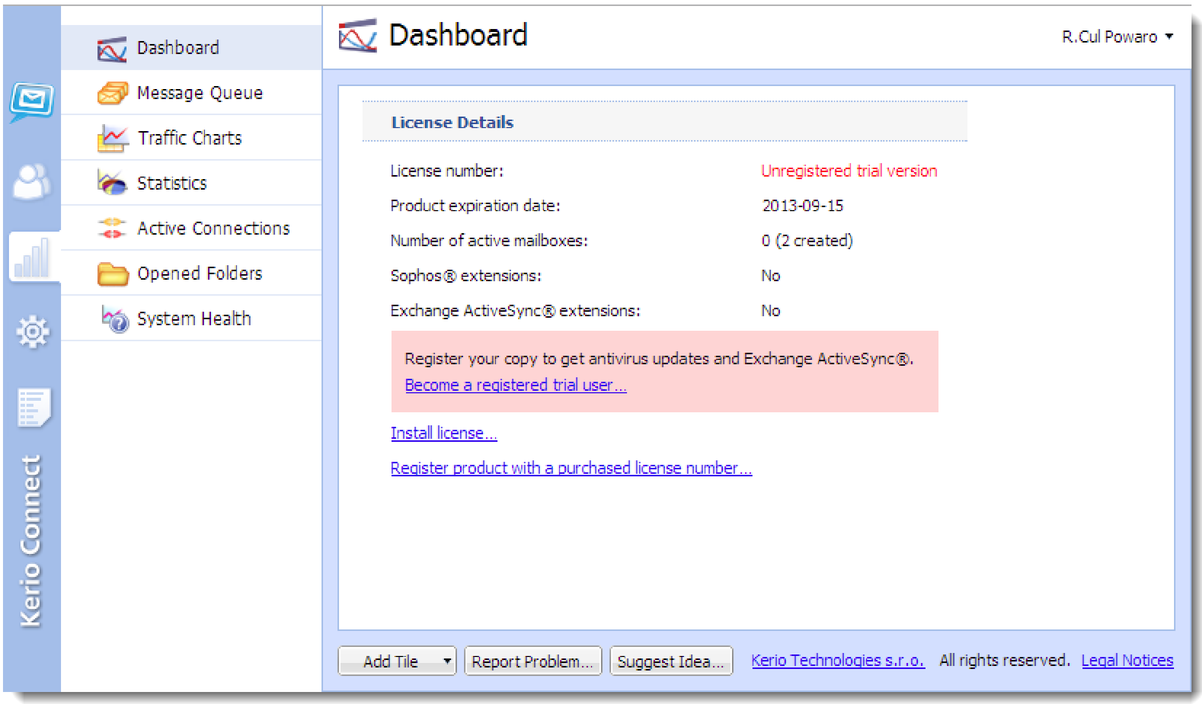
You can register Kerio Connect from the **Dashboard** of the administration interface.

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

Registering a trial version

1. Login to the administration interface and click on **Become a registered trial user** on the **Dashboard**.
2. Fill in the info in the opened dialog window.
3. Confirm.

A **Trial ID** is created.



License Details

License number: Unregistered trial version

Product expiration date: 2013-09-15

Number of active mailboxes: 0 (2 created)

Sophos® extensions: No

Exchange ActiveSync® extensions: No

Register your copy to get antivirus updates and Exchange ActiveSync®.
Become a registered trial user...

Install license...

Register product with a purchased license number...

Figure 1 Product Registration

Trial ID

Your Trial ID is displayed on the dashboard. Use this Trial ID whenever you contact the technical support.

If you decide to reinstall your trial version, backup the `mailserver.cfg` file (in the Kerio Connect installation folder) which contains also your Trial ID.

Registering full version

If you registered a trial version and you have purchase the full version of Kerio Connect, the license file will be automatically imported to your product within 24 hours from your purchase. The Trial ID will become your license number.

If you haven't registered your trial version:

1. In the Kerio Connect dashboard, click on **Register product with a purchased license number**.
2. Type the information required, including your license number (acquired upon purchase).
3. Kerio Connect will contact the registration server, checks the validity of the data inserted and automatically downloads the license file (digital certificate).
4. Finish the installation wizard.

Installing license manually

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

Registering Kerio Connect via WWW

You purchased a license and your Kerio Connect cannot access the Internet? Follow these steps to register:

1. Go to https://secure.kerio.com/reg/
2. Register using your purchased license number.
3. Once you register, you will receive a license key (the *.key file including the corresponding certificate) which must be imported to Kerio Connect.

> The trial version of Kerio Connect cannot be registered via the website.

Accessing Kerio Connect administration

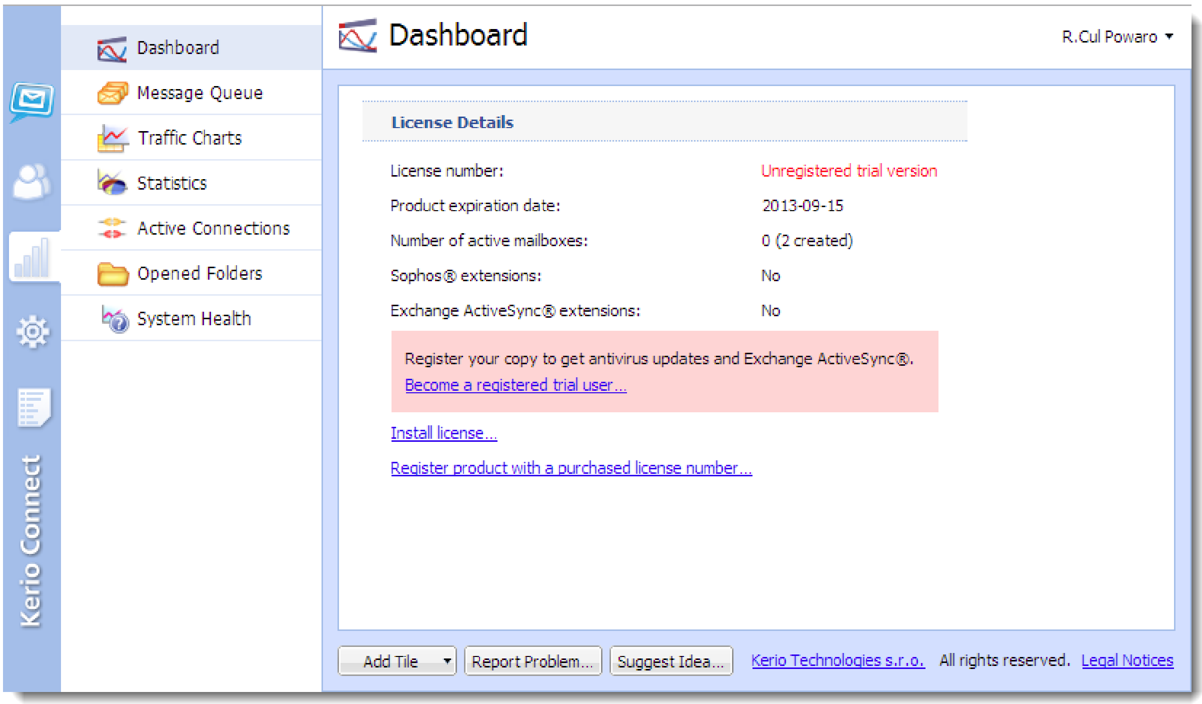
Accessing Kerio Connect administration

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.



License Details

License number: Unregistered trial version

Product expiration date: 2013-09-15

Number of active mailboxes: 0 (2 created)

Sophos® extensions: No

Exchange ActiveSync® extensions: No

Register your copy to get antivirus updates and Exchange ActiveSync®.
Become a registered trial user...

Install license...

Register product with a purchased license number...

Figure 1 Welcome to Kerio administration

Accessing the administration interface remotely

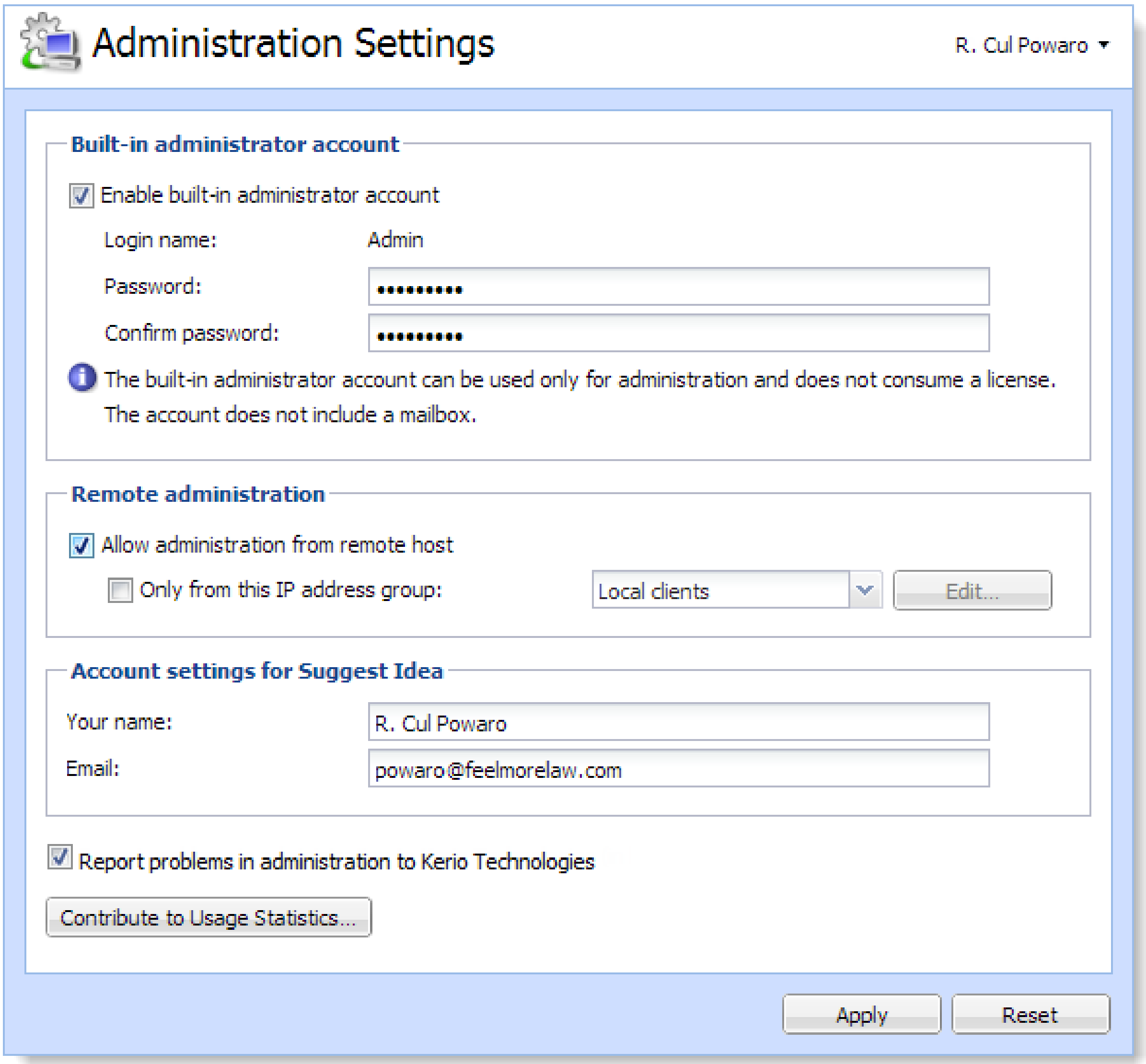
Administrators can access the administration interface:

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.



Administration Settings

R. Cul Powaro ▾

Built-in administrator account

☑ Enable built-in administrator account

Login name:	Admin
Password:	••••••••••
Confirm password:	••••••••••

The built-in administrator account can be used only for administration and does not consume a license. The account does not include a mailbox.

Remote administration

☑ Allow administration from remote host

□ Only from this IP address group: Local clients

Account settings for Suggest Idea

Your name:	R. Cul Powaro
Email:	powaro@feelmorelaw.com

☑ Report problems in administration to Kerio Technologies

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.

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.

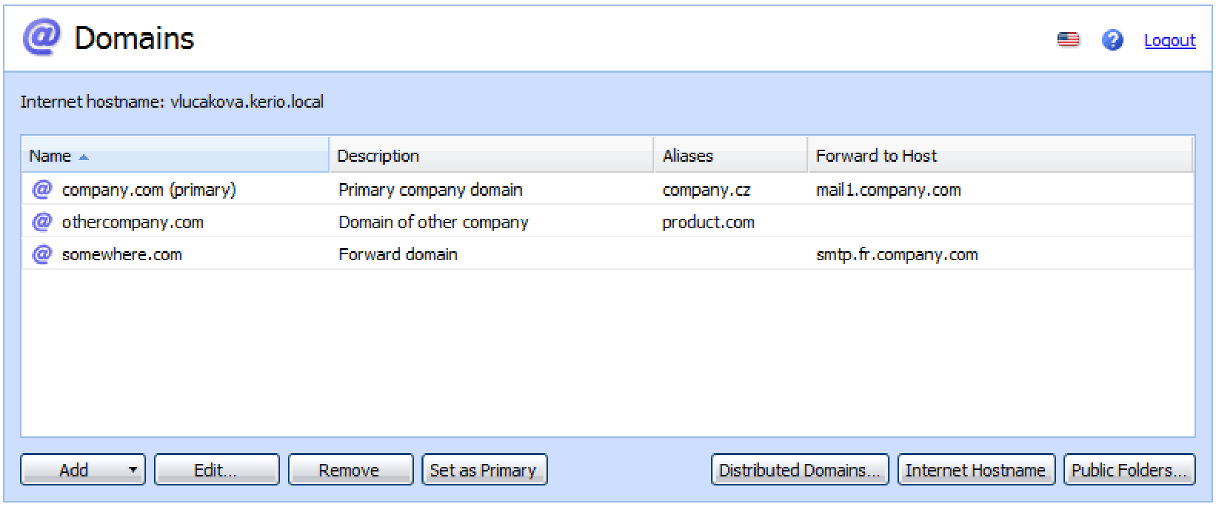
Email domain can differ from the name of the server where Kerio Connect is installed. See the following example:

- 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**.



Internet hostname: vlucakova.kerio.local

Name	Description	Aliases	Forward to Host
company.com (primary)	Primary company domain	company.cz	mail1.company.com
othercompany.com	Domain of other company	product.com	
somewhere.com	Forward domain		smtp.fr.company.com

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.

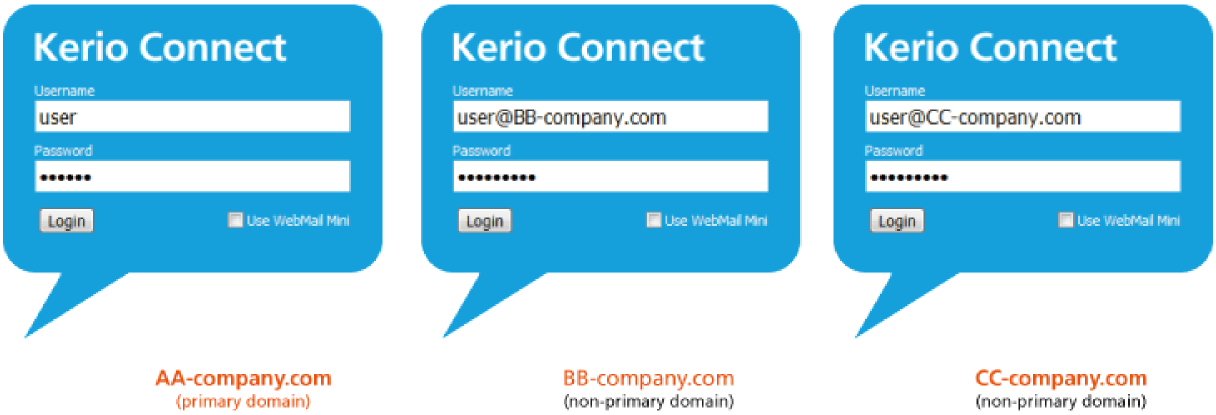
Upon initializing the SMTP communication, the EHLO command is used for retrieving reverse DNS record. The server that communicates with Kerio Connect can perform checks of the reverse DNS record.

> 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.



Username: user
Password: ••••••

Username: user@BB-company.com
Password: •••••••••

Username: user@CC-company.com
Password: •••••••••

Figure 2 Login to Kerio Connect client for users in different domains in one instance of Kerio Connect

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. Enter the domain name and description.

   You should use description for better reference if you create multiple domains.

3. Set limit for the maximum number of domain users who can connected to Kerio Connect at a time (recommended for the ISPs).

   For better reference, 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

In Kerio Connect 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 to 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 (WebMail) login and domain login.

⚠

- Mapping is one-way only. Data are 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.

Connecting to directory service

To connect domains to a directory service:

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click the domain and go to tab **Directory Service**.

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

4. Configure the directory service.

Microsoft Active Directory

1. 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 it to the DNS name/IP address.

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

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

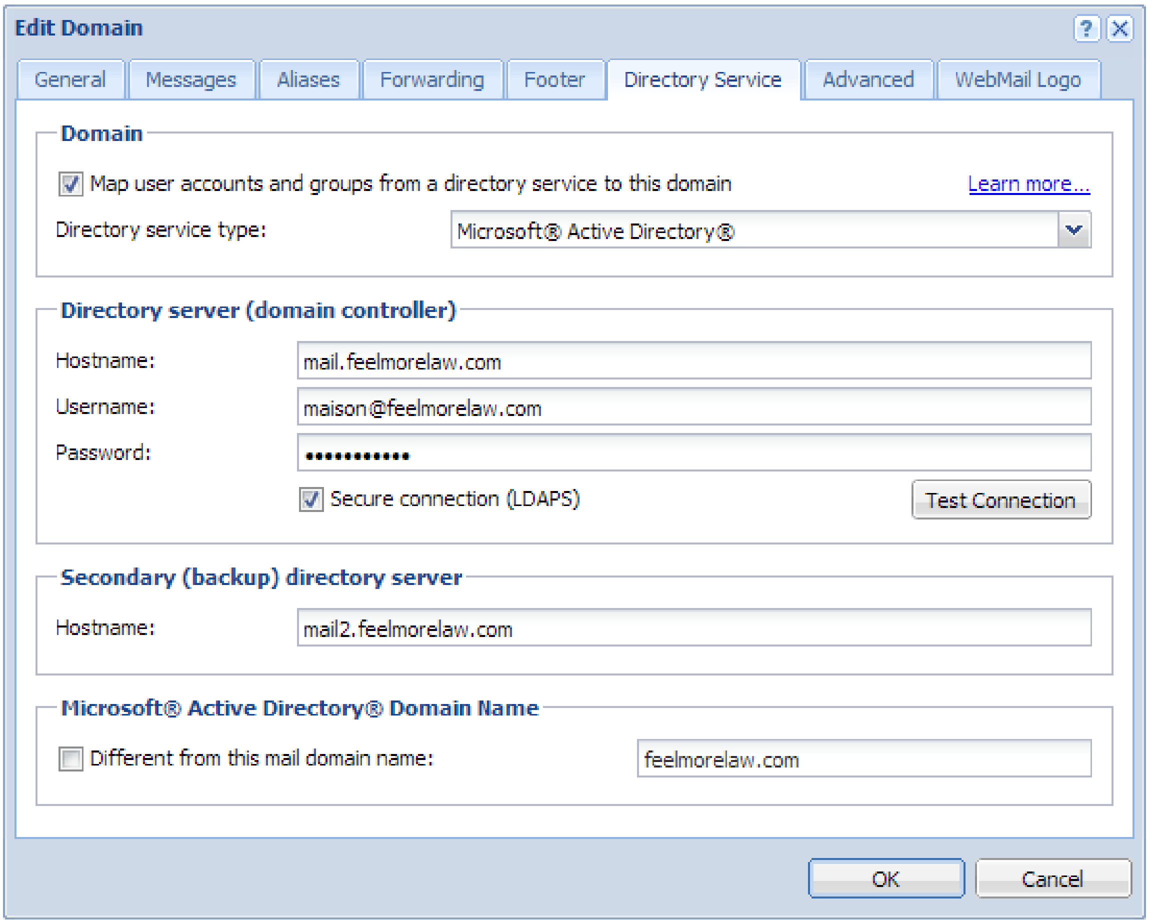
   If you enable LDAPS, the DNS names is required in step 1.

4. **Test connection** to verify you entered the correct data.

5. Save the settings.

Now you can map users to Kerio Connect.

Install Kerio Active Directory Extension to fully benefit from the connection.



Domain

☑ Map user accounts and groups from a directory service to this domain

Directory service type: Microsoft® Active Directory®

Directory server (domain controller)

Hostname: mail.feelmorelaw.com

Username: maison@feelmorelaw.com

Password: •••••••••••

☑ Secure connection (LDAPS)

Secondary (backup) directory server

Hostname: mail2.feelmorelaw.com

Microsoft® Active Directory® Domain Name

☐ Different from this mail domain name: feelmorelaw.com

Figure 1 Configuring Microsoft Active Directory

Apple Open Directory

1. 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.

2. Type **Username** and **Password** of an Apple Open Directory administrator with full access rights to the administration.

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

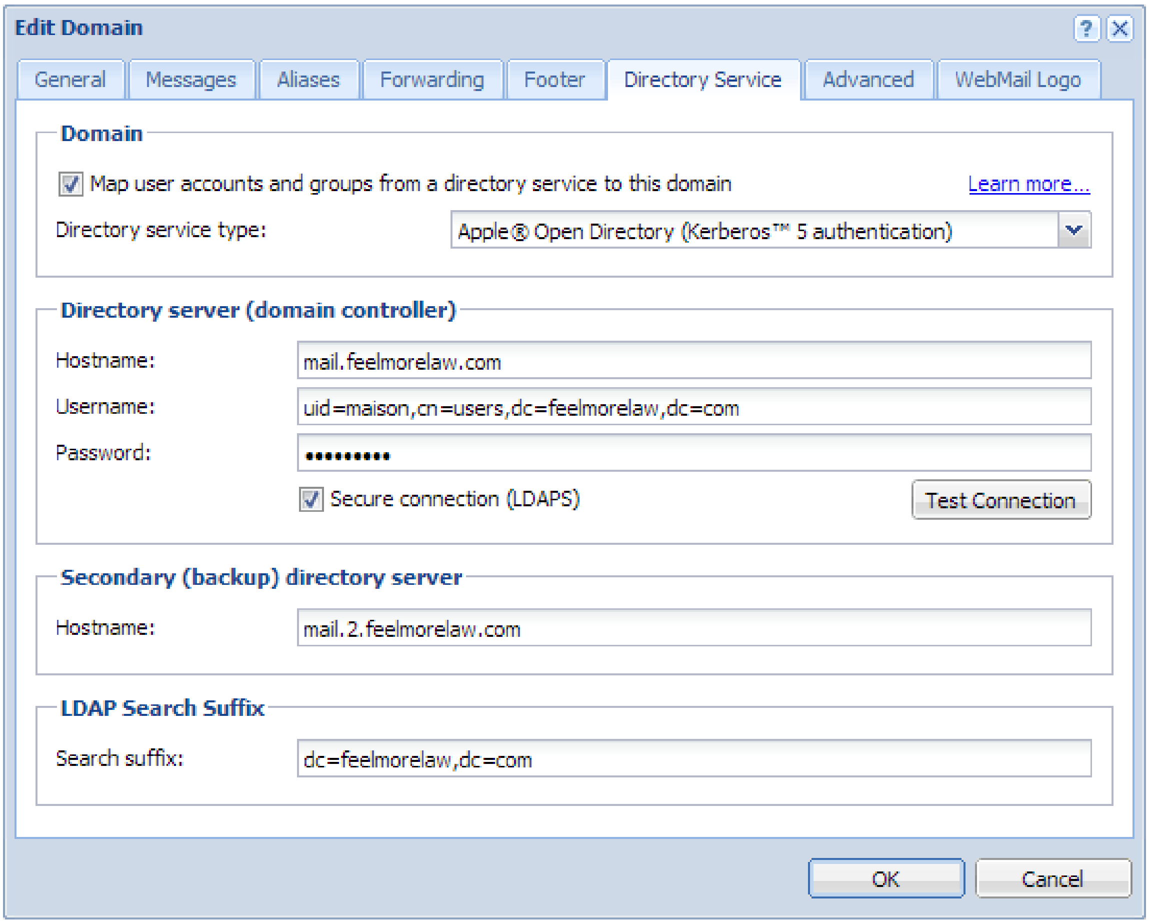
   If you enable LDAPS, the DNS names is required in step 1.

4. **Test connection** to verify you entered the correct data.

5. Save the settings.

Now you can map users to Kerio Connect.

Install Kerio Open Directory Extension to fully benefit from the connection.



Domain

☑ Map user accounts and groups from a directory service to this domain

Directory service type: Apple® Open Directory (Kerberos™ 5 authentication)

Directory server (domain controller)

Hostname: mail.feelmorelaw.com

Username: uid=maison,cn=users,dc=feelmorelaw,dc=com

Password: ••••••••••

☑ Secure connection (LDAPS)

Secondary (backup) directory server

Hostname: mail.2.feelmorelaw.com

LDAP Search Suffix

Search suffix: dc=feelmorelaw,dc=com

Figure 2 Configuring Apple Open Directory

Mapping users

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

Troubleshooting

All information about directory service can be found in the Config log.

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

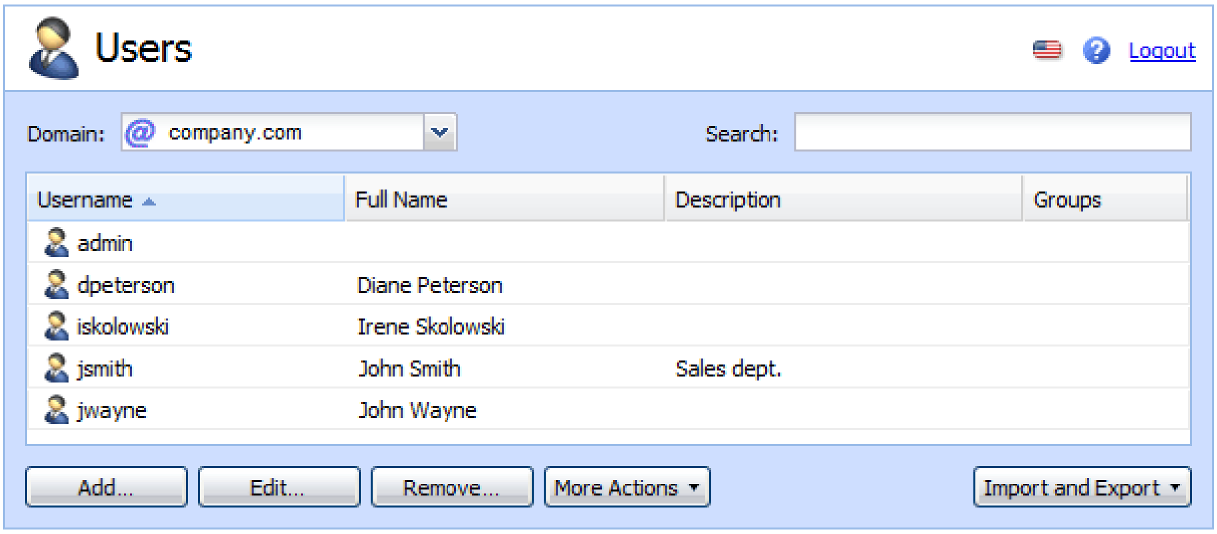
What are user accounts

In Kerio Connect, user accounts represent physical email boxes.

User accounts are used to:

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

Users are managed in the administration interface in section **Accounts** → **Users**.



Domain: company.com

Search:

Username	Full Name	Description	Groups
admin			
dpeterson	Diane Peterson		
iskolowski	Irene Skolowski		
jsmith	John Smith	Sales dept.	
jwayne	John Wayne		

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 account can also be imported to Kerio Connect. Read this article for more info.

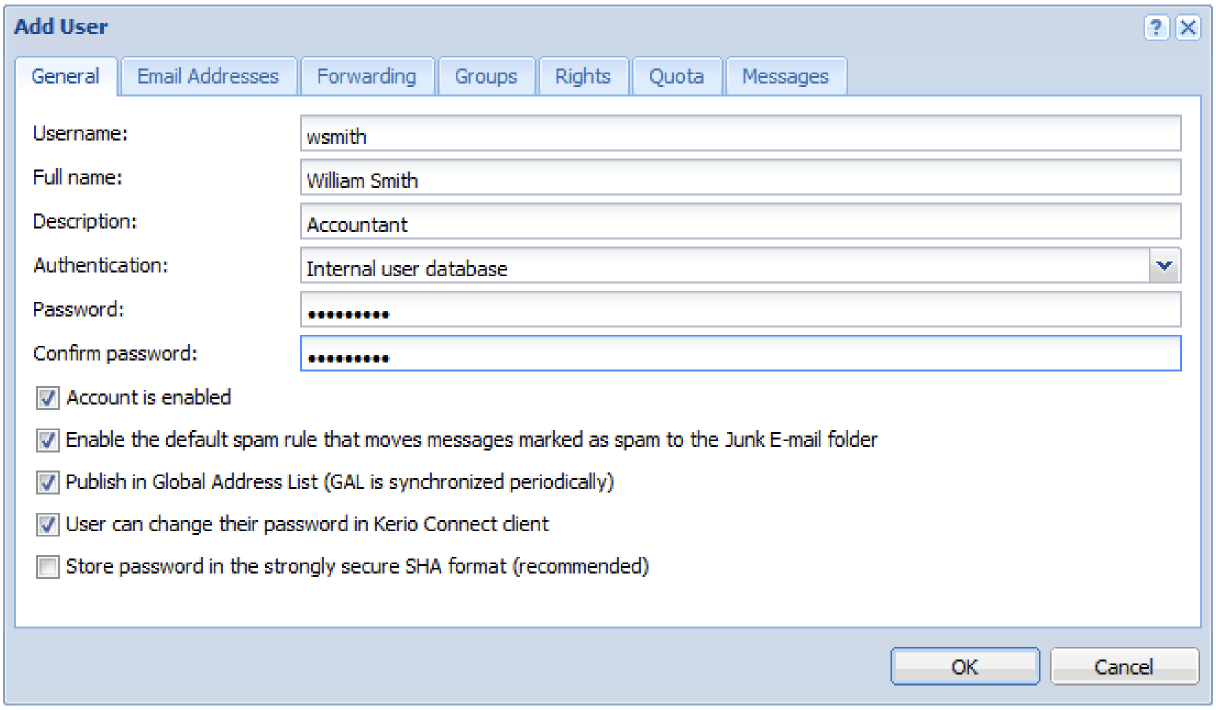
Creating local accounts

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

1. Go to section **Accounts** → **Users** and select a domain in which you want to create an account.
2. Click **Add** → **Add Local User** (or use a template).
3. On the **General** tab, enter a username and password.

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

4. Now, you can save the settings.



Add User

Username: wsmith

Full name: William Smith

Description: Accountant

Authentication: Internal user database

Password: •••••••••

Confirm password: •••••••••

☑ Account is enabled

☑ Enable the default spam rule that moves messages marked as spam to the Junk E-mail folder

☑ Publish in Global Address List (GAL is synchronized periodically)

☑ User can change their password in Kerio Connect client

□ Store password in the strongly secure SHA format (recommended)

Figure 2 Adding users

Although other settings of user accounts are optional, you can:

- 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

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

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. In the displayed dialog, select any users you wish to map to Kerio Connect (you can add users later).
4. Click on **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 section **Configuration** → **Definitions** → **User Templates**.
2. Enter 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 on **Add** → **Use Template** and complete the user settings.

Deleting user accounts

User accounts can be suspended temporarily or deleted permanently.

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 availbale in Kerio Connect.

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

User now cannot access Kerio Connect client (WebMail) or the Kerio Connect administration.

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

This action is not identical to account blocking when a password guessing attack occurs.

Deleting users permanently

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

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

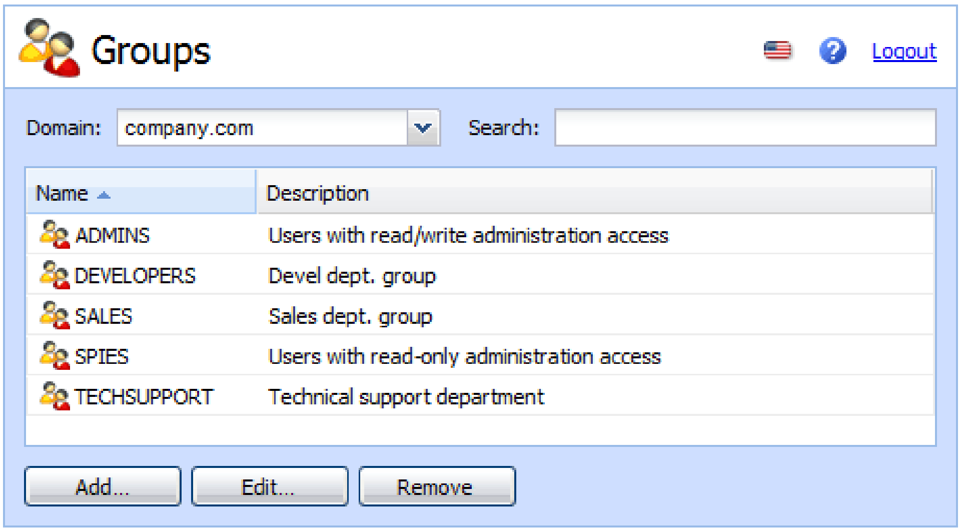
Creating user groups in Kerio Connect

What are user groups

With user groups in Kerio Connect, you can:

- set access rights to Kerio Connect administration for multiple users
- deliver messages to multiple users via a single email address within a particular domain (see also mailing lists)

User groups are managed in the administration interface in section **Accounts** → **Groups**.



Domain: company.com

Search:

Name	Description
ADMINS	Users with read/write administration access
DEVELOPERS	Devel dept. group
SALES	Sales dept. group
SPIES	Users with read-only administration access
TECHSUPPORT	Technical support department

Figure 1 Groups

Creating user groups

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

User groups must 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.

Creating local groups

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

1. Go to section **Accounts** → **Groups** and select a domain in which you want to create a group.
2. Click **Add**.

3. On the **General** tab, enter a group name.

4. On tab **Users** click **Add**.

5. Select users you wish to add to the group and confirm.

> You can also go to **Accounts** → **Users** and select a group in user's settings.

6. Save the settings.

Although other settings of user groups are optional, you can:

- create email addresses for groups

  > You can create as many addresses as you wish. You can even use an existing username — just bear in mind that any messages meant for the group will also be delivered to the original user.

- configure access rights for the administration interface

- export all members into a CSV file (with name `users_domain_group_date.csv`).

> Users from a directory service cannot be added to local groups.

Mapping groups from a directory service

To add groups from a directory service, you must:

- connect Kerio Connect to a directory service

- activate groups in the administration interface

To activate the groups:

1. Go to section **Accounts** → **Groups** and select a domain in which you want to create a group.

2. Click **Add** → **Add From a Directory Service**.

3. In the displayed dialog, select groups you wish to map to Kerio Connect (you can add groups later).

4. Click **Next.**

5. Click **Finish.**

The groups are displayed in section **Accounts** → **Groups**.

Local users cannot be added to groups from a directory service.

Exporting group members

To see alist of members in each group, Kerio Connect allows you to export members of individual groups into a CSV file.

To export members of a group:

1. In the administration interface, go to section **Accounts** → **Groups**.

2. Double click a group.

3. On tab **Users** click **Export.**

Kerio Connect saves the CSV file to your harddrive with name

`users_<domain_name>_<group_name>_<date>.csv`

Open the CSV file in a spreadsheet or a text editor.

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

Troubleshooting

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

Setting access rights in Kerio Connect

What levels of access rights are available

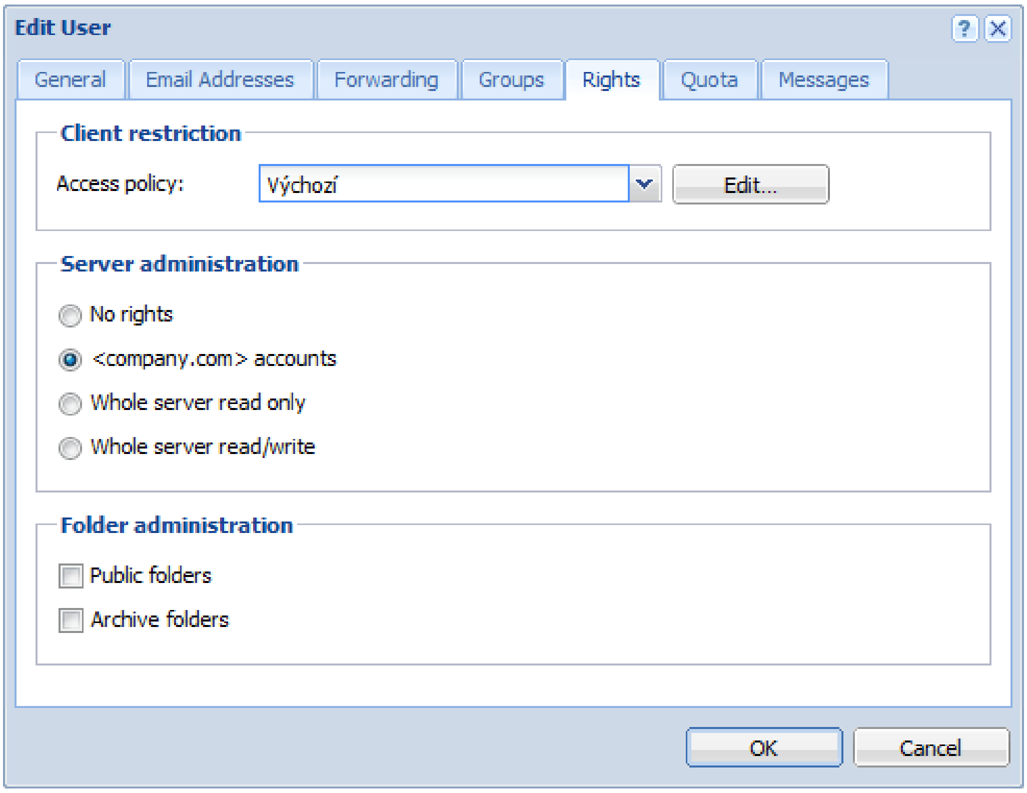
Users/groups can have assigned the following levels of access rights:

- 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.



Client restriction

Access policy: Výchozí

Server administration

○ No rights

● <company.com> accounts

○ Whole server read only

○ Whole server read/write

Folder administration

□ Public folders

□ Archive folders

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.

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:

```
psycho@yahoo.com;Peter Sycho
```

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

Where to import from

In Kerio Connect you can import users from

- CSV file
- directory service

Importing creates local user accounts..

For information on importing users to a mailing list, read articleCreating mailing lists in Kerio Connect.

Importing from a file

Creating a CSV file

You can import users from a CSV file. Headlines of individual columns in the file must correspond with Kerio Connect's items.

Individual items can be divided by:

- semicolons (;) — divide multiple items by 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
  ```

- commas (,) — put multiple items in quotation marks ("") and divide them by commas (,)

  ```
  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 for the order of the columns. Only the Name (username) is obligatory.

Importing from a CSV file

To import the file:

1. Go to section **Accounts** → **Users** and select a domain to which you wish to import users.
2. Click on **Import and Export** → **Import from a CSV File**.
3. Select the CSV file and confirm.
4. This displays a list of users from the CSV file — select those you wish to import (you can even use a template) and confirm.

Importing from a directory service

Windows NT domain

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

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

   During the import, sensitive data are transmitted (such as user passwords) — secure the communication by using an SSL encryption.

4. This displays a list of users — select those you wish to import (you can use a template) and confirm.

Microsoft Active Directory

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

3. Enter the name of the Microsoft Active Directory domain, the name of the server with Active Directory and username and password of Active Directory user (with at least read rights). Confirm.

> During the import, sensitive data are transmitted (such as user passwords) — secure the communication by using an SSL encryption.

4. This displays a list of users — select those you wish to import (you can use a template) and confirm.

Novell eDirectory

1. Go to section **Accounts** → **Users** and select a domain to which you wish to import users.

2. Click on **Import and Export** → **Import from a Directory Service**.

3. Enter the name of organization users will be imported from, the name or IP address of the server on which the service for this domain is running and username and password of a user in this domain (with at least read rights). Confirm.

> During the import, sensitive data are transmitted (such as user passwords) — secure the communication by using an SSL encryption.

4. This displays a list of users — select those you wish to import (you can use a template) and confirm.

Troubleshooting

Enable the **Directory Service Lookup** option in the Debug log before starting the import process. Logged information about the import process will help you where troubleshooting is necessary.

Exporting users in Kerio Connect

What can be exported

In Kerio Connect you 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 items in the file are separated by semicolons (;). Multiple information is separated by commas (,).

> Administrators with at least read rights can export users.

Exporting users from a domain

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

The file name is created by the following pattern: `users_<DomainName>_<date>.csv`

Exporting users from a group

1. In the administration interface, go to section **Accounts** → **Groups.**
2. Select the domain and double-click the group.
3. On the **Members** tab click **Export.**

The file name will be created by the following pattern: `users_<DomainName>_<GroupName>_<date>.csv`

Exporting users from a mailing list

1. In the administration interface, go to section **Accounts** → **Mailing Lists**.
2. Select the domain where the mailing list is created.
3. Click on **Import and Export** → **Export to a CSV file.**

The file name will be created by the following pattern: `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)

Both types of aliases can be combined:

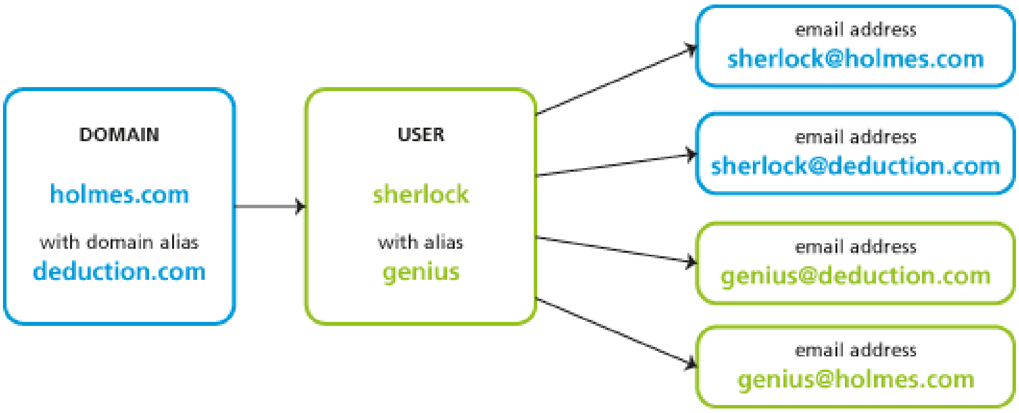


Figure 1 Map of aliases for a single user account

Domain aliases

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

Domain aliases are used 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):

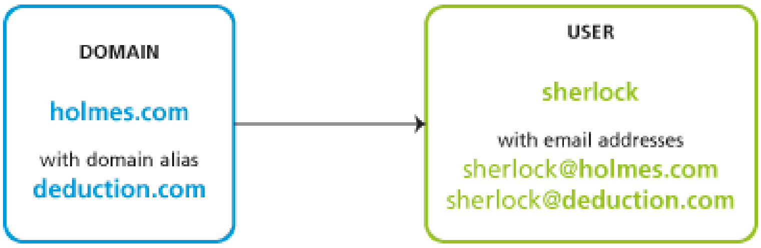


Figure 2 Domain aliases

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):

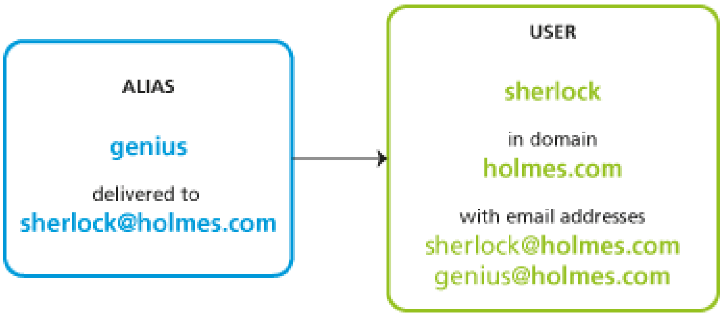


Figure 3 Domain aliases

Creating username aliases

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

1. In the administration interface, go to **Accounts** → **Aliases**.
2. Select a domain where the aliases will be created. Click **Add**.
3. Enter 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 sent to:

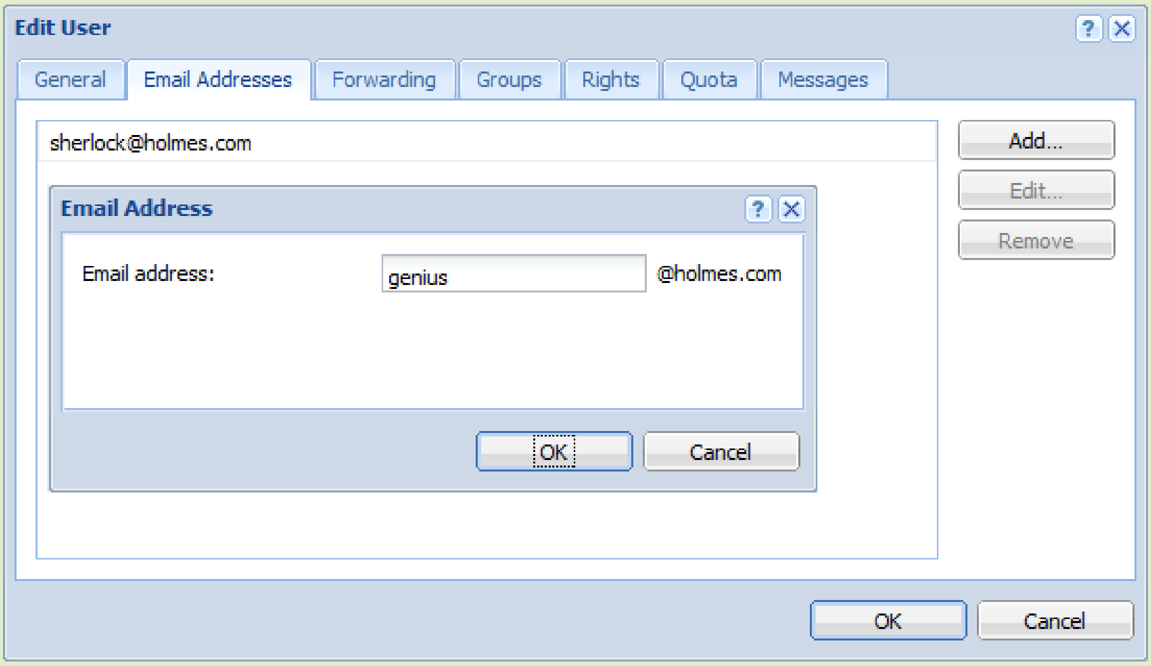
   - an email address — click **Select**
   - public folder — enter the name of the public folder in this format: `#public/folder_name`

   > This item is active only in case at least one public folder of the *Mail* type is created.

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:



Edit User

General | Email Addresses | Forwarding | Groups | Rights | Quota | Messages

sherlock@holmes.com

Email Address

Email address: genius @holmes.com

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

What are resources

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

In email clients, resources can be scheduled by creating new events in calendars.

Resources do not count into your license.

Resource administrators

Each resource has a reservation manager. Reservation managers are users who manage the resource calendar. In Kerio Connect client, they can delete any reservation for a resource.

You can set the reservation managers in the resource settings on tab **Permissions**.

Creating new resources

To create a new resource in the administration interface, follow these steps:

1. In section **Accounts** → **Resources**, select the domain to which you want to add a resourc. Click **Add**.

2. Enter a name for the resource and select the type.

3. Make sure the **Resource is available** option is checked.

   > If you wish to temporarily remove a resource (e.g. while a car is being repaired), uncheck this option.

4. By default, permissions to use resources are set to all users from the domain. You can add or remove any user/group on tab **Permissions**.

5. On tab **Permissions**, select a reservation manager.

   By default, the domain administrator is set.

6. Confirm the settings.

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:

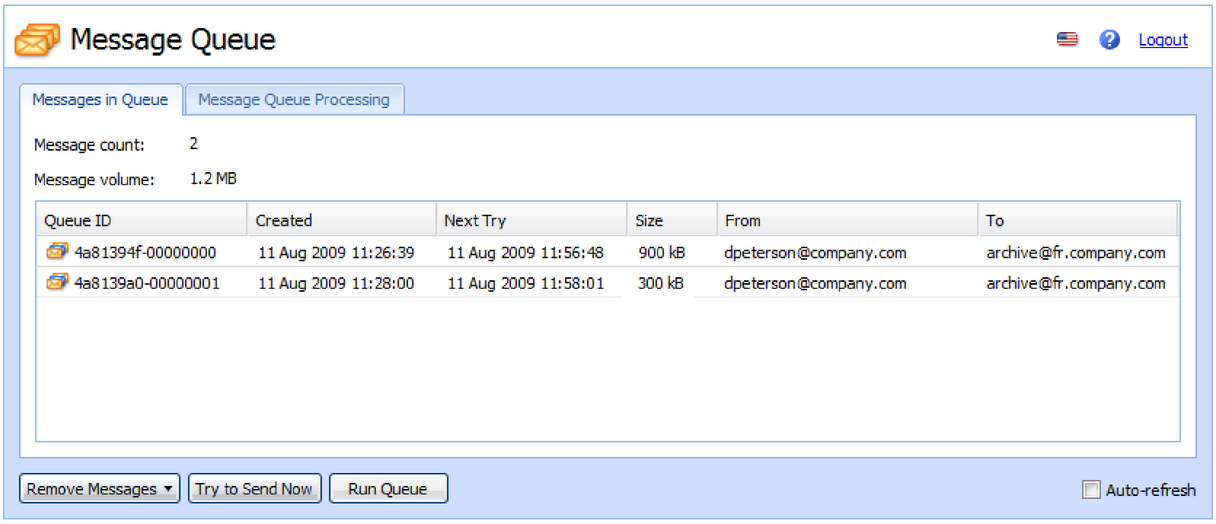
- `*.eml` — message itself
- `*.env` — SMTP envelope of the message

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`.



Message count: 2

Message volume: 1.2 MB

Queue ID	Created	Next Try	Size	From	To
4a81394f-00000000	11 Aug 2009 11:26:39	11 Aug 2009 11:56:48	900 kB	dpeterson@company.com	archive@fr.company.com
4a8139a0-00000001	11 Aug 2009 11:28:00	11 Aug 2009 11:58:01	300 kB	dpeterson@company.com	archive@fr.company.com

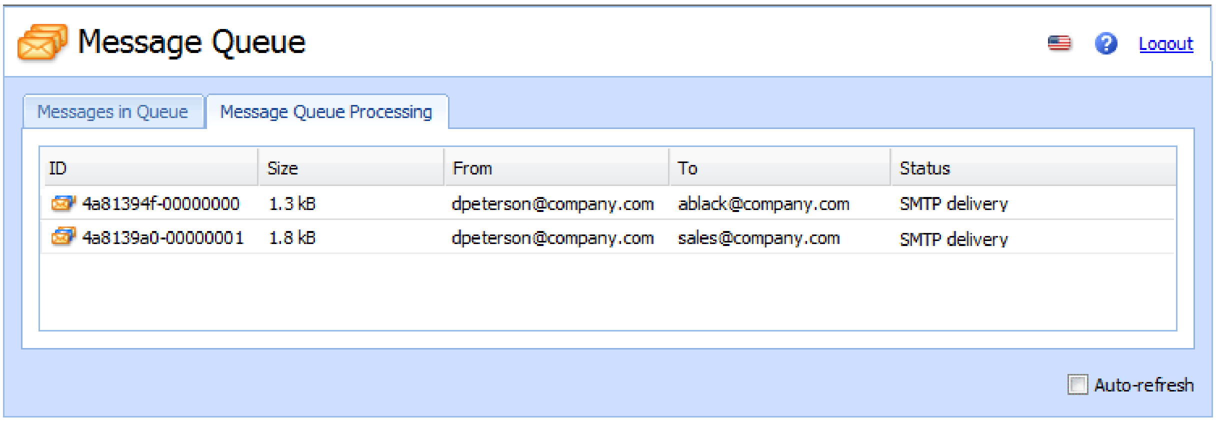
Figure 1 Viewing message queue

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.



ID	Size	From	To	Status
4a81394f-00000000	1.3 kB	dpeterson@company.com	ablack@company.com	SMTP delivery
4a8139a0-00000001	1.8 kB	dpeterson@company.com	sales@company.com	SMTP delivery

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.

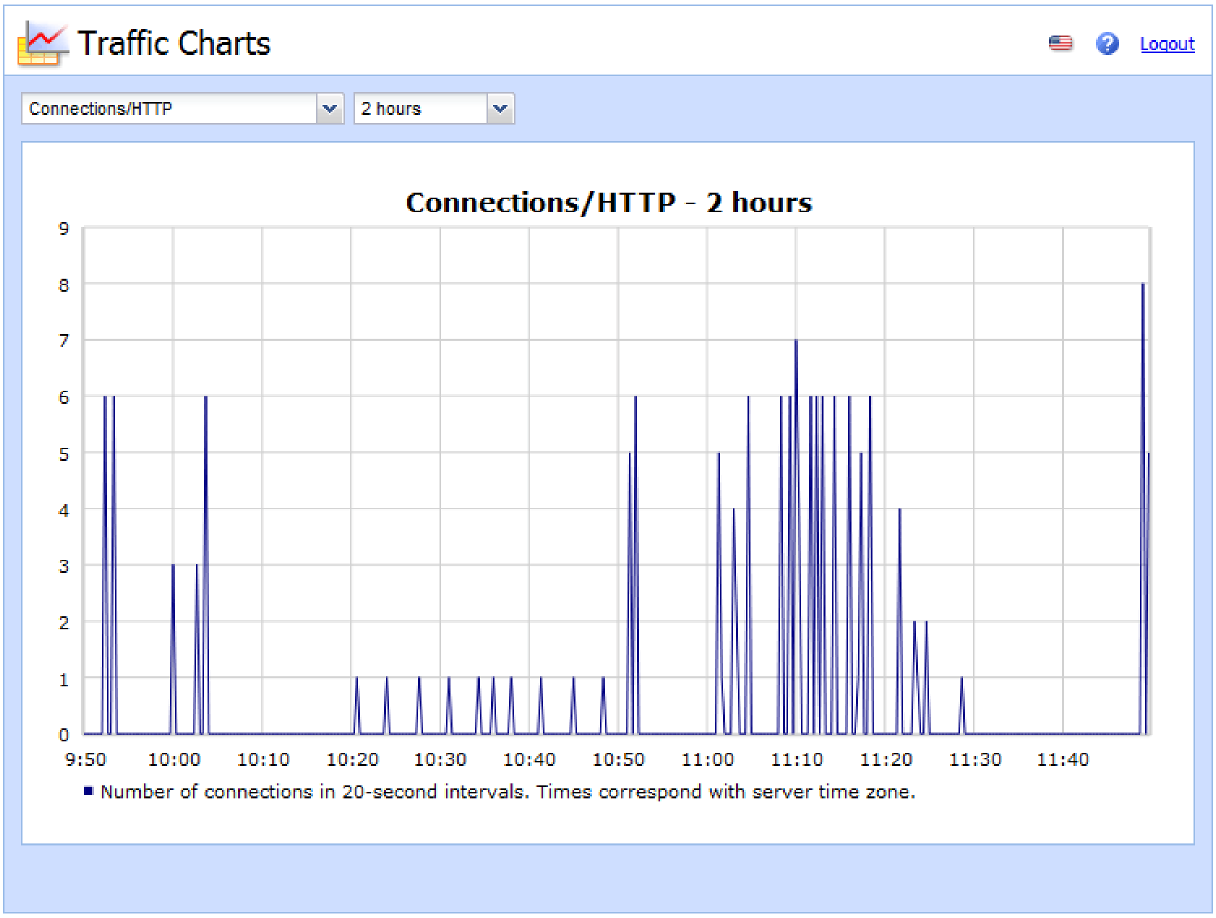
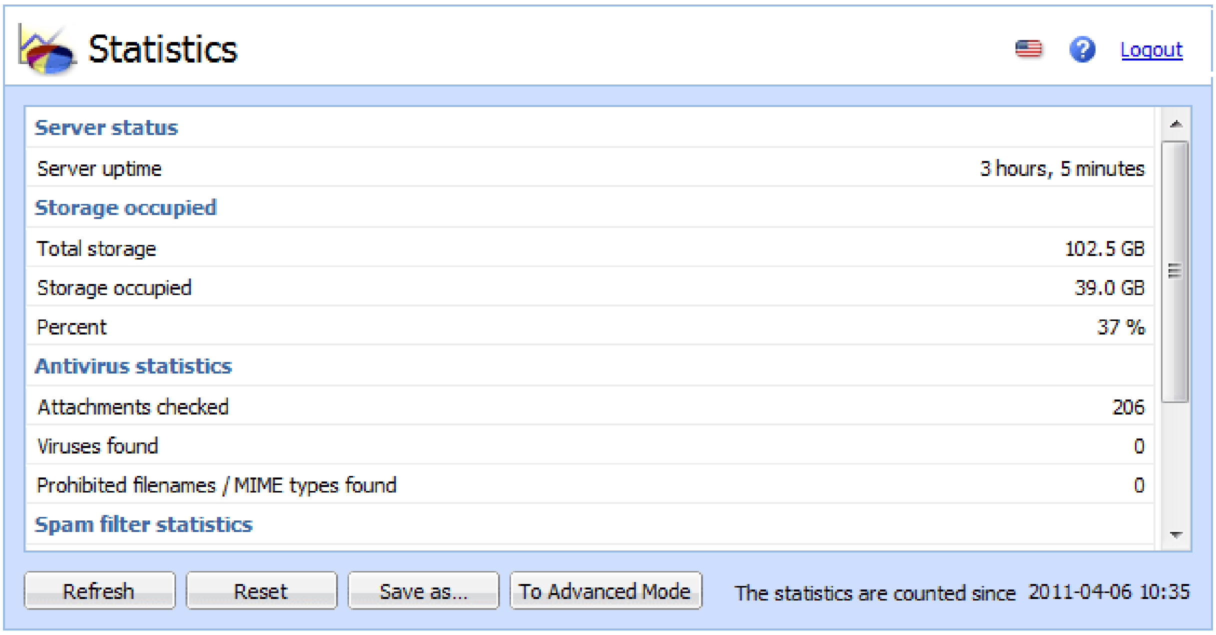

Traffic Charts
Logout
Connections/HTTP
2 hours
Connections/HTTP - 2 hours
0
1
2
3
4
5
6
7
8
9
9:50
10:00
10:10
10:20
10:30
10:40
10:50
11:00
11:10
11:20
11:30
11:40
■ Number of connections in 20-second intervals. Times correspond with server time zone.

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.



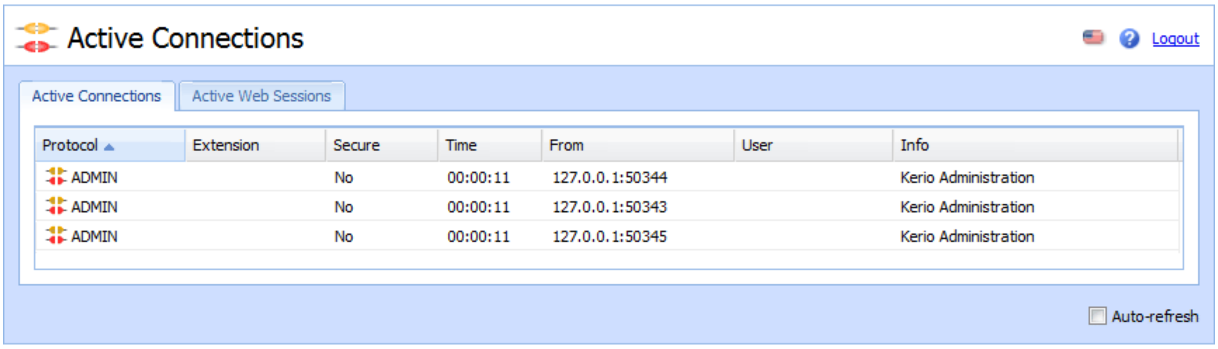
Server status	
Server uptime	3 hours, 5 minutes
Storage occupied	
Total storage	102.5 GB
Storage occupied	39.0 GB
Percent	37 %
Antivirus statistics	
Attachments checked	206
Viruses found	0
Prohibited filenames / MIME types found	0
Spam filter statistics	

The statistics are counted since 2011-04-06 10:35

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**.

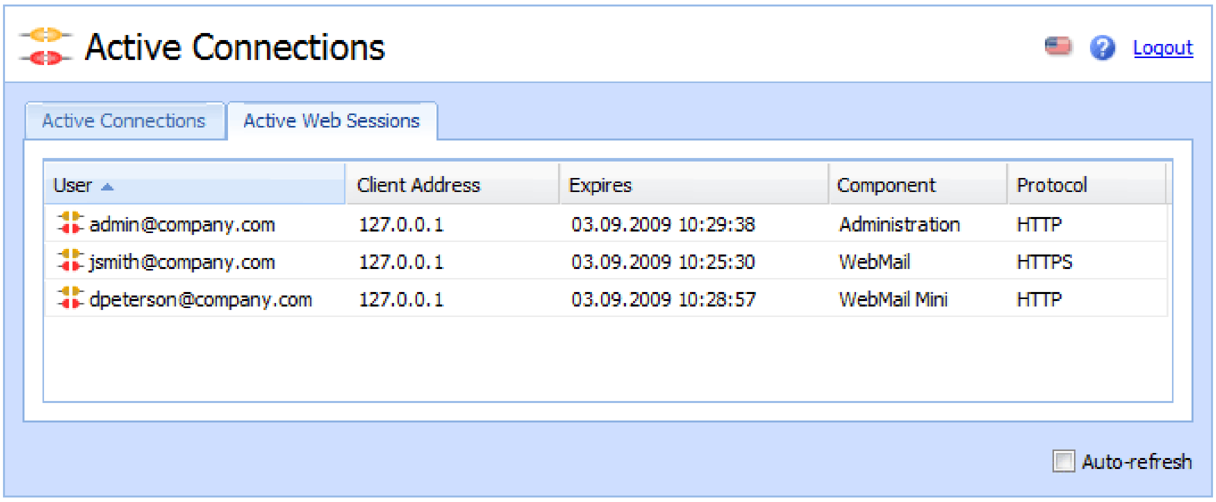


Protocol	Extension	Secure	Time	From	User	Info
ADMIN		No	00:00:11	127.0.0.1:50344		Kerio Administration
ADMIN		No	00:00:11	127.0.0.1:50343		Kerio Administration
ADMIN		No	00:00:11	127.0.0.1:50345		Kerio Administration

□ Auto-refresh

Figure 5 Active connections

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



User ▲	Client Address	Expires	Component	Protocol
admin@company.com	127.0.0.1	03.09.2009 10:29:38	Administration	HTTP
jsmith@company.com	127.0.0.1	03.09.2009 10:25:30	WebMail	HTTPS
dpeterson@company.com	127.0.0.1	03.09.2009 10:28:57	WebMail Mini	HTTP

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

New in Kerio Connect 8.2!

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

Parameters for services can be set in section **Configuration** → **Services**.

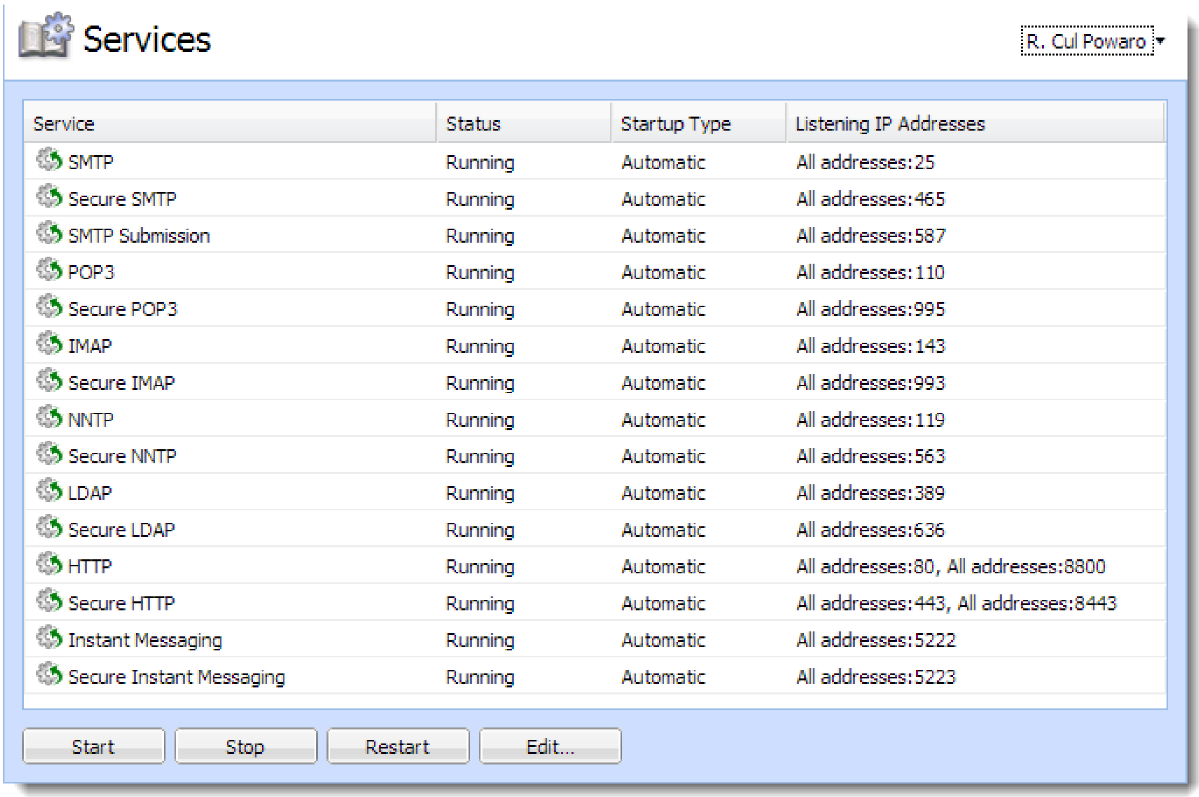
By default, all services are running on their standard ports upon the first startup of Kerio Connect.

If you know that any service will not be used, we recommend to disable them for security reasons.

For each service, you can:

- specify whether the service will be run automatically upon 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

  When you plan to limit the number of connections, consider the number of server users. For unlimited number of connections set the value to 0.



Services

Service	Status	Startup Type	Listening IP Addresses
SMTP	Running	Automatic	All addresses:25
Secure SMTP	Running	Automatic	All addresses:465
SMTP Submission	Running	Automatic	All addresses:587
POP3	Running	Automatic	All addresses:110
Secure POP3	Running	Automatic	All addresses:995
IMAP	Running	Automatic	All addresses:143
Secure IMAP	Running	Automatic	All addresses:993
NNTP	Running	Automatic	All addresses:119
Secure NNTP	Running	Automatic	All addresses:563
LDAP	Running	Automatic	All addresses:389
Secure LDAP	Running	Automatic	All addresses:636
HTTP	Running	Automatic	All addresses:80, All addresses:8800
Secure HTTP	Running	Automatic	All addresses:443, All addresses:8443
Instant Messaging	Running	Automatic	All addresses:5222
Secure Instant Messaging	Running	Automatic	All addresses:5223

Figure 1 Services in Kerio Connect

If any services available in Kerio Connect is 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)

However, assigning the IP addresses is not recommended while using 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

SMTP protocol server is used for sending outgoing email messages, for receiving incoming messages and messages creating 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 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 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
- to automatically update Kerio Outlook Connector (Offline Edition)
- to 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

New in Kerio Connect 8.1!

Instant messaging allows user 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 POP3 server arise, enabling the **POP3 Server** option might be helpful.

IMAP

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

NNTP

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

LDAP

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

HTTP

- **HTTP Server** — this option enables logging of HTTP traffic on the server's side.
- **WebDAV Server Request** — this option enables logging of queries sent from the WebDAV server. It can be used in *Microsoft Entourage* or *Apple Mail* where problems with Exchange accounts arise.
- **PHP Engine Messages** — enables log which may be helpful when solving problems with the Kerio Connect client interface.

Instant messaging

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

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

Protecting SMTP the server in Kerio Connect

Why to configure the SMTP server

When correctly configured, the SMTP will protect your Kerio Connect from misuse. It enables you to define who will be allowed to send outgoing message via this server and what actions they can perform.

Once an unprotected SMTP server is accessible from the Internet (anytime when at least one MX record is directed to it and the port 25 is available for access), anyone can connect to the server and send email messages through it (usually spam).

> Spammers may use your SMTP server to send out spam messages. Thus your company may be added to a spam blacklist.

How to configure who can connect to SMTP server

To configure SMTP settings, login to the administration interface:

1. Go to section **Configuration** → **SMTP Server** → **tab Relay Control.**
2. Select **Allow relay only for**.

   > If you enable this option, users not specified will be able to send messages only to the local domains.

3. Check **Users from IP address group** to specify a group of IP address which can send outgoing messages.

   > Usually local addresses are added. However if you wish to protect users who send messages from local addresses, check option Require authentication when accepting message with sender from a local domain.

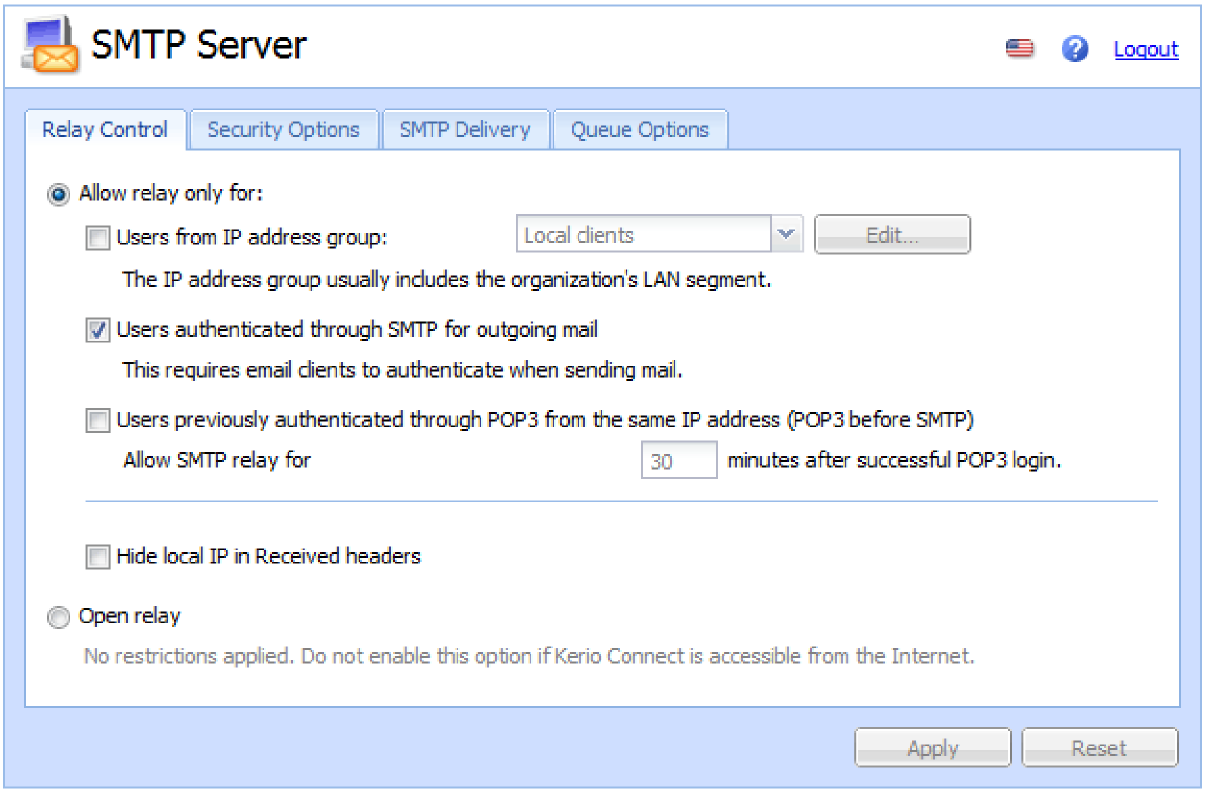
4. Check **Users authenticated through SMTP for outgoing mail** to allow all Kerio Connect users sending outgoing messages.

5. Check **Users previously authenticated through POP3 ....** to allow sending outgoing messages to all users who have previously authenticated through POP3 from the same IP address and specify the time between POP3 and SMTP authentication.

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

6. Confirm the settings.

> Messages from allowed users will not be checked by SPF, Caller ID and SpamAssassin.



SMTP Server

● Allow relay only for:

□ Users from IP address group: Local clients

The IP address group usually includes the organization's LAN segment.

☑ Users authenticated through SMTP for outgoing mail

This requires email clients to authenticate when sending mail.

□ Users previously authenticated through POP3 from the same IP address (POP3 before SMTP)

Allow SMTP relay for 30 minutes after successful POP3 login.

□ Hide local IP in Received headers

○ Open relay

No restrictions applied. Do not enable this option if Kerio Connect is accessible from the Internet.

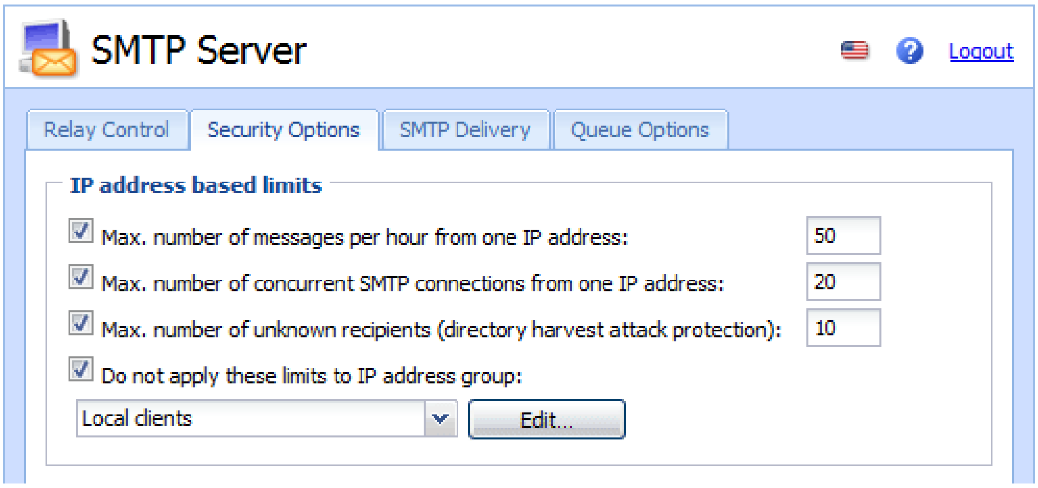
Figure 1 SMTP server

How to configure security options of the SMTP server

In Kerio Connect, you can configure several limits for IP addresses. This can be done in the administration interface in section **Configuration → SMTP Server → tab Security Options**

For a single IP address, you can set:

- Maximum number of messages sent in one hour — any new message sent from the IP address where the limit was exceeded in the recent our is discarded
- Max. number of concurrent connections — protection from so-called DoS attacks which overloads the server
- Maximum number of unknown recipients — protection from so-called directory harvest attacks when an application connects to your server and uses dictionary to generate possible usernames



IP address based limits

☑ Max. number of messages per hour from one IP address: 50

☑ Max. number of concurrent SMTP connections from one IP address: 20

☑ Max. number of unknown recipients (directory harvest attack protection): 10

☑ Do not apply these limits to IP address group:

Local clients

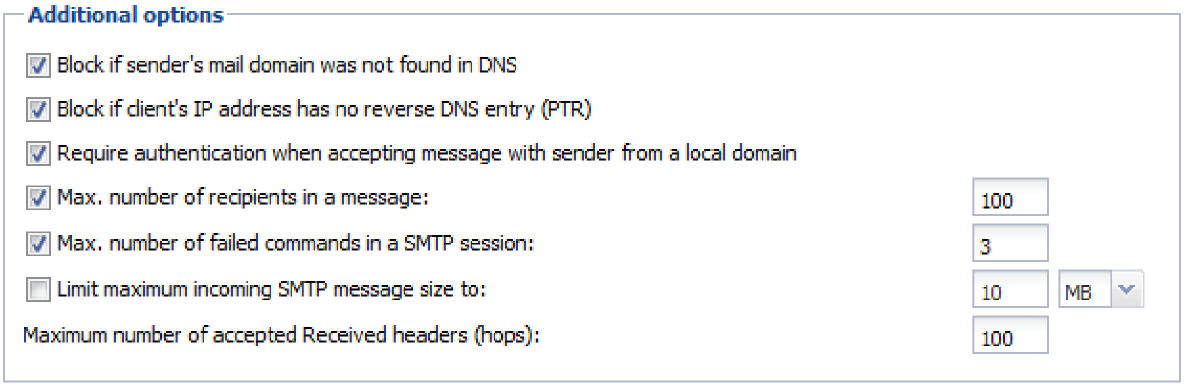
Figure 2 SMTP server

Select a group of trusted IP addresses which will not be affected by these settings.

With the following additional options you can:

- Block messages if the sender's domain does not have a DNS record (or revers DNS entry) — protection from senders with fictional email addresses
- Require authentication even when sender is from a local domain — ensures the authenticity of anyone sending from a local domain
- Set maximum number of recipients per message — protects from spam messages set to a large number of recipients
- Maximum number of failed commands in SMTP session — spam is often sent by special applications that connect to SMTP servers and ignore its error reports. Kerio

Connect will close the SMTP connection automatically after the defined number of failed commands is reached.



Additional options

☑ Block if sender's mail domain was not found in DNS

☑ Block if client's IP address has no reverse DNS entry (PTR)

☑ Require authentication when accepting message with sender from a local domain

☑ Max. number of recipients in a message: 100

☑ Max. number of failed commands in a SMTP session: 3

□ Limit maximum incoming SMTP message size to: 10 MB

Maximum number of accepted Received headers (hops): 100

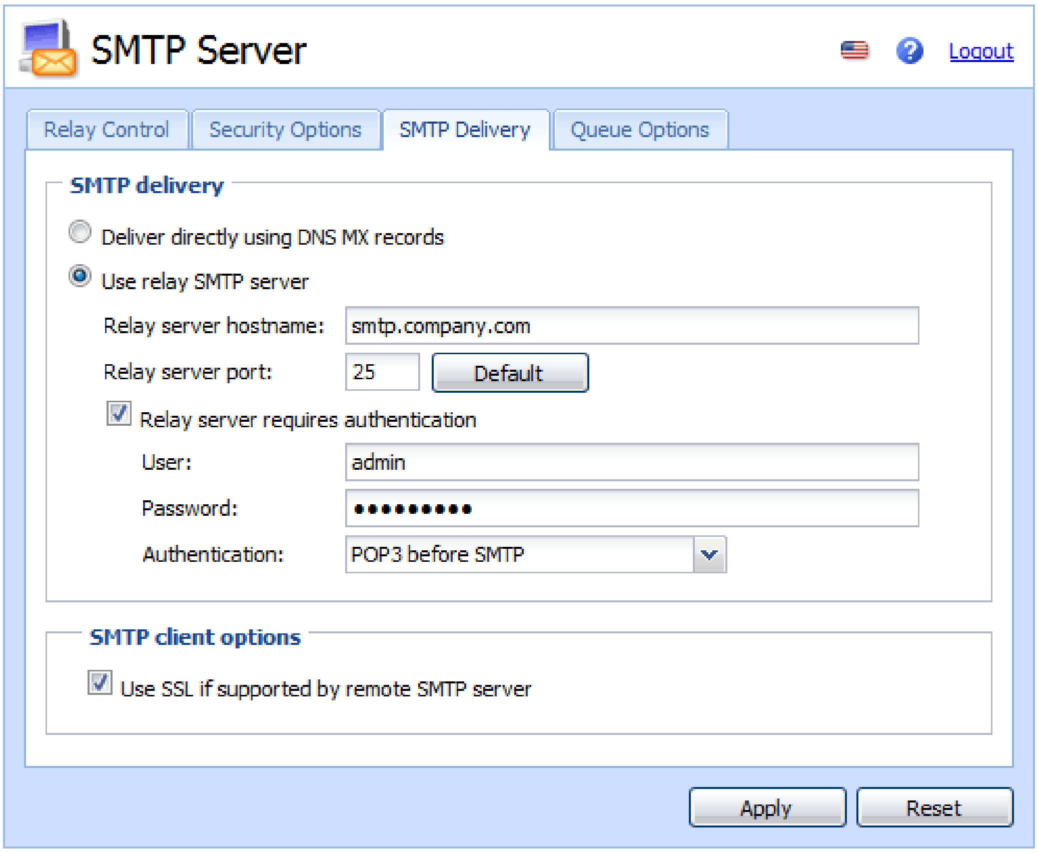
Figure 3 SMTP server

How to send outgoing messages through another server

In Kerio Connect, messages can be delivered

- directly to destination domains using MX records or
- through another SMTP server, so called relay SMTP server

This can be configured in the administration interface in section **Configuration** → **SMTP Server** → **tab SMTP Delivery**.



SMTP Server

SMTP delivery

○ Deliver directly using DNS MX records

● Use relay SMTP server

Relay server hostname: smtp.company.com

Relay server port: 25 Default

☑ Relay server requires authentication

User: admin

Password: ●●●●●●●●●

Authentication: POP3 before SMTP

SMTP client options

☑ Use SSL if supported by remote SMTP server

Figure 4 SMTP server

Troubleshooting

We strongly recommend to use these settings to protect your SMTP server. However, sometimes even a correct message can be rejected, e.g. when a sales person sends multiple messages to customers, they may exceed the limits set. Thus whenever a problem with delivering messages occurs, ask the users and check the SMTP server settings.

Securing Kerio Connect

Issues to address

- Restrict communication on firewall to necessary IP addresses and ports
- Create strong passwords policy
- Configure security policy
- Configure SMTP server
- Use antispam and antivirus
- Enable DKIM signature
- Enable the sender anti-spoofing protection

Configuring your firewall

If you install Kerio Connect in the local network behind a firewall, map the following ports:

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

For information on passwords, read article Password policy in Kerio Connect.

Configuring secure connection to Kerio Connect

Kerio Connect can secure:

- user authentication
- whole communication

For settings, go to section **Configuration** → **Security** → **tab Security Policy** (**Configuration** → **Advanced Options** → **tab Security Policy** for Kerio Connect 8.1 and older).

You can define a group of IP addresses which will be allowed to authenticate insecurely (e.g. from local networks).

Securing user authentication

Kerio Connect will always require secure user authentication:

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

⚠ If users' passwords are saved in the SHA format:

- do not apply CRAM-MD5, DIGEST-MD5, NTLM
- do not map users from a directory service

Encrypting user communication

Client applications will connect to any service using encrypted connection (the communication cannot be tapped).

⚠ SSL must be allowed to all protocols on all client stations.
Many SMTP servers do not support SMTPS and STARTTLS. To provide sufficient security, the SMTP server requires secure user authentication.

Setting secure connection

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

2. Select a security policy.

3. Select group of trustworthy IP addresses.

4. Select authentication methods.

   If more methods are selected, they will be performed in order of appearance and availability.

   If user passwords are saved in the SHA format, select either **PLAIN** and/or **LOGIN**. Otherwise, users will not be able to login to Kerio Connect client.

5. Save the settings.

Configuring anti-spoofing in Kerio Connect

About anti-spoofing

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

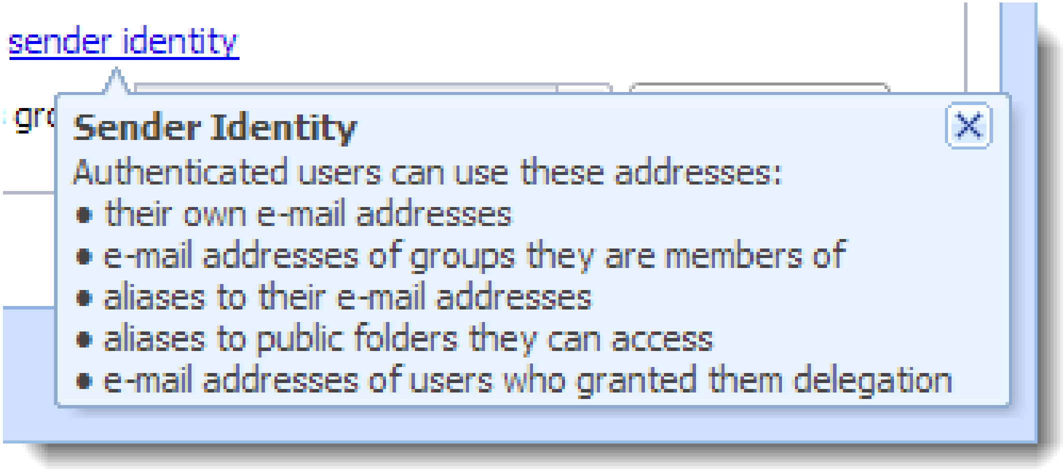
To avoid such possibility, enable anti-spoofing in Kerio Connect.

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.

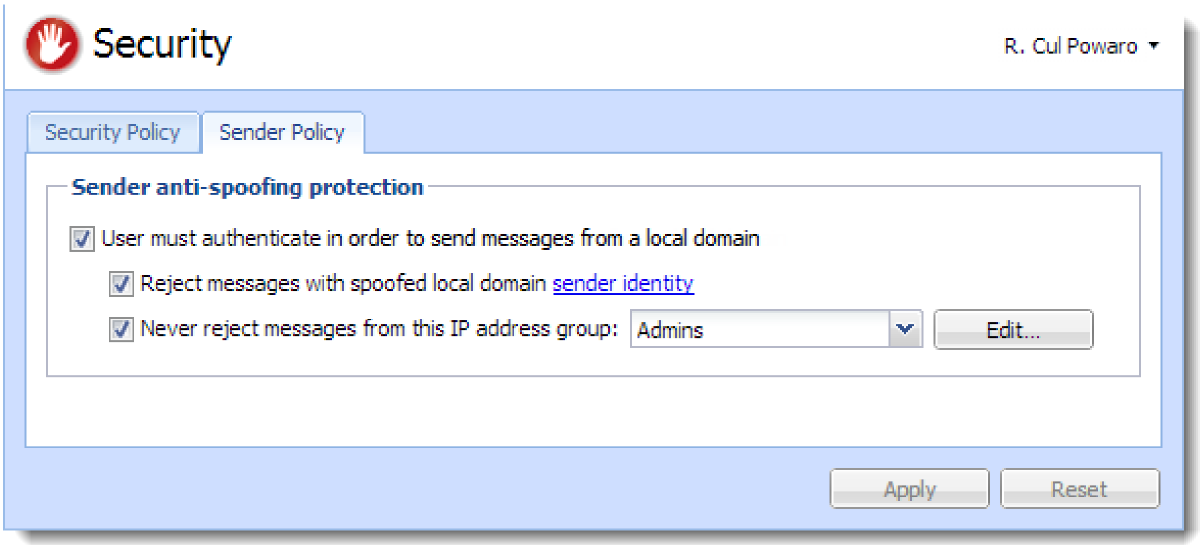


Sender Identity

Authenticated users can use these addresses:

- their own e-mail addresses
- e-mail addresses of groups they are members of
- aliases to their e-mail addresses
- aliases to public folders they can access
- e-mail addresses of users who granted them delegation

   You can define a group of trusted IP addresses.



Sender anti-spoofing protection

☑ User must authenticate in order to send messages from a local domain

☑ Reject messages with spoofed local domain sender identity

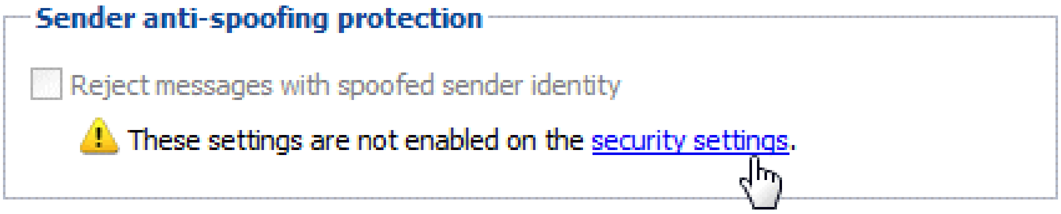
☑ Never reject messages from this IP address group: Admins

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.

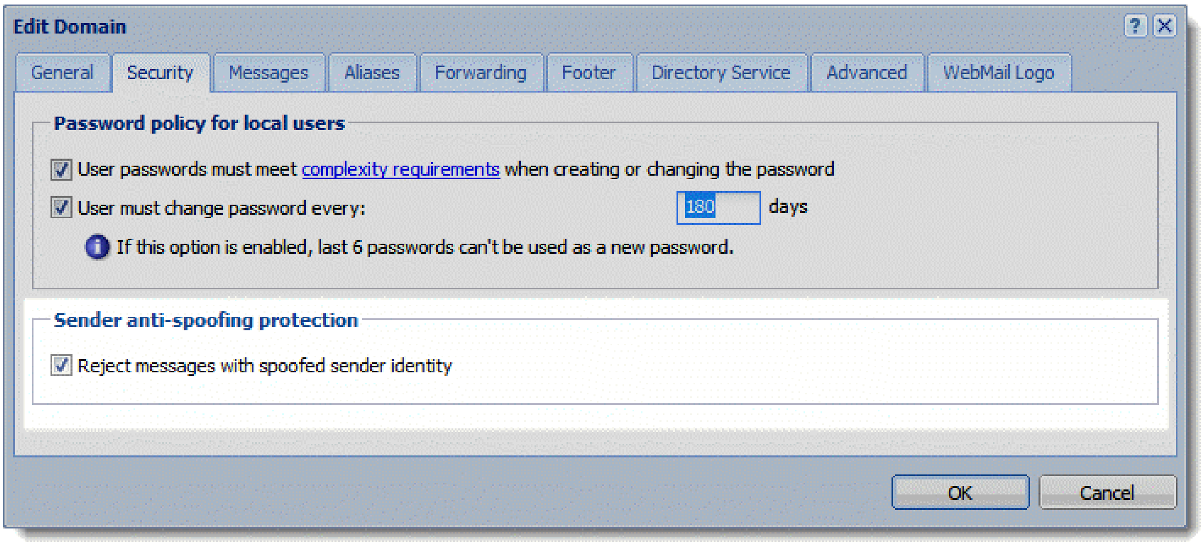


Sender anti-spoofing protection

□ Reject messages with spoofed sender identity

These settings are not enabled on the security settings.

4. Save the domain settings.



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

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.

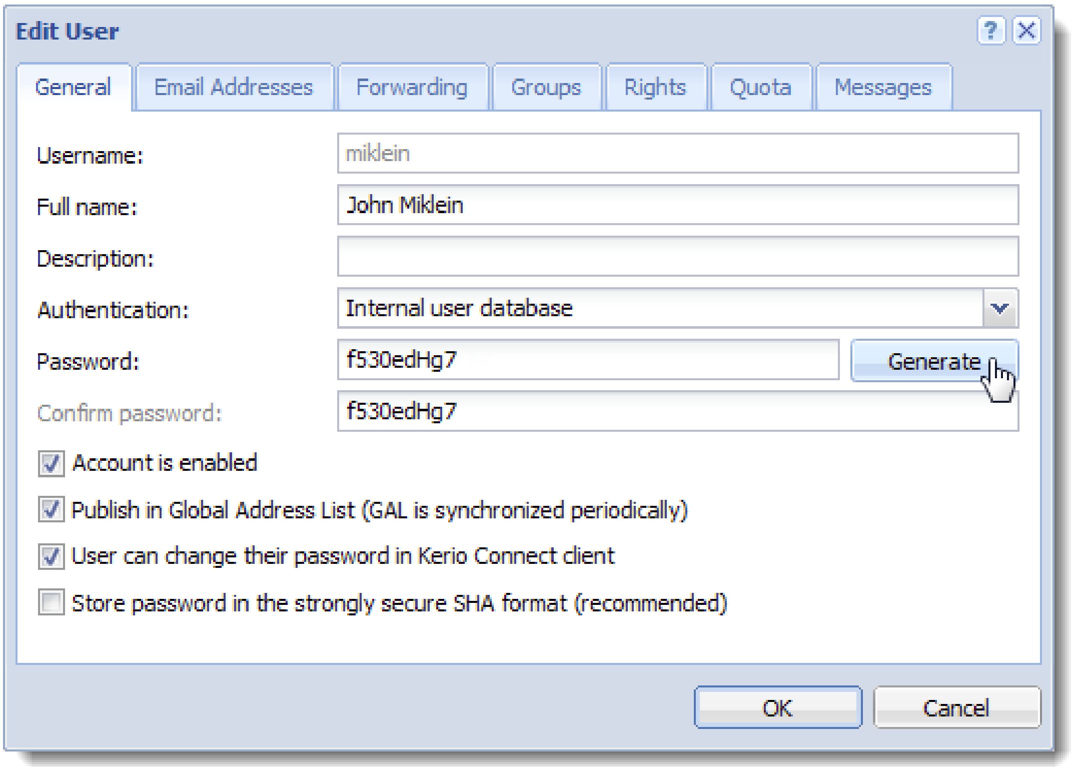
You can also read this Wikipedia article for more information.

Generating strong passwords

New in Kerio Connect 8.2!

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.



Username: miklein

Full name: John Miklein

Description:

Authentication: Internal user database

Password: f530edHg7

Confirm password: f530edHg7

☑ Account is enabled

☑ Publish in Global Address List (GAL is synchronized periodically)

☑ User can change their password in Kerio Connect client

□ Store password in the strongly secure SHA format (recommended)

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

Requiring complex passwords (for local users)

New in Kerio Connect 8.2!

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

Complex password:

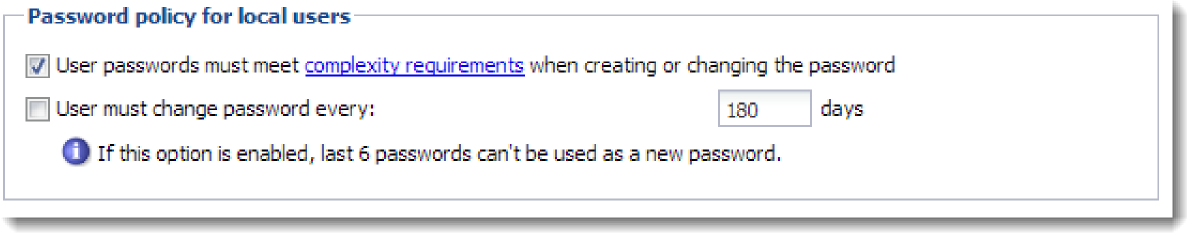
- must be at least 8 characters long,
- must include at least 3 types of characters (lowercase, uppercase, numbers, symbols),
- cannot include user’s domain and username, and any part of user’s fullname (longer than 2 characters).

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.



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.

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)

New in Kerio Connect 8.2!

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

New in Kerio Connect 8.2!

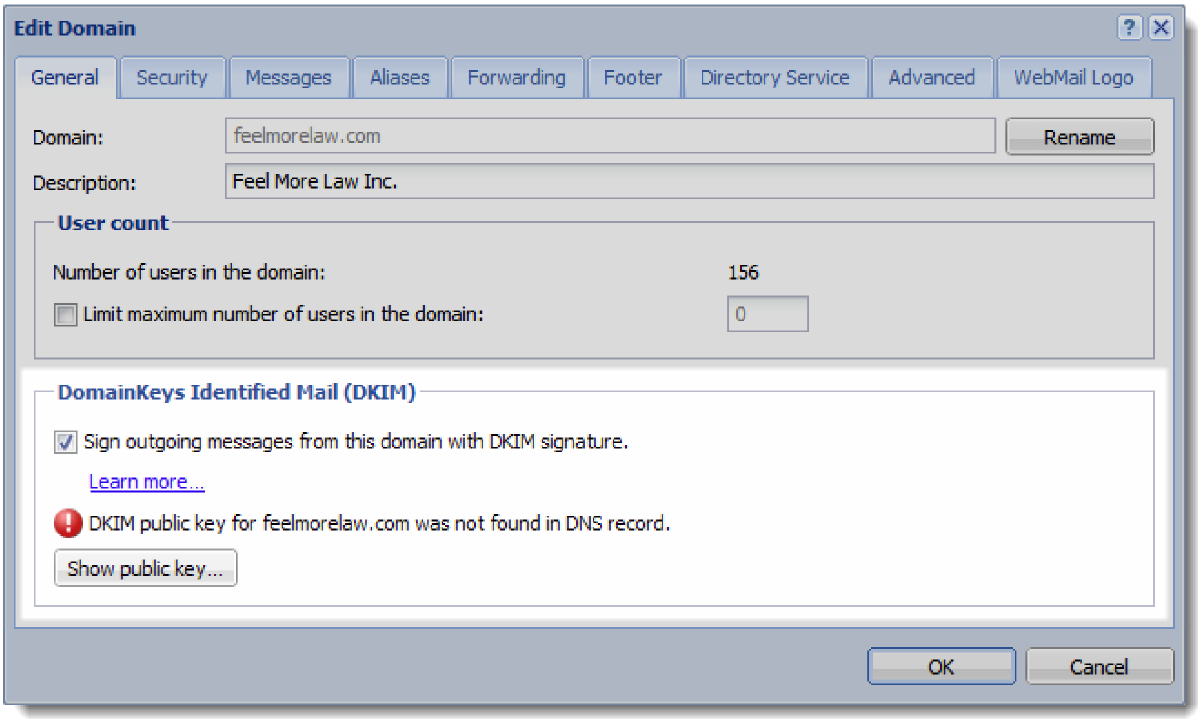
DomainKeys Identified Mail (DKIM) signs outgoing messages from Kerio Connect with a special signature to identify the sender. Your users thus take responsibility for the messages they send and the recipients are sure the messages came from a verified user (by retrieving your public key).

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.



Domain: feelmorelaw.com

Description: Feel More Law Inc.

User count

Number of users in the domain: 156

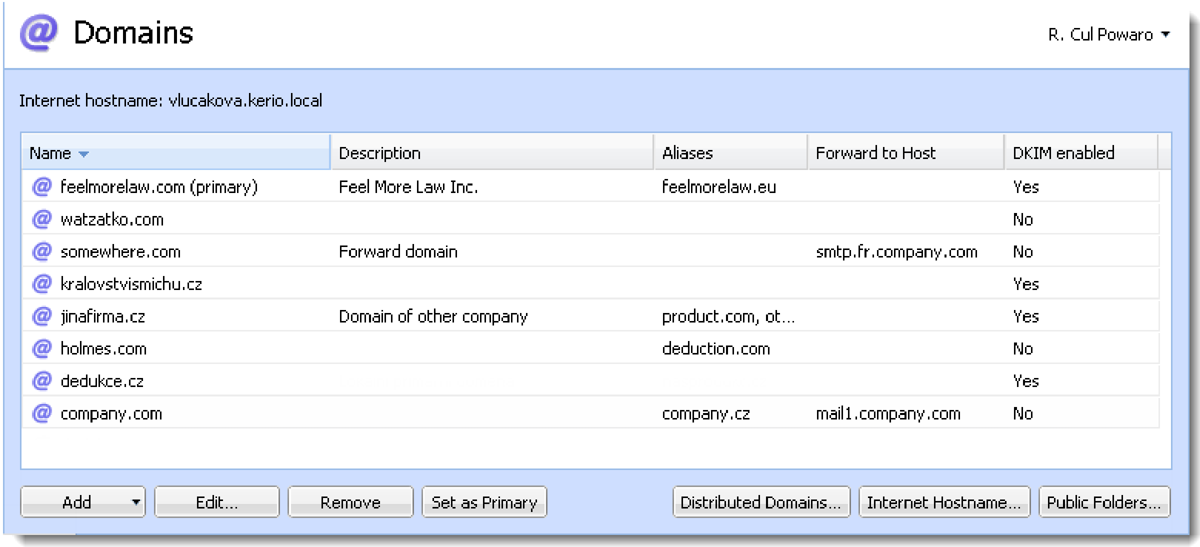
☐ Limit maximum number of users in the domain: 0

DomainKeys Identified Mail (DKIM)

☑ Sign outgoing messages from this domain with DKIM signature.

DKIM public key for feelmorelaw.com was not found in DNS record.

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



Internet hostname: vlucakova.kerio.local

Name	Description	Aliases	Forward to Host	DKIM enabled
feelmorelaw.com (primary)	Feel More Law Inc.	feelmorelaw.eu		Yes
watzatko.com				No
somewhere.com	Forward domain		smtp.fr.company.com	No
kralovstvismichu.cz				Yes
jinafirma.cz	Domain of other company	product.com, ot...		Yes
holmes.com		deduction.com		No
dedukce.cz				Yes
company.com		company.cz	mail1.company.com	No

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

New in Kerio Connect 8.2!

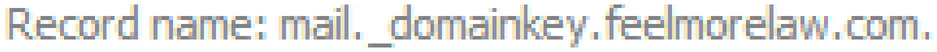
The process of adding a DKIM record to your DNS may vary according to your provider.

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

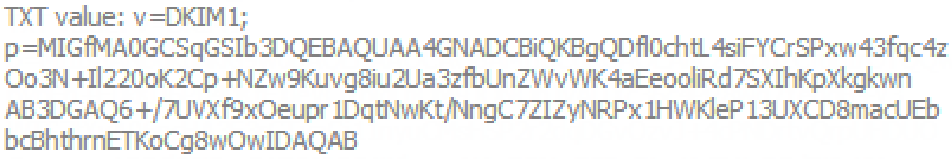
You can find the public key in Kerio Connect. The key includes two parts:

- **Record name** (or selector)



```
Record name: mail._domainkey.feelmorelaw.com.
```

- **TXT value**



```
TXT value: v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z
Oo3N+Il220oK2Cp+NZw9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn
AB3DGAQ6+/7UVXf9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb
bcBhthrnETKoCg8wOwIDAQAB
```

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.

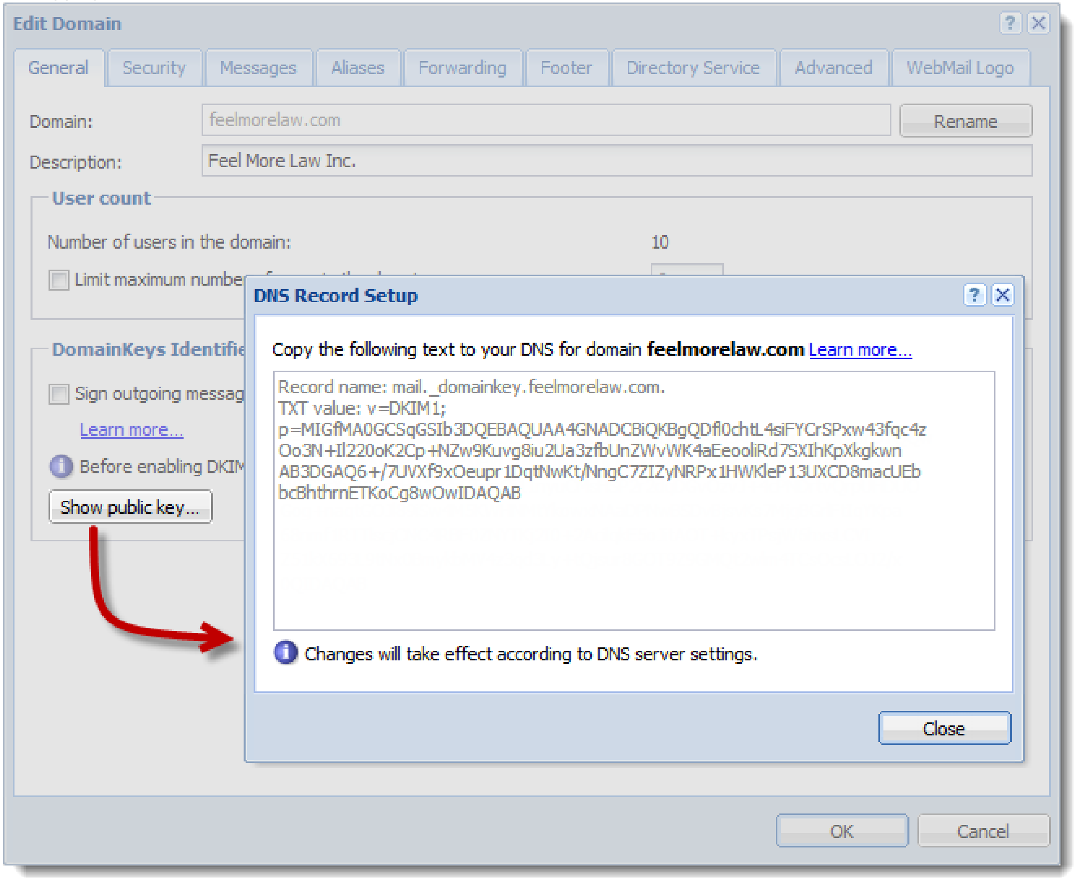
If a domain includes aliases, add DNS record for DKIM also to all aliases.

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.



Domain: feelmorelaw.com

Description: Feel More Law Inc.

Number of users in the domain: 10

□ Limit maximum numbe

□ Sign outgoing messag

Before enabling DKIM

Copy the following text to your DNS for domain **feelmorelaw.com** Learn more...

```
Record name: mail._domainkey.feelmorelaw.com.
TXT value: v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z
Oo3N+Il220oK2Cp+NZw9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn
AB3DGAQ6+/7UVXf9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb
bcBhthrnETKoCg8wOwIDAQAB
```

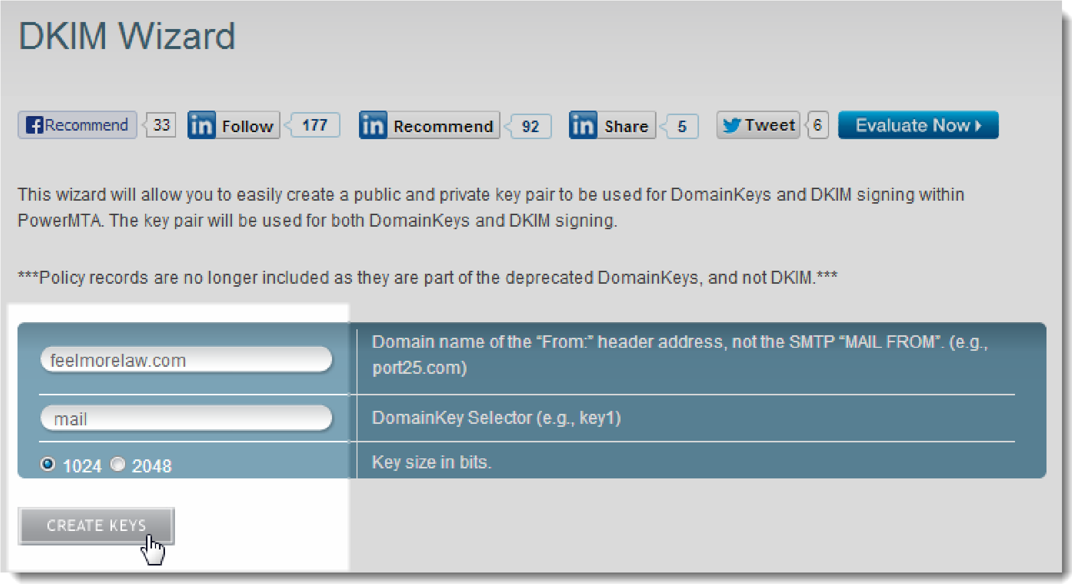
Changes will take effect according to DNS server settings.

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. 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**.



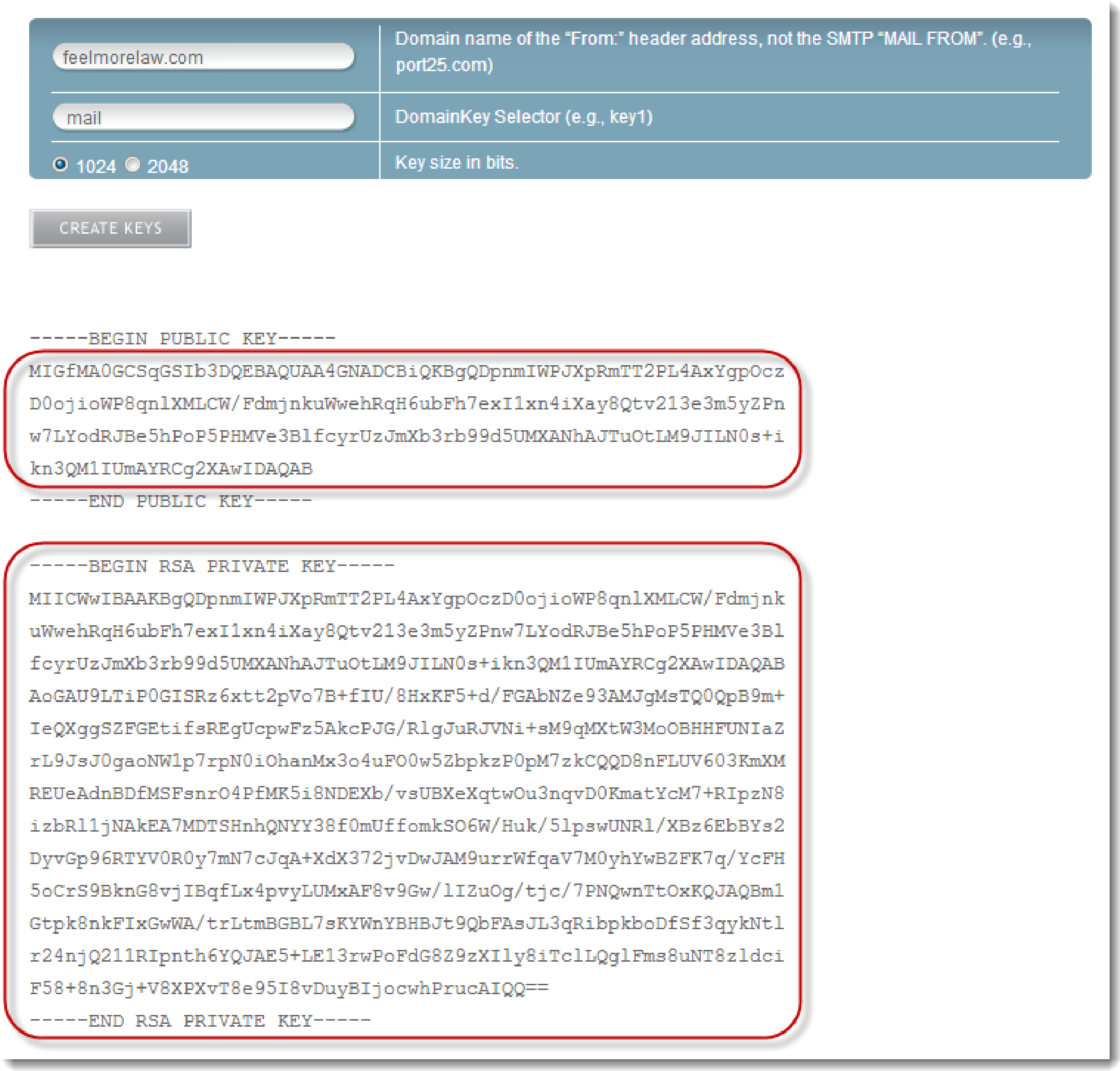
DKIM Wizard

This wizard will allow you to easily create a public and private key pair to be used for DomainKeys and DKIM signing within PowerMTA. The key pair will be used for both DomainKeys and DKIM signing.

Policy records are no longer included as they are part of the deprecated DomainKeys, and not DKIM.

feelmorelaw.com	Domain name of the "From:" header address, not the SMTP "MAIL FROM". (e.g., port25.com)
mail	DomainKey Selector (e.g., key1)
● 1024 ○ 2048	Key size in bits.

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



feelmorelaw.com	Domain name of the "From:" header address, not the SMTP "MAIL FROM". (e.g., port25.com)
mail	DomainKey Selector (e.g., key1)
● 1024 ○ 2048	Key size in bits.

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDpnmIWPJXpRmTT2PL4AxYgpOcz
D0ojioWP8qnlXMLCW/FdmjnkuWwehRqH6ubFh7exI1xn4iXay8Qtv213e3m5yZPn
w7LYodRJBe5hPoP5PHMVe3BlfcyrUzJmXb3rb99d5UMXANhAJTuOtLM9JILN0s+i
kn3QM1IUmAYRCg2XAwIDAQAB
-----END PUBLIC KEY-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDpnmIWPJXpRmTT2PL4AxYgpOczD0ojioWP8qnlXMLCW/Fdmjnk
uWwehRqH6ubFh7exI1xn4iXay8Qtv213e3m5yZPnw7LYodRJBe5hPoP5PHMVe3Bl
fcyrUzJmXb3rb99d5UMXANhAJTuOtLM9JILN0s+ikn3QM1IUmAYRCg2XAwIDAQAB
AoGAU9LTiP0GISRz6xtt2pVo7B+fIU/8HxKF5+d/FGAbNZe93AMJgMsTQ0QpB9m+
IeQXggSZFGEtifsREgUcpwFz5AkcPJG/RlgJuRJVNi+sM9qMXtW3MoOBHHFUNIaZ
rL9JsJ0gaoNW1p7rpN0iOhanMx3o4uFO0w5ZbpkzP0pM7zkCQQD8nFLUV603KmXM
REUeAdnBDfMSFsnrO4PfMK5i8NDEXb/vsUBXeXqtwOu3nqvD0KmatYcM7+RIpzN8
izbRl1jNAkEA7MDTSHnhQNYY38f0mUffomkSO6W/Huk/5lpswUNRl/XBz6EbBYs2
DyvGp96RTYV0R0y7mN7cJqA+XdX372jvDwJAM9urrWfqaV7M0yhYwBZFK7q/YcFH
5oCrS9BknG8vjIBqfLx4pvyLUMxAF8v9Gw/lIZuOg/tjc/7PNQwnTtOxKQJAQBml
Gtpk8nkFIxGwWA/trLtmBGBL7sKYWnYBHBJt9QbFAsJL3qRibpkboDfSf3qykNtl
r24njQ211RIpnth6YQJAE5+LE13rwPoFdG8Z9zXIly8iTclLQglFms8uNT8zldci
F58+8n3Gj+V8XPXvT8e95I8vDuyBIjocwhPrucAIQQ==
-----END RSA PRIVATE KEY-----
```

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 to backup 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:

```
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z"
"Oo3N+Il22OoK2Cp+NZw9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn"
"AB3DGAQ6+/7UVXf9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb"
"bcBhthrnETKoCg8wOwIDAQAB")
```

Configuring spam control in Kerio Connect

Antispam methods and tests in Kerio Connect

Spam is an unwanted, usually advertisement email. 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.

  Detailed information in this article.

- **SpamAssassin** — SpamAssassin is a famous antispam filter which uses several testing methods.

- **Caller ID** and **SPF** — they allow to filter out messages with fake sender addresses.

  Detailed information in this article.

- **Greylisting** — The greylisting method uses a special server which stores information about messages and delivers only messages from the known senders.

  Detailed information in article Configuring greylisting.

- **Delayed response to SMTP greeting (Spam Repellent)** — Set a delayed SMTP greeting which will prevent delivery of messages sent from spam servers.

  > Messages rejected Spam Repellent are not processed by other antispam and antivirus tests. This decreases the load on your server.

- **Custom rules** — You can create your own rules which will satisfy your needs.

  Detailed information in this article.

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

Each testing type uses specific methods to detect spam. There is, however, a feature most of the tests have in common. For all methods except the delayed response to SMTP greeting, two actions can be set to specify how spam messages would be handled:

- Messages will be denied — it helps reducing load on the server
- So called message spam score will be raised — it helps eliminating possible "false positives"

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

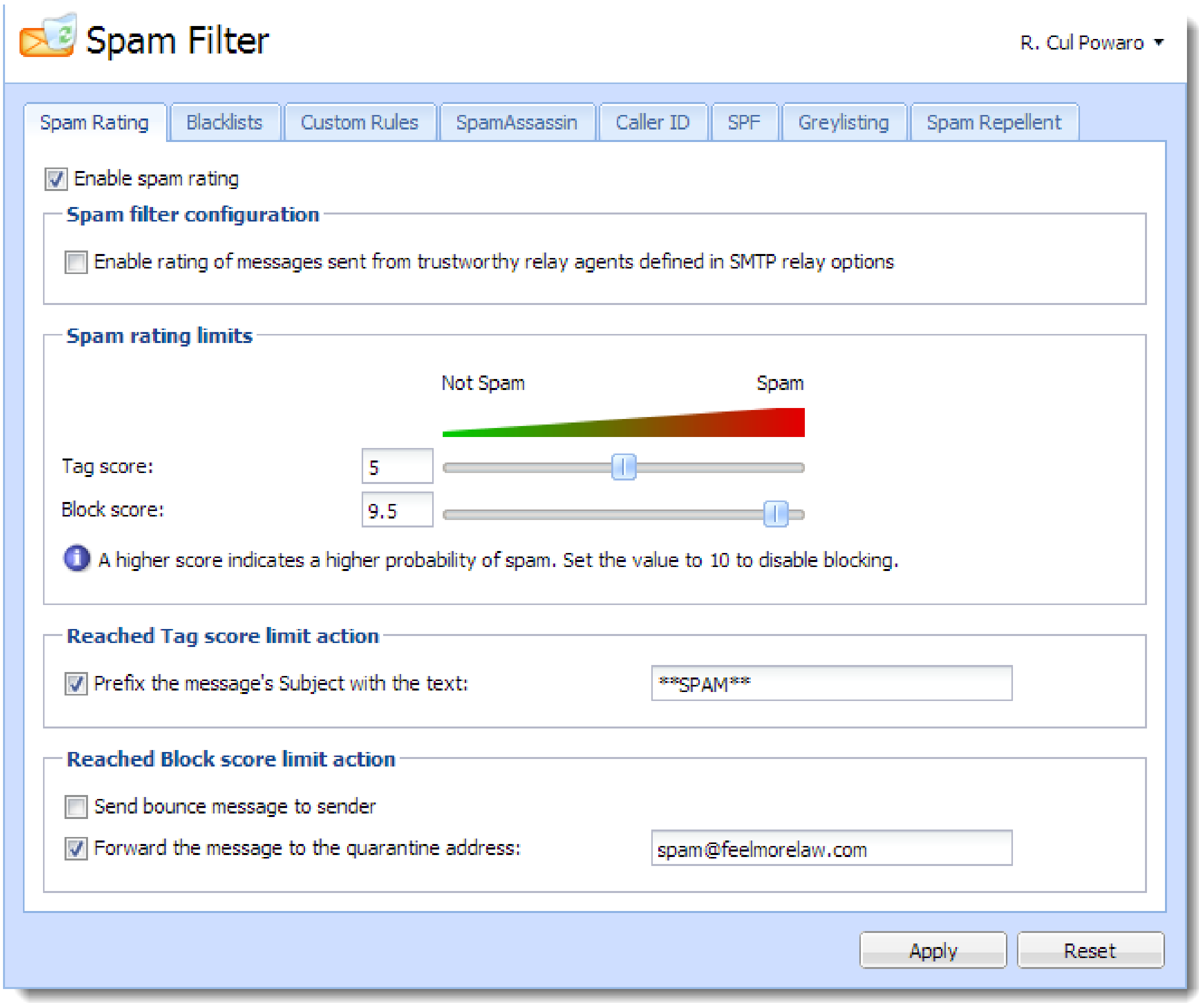
Spam score

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

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

- **Tag core** — 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 the value is too low, legitimate messages might be discarded along with spam. Therefore, it is recommended to use the Forward the message to quarantine address option when testing and optimizing the spam filter and specify an account where copies of all blocked messages will be delivered and stored.



☑ Enable spam rating

Spam filter configuration

□ Enable rating of messages sent from trustworthy relay agents defined in SMTP relay options

Spam rating limits

Tag score: 5

Block score: 9.5

A higher score indicates a higher probability of spam. Set the value to 10 to disable blocking.

Reached Tag score limit action

☑ Prefix the message's Subject with the text: **SPAM**

Reached Block score limit action

□ Send bounce message to sender

☑ Forward the message to the quarantine address: spam@feelmorelaw.com

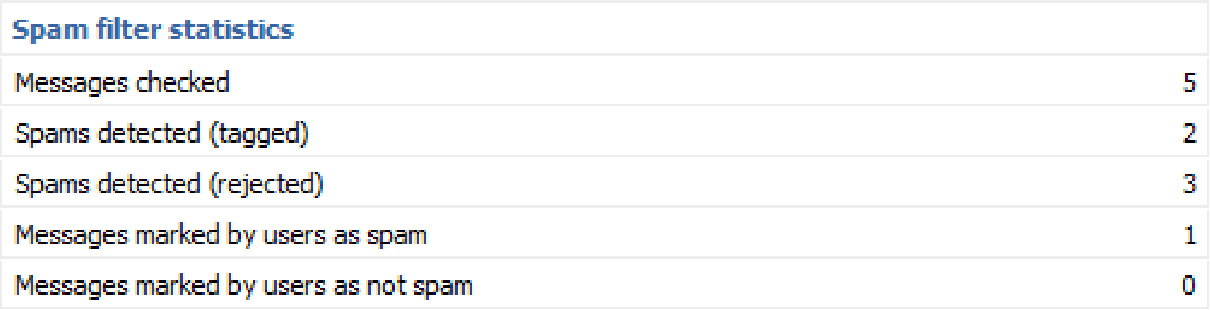
Figure 1 Spam rating

Monitoring spam filter's functionality and efficiency

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

Spam filter statistics

Kerio Connect generates statistics of its spam filter. The statistics can be found in section **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 2 Spam Filter statistics

Graphical overviews

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

The following graphs focus on spam:

Connections/Rejected SMTP

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

Messages/Spam

With time dependence, the chart displays how large amount of spam is delivered to Kerio Connect and when.

Logs

Problems that occur regarding the antispam filter might be solved with help of Kerio Connect's logs.

The following logs might be helpful:

Spam

All messages marked as spam are recorded in this log.

Debug log

Logging of particular information can be performed by this special log. Spam issues may be worked out by using of the following information (right-click the Debug log area and click on **Messages**):

- **Spam Filter** — the option logs spam rating of each message which passed through the Kerio Connect's antispam filter.
- **SPF Record Lookup** — the option gathers information of SPF queries sent to SMTP servers.
- **SpamAssassin Processing** — the option enables tracing of processes occurred during SpamAssassin antispam tests.

Configuring greylisting

What is greylisting

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

Greylisting is an effective antispam method which complements other antispam methods and mechanisms.

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, follow these instructions:

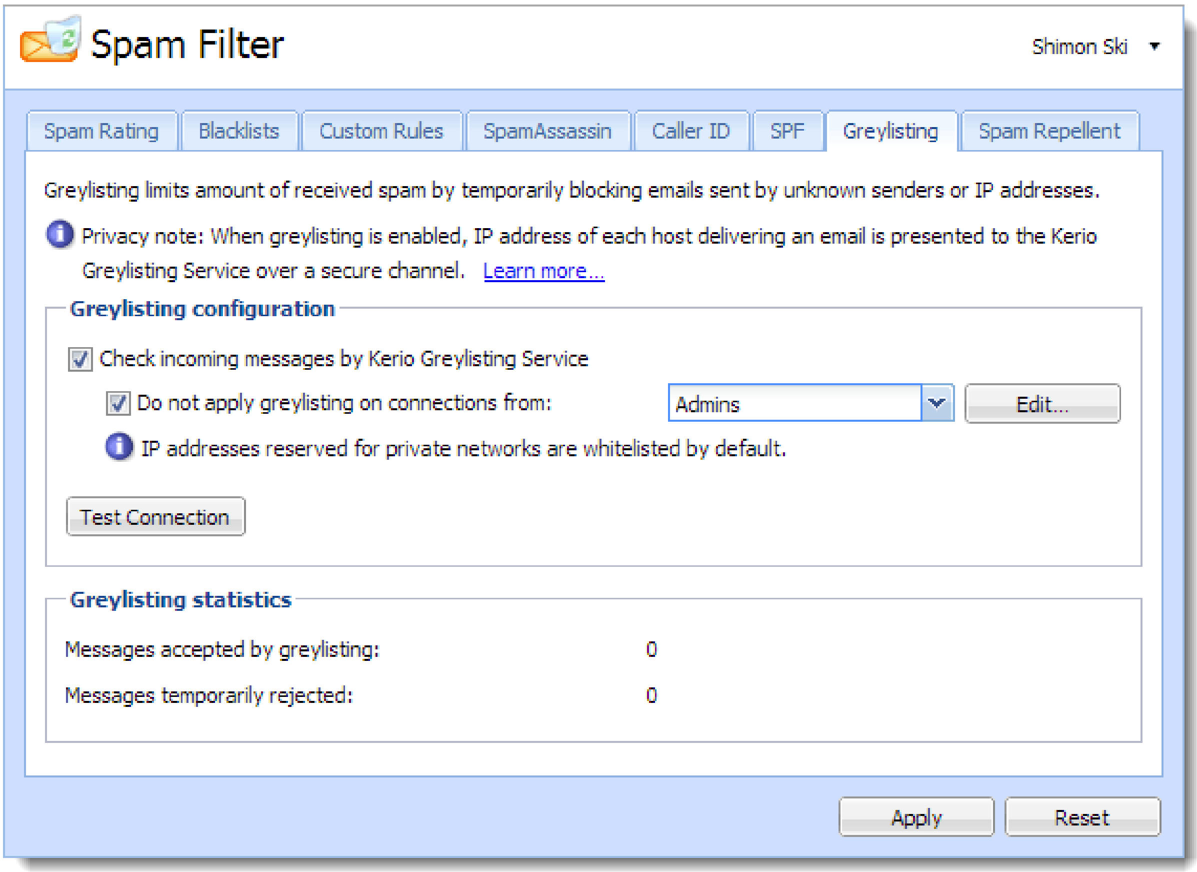
1. In the administration interface, go to section **Configuration** → **Content filter** → **Spam Filter** tab **Greylisting**.
2. Check option **Check incoming messages by Kerio Greylisting Service**.

   > Make sure your firewall allows outgoing connection on port 8045.

3. You can create a list of IP addresses which will not be included in the greylisting check.
4. **Test Connection** with the Kerio Greylisting Service.

   > The connection is established every time Kerio Connect server is restarted.

5. Save the settings.



Greylisting limits amount of received spam by temporarily blocking emails sent by unknown senders or IP addresses.

Privacy note: When greylisting is enabled, IP address of each host delivering an email is presented to the Kerio Greylisting Service over a secure channel. Learn more...

Greylisting configuration

☑ Check incoming messages by Kerio Greylisting Service

☑ Do not apply greylisting on connections from: Admins

IP addresses reserved for private networks are whitelisted by default.

Greylisting statistics

Messages accepted by greylisting: 0

Messages temporarily rejected: 0

Figure 1 Greylisting

How greylisting works

What 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 does contain** the message sender's IP address, the message is delivered immediately.

3. If **the list does not contain** the sender's IP address, the greylisting server delays the delivery — trustworthy mailservers retry to deliver 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 be delivered immediately (see step 2).

To learn more about the greylisting method, 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 envelope email address and recipient envelope email addresses
- the IP address of the host delivering the message

The data is periodically deleted.

If the 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.

Troubleshooting

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

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

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

If you wish 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 or renew your license, it may take several minutes before the Kerio Greylisting Service recognizes it. You may get warning messages in the meantime. This does not affect message delivery.

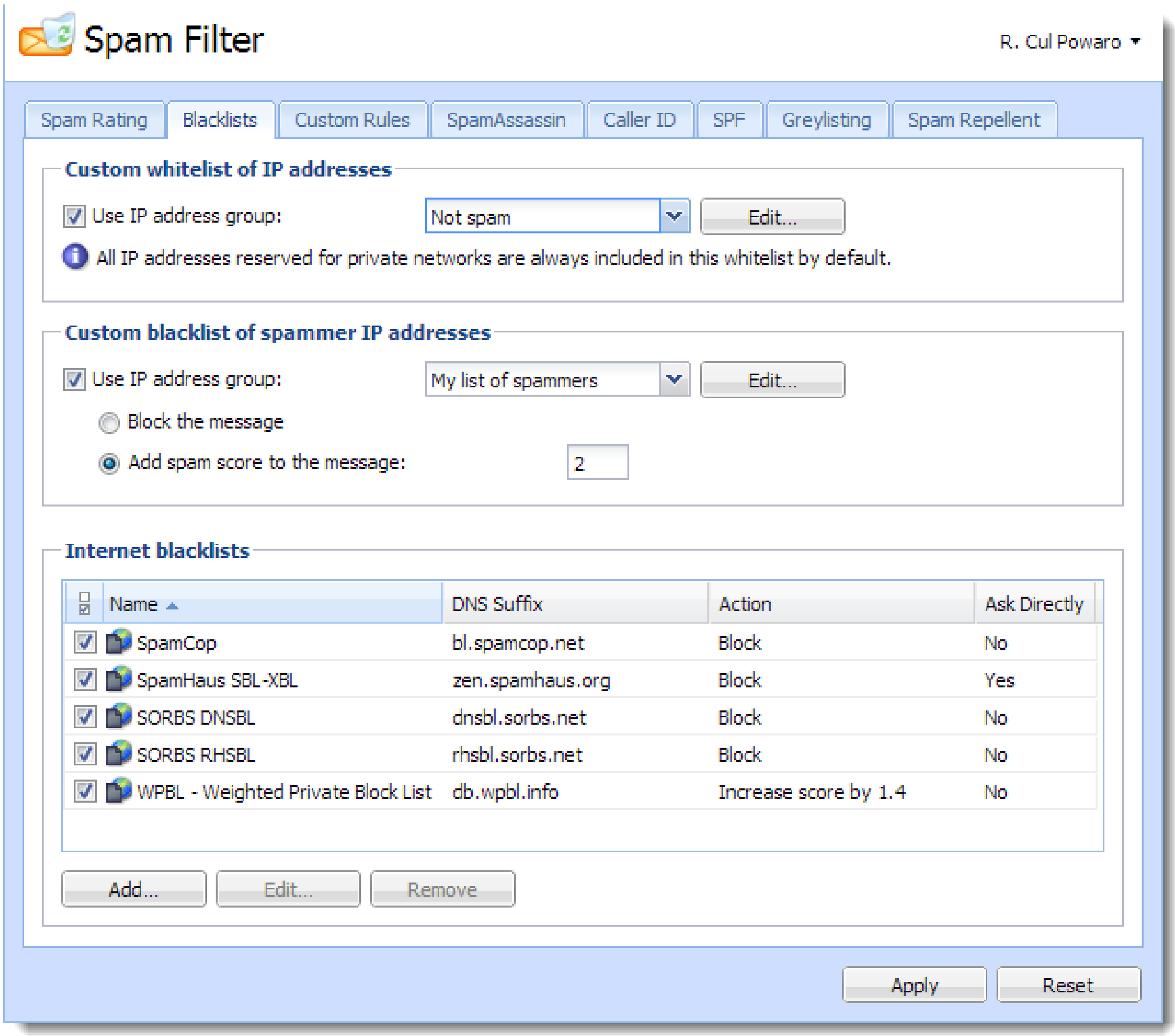
Blocking messages from certain servers

How to automatically block or allow messages from certain servers

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

You can do so by:

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



Custom whitelist of IP addresses

☑ Use IP address group: Not spam

All IP addresses reserved for private networks are always included in this whitelist by default.

Custom blacklist of spammer IP addresses

☑ Use IP address group: My list of spammers

○ Block the message

● Add spam score to the message: 2

Internet blacklists

	Name	DNS Suffix	Action	Ask Directly
☑	SpamCop	bl.spamcop.net	Block	No
☑	SpamHaus SBL-XBL	zen.spamhaus.org	Block	Yes
☑	SORBS DNSBL	dnsbl.sorbs.net	Block	No
☑	SORBS RHSBL	rhsbl.sorbs.net	Block	No
☑	WPBL - Weighted Private Block List	db.wpbl.info	Increase score by 1.4	No

Figure 1 Blacklists tab

Blocking messages from spam servers — custom blacklists

To create your own **Blacklists** you need the IP addresses of the servers which you wish to block

1. In section **Configuration** → **Definition** → **IP Address Groups** create a new group with IP addresses of spam servers.
2. Go to section **Configuration** → **Content Filter** → **Spam Filter** → **tab Blacklists**.
3. In section **Custom blacklist of spammer IP addresses**, check option **Use IP address group**.
4. Select or create a group of IP addresses in the drop-down menu.
5. Select the action which will be performed once messages meet your criteria. You can:
    - block messages (mark them as spam)
    - add spam score to message rating
6. Click on **Apply** in the bottom right corner.

Blocking messages from spam servers — public databases

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

If you wish to use blacklists from **public databases**, follow these steps:

1. Go to section **Configuration** → **Content Filter** → **Spam Filter** → **tab Blacklists**.
2. In section **Internet blacklists**, check all the public databases you wish to use.
3. Double-click a blacklist to select the action which will be performed when Kerio once messages meet the blacklist's criteria. You can:
    - block messages (mark them as spam)
    - add spam score to message rating
4. Click on **Apply** in the bottom right corner.

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

1. In the same section, click on **Add**.
2. Enter the DNS name of the server which handles the enquires of Kerio Connect.
3. Select the action which will be performed once messages meet blacklist's criteria. You can:

- block messages (mark them as spam)
- add spam score to message rating

4. Click on **Apply** in the bottom right corner.

You can also change any blacklist by double-clicking on it.

If you use a paid blacklist, always check 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.

If you wish to create your own whitelist:

1. In section **Configuration** → **Definition** → **IP Address Groups** create a new group with IP addresses of trusted servers.

2. Go to section **Configuration** → **Content Filter** → **Spam Filter** → **tab Blacklists**.

3. In section **Custom whitelist of IP addresses**, check option **Use IP address group**.

4. Select the group of IP addresses in the drop-down menu.

5. Confirm.

Configuring Caller ID and SPF in Kerio Connect

What is Caller ID and SPF

Caller ID and SPF allow 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.

How to configure Caller ID

1. In the administration interface, go to section **Configuration** → **Content Filter** → **Spam filter** → **tab Caller ID.**

2. Enable option **Check Caller ID of every incoming message**.

3. If a message is intercepted, Kerio Connect can

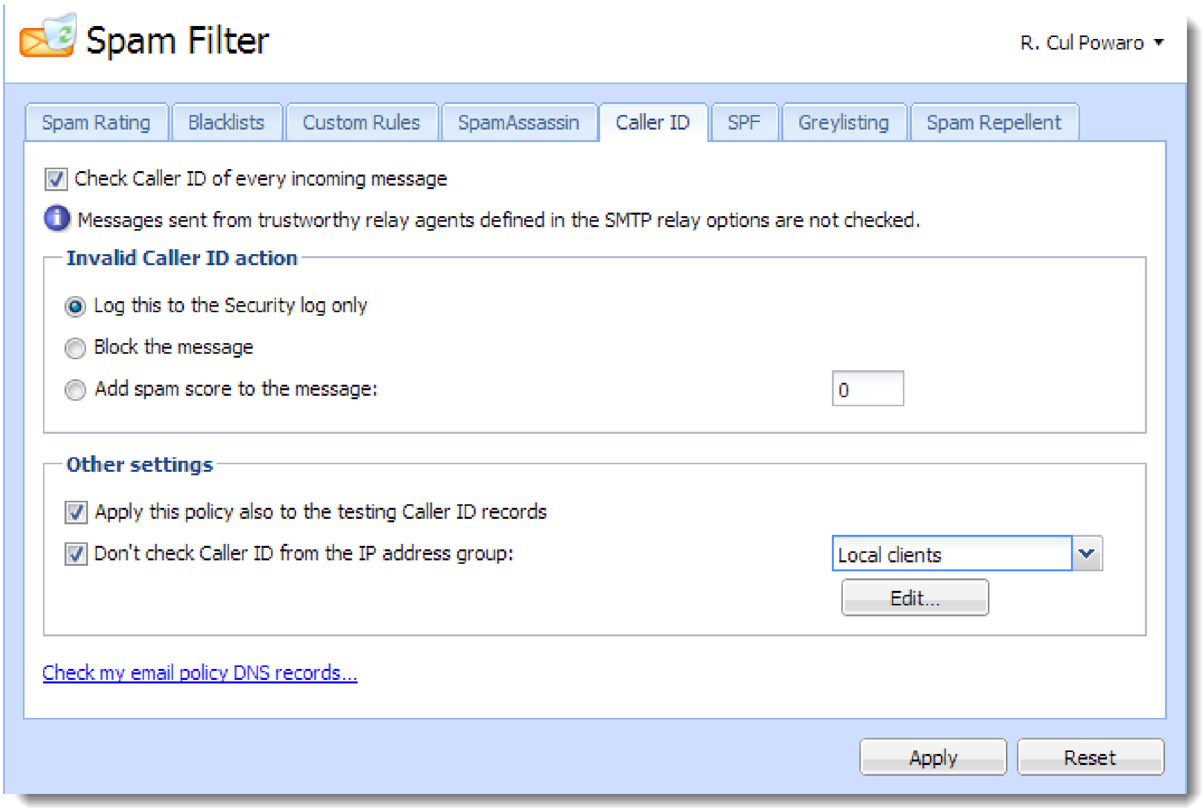
   - log it in the Security log
   - reject it
   - increase/decrease spam score of the message

4. Caller ID is nowadays often used by domains in testing mode only. We recommend to enable **Apply this policy also to testing Caller ID records**.

5. If messages are sent through backup server, create a group of IP addresses of such servers which will not be checked by Caller ID.

6. Confirm.

Kerio Technologies enables you to check your own DNS records. Link **Check my email policy DNS records** in this tab will display a website where you can check them. Check this article for information about creating SPF and Caller ID records.



☑ Check Caller ID of every incoming message

Messages sent from trustworthy relay agents defined in the SMTP relay options are not checked.

● Log this to the Security log only

○ Block the message

○ Add spam score to the message: 0

☑ Apply this policy also to the testing Caller ID records

☑ Don't check Caller ID from the IP address group: Local clients

Figure 1 Caller ID

How to configure SPF

1. In the administration interface, go to section **Configuration** → **Content Filter** → **Spam filter** → **SPF.**

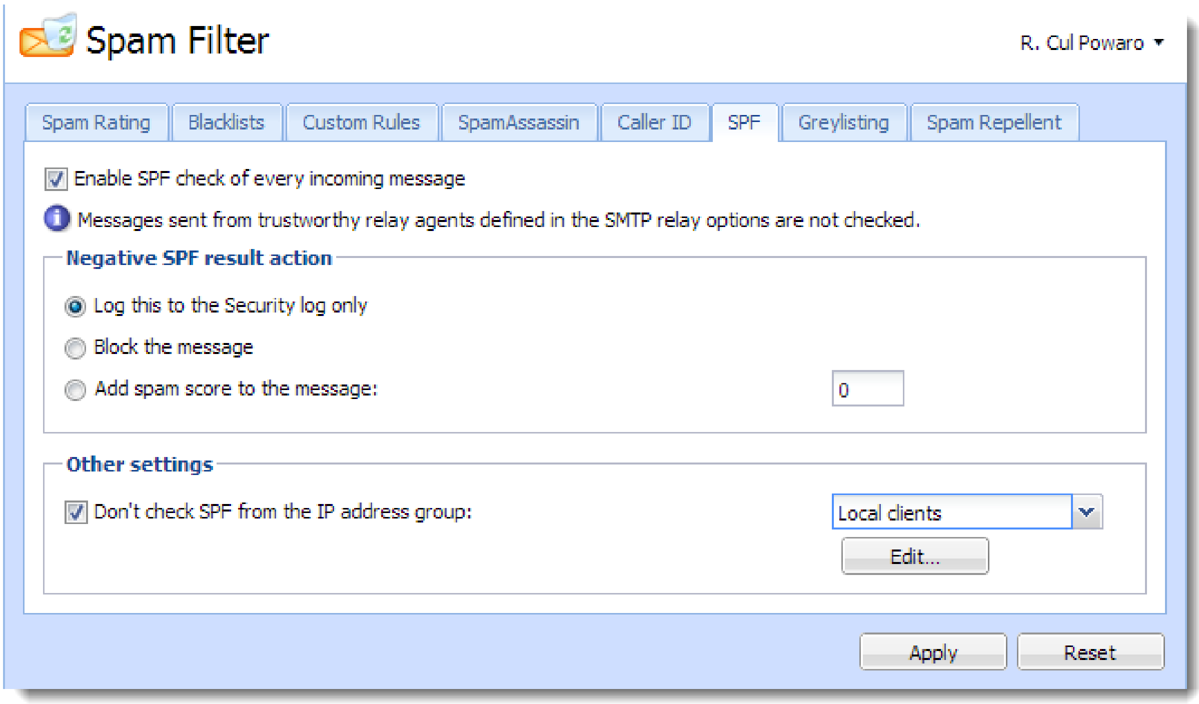
2. **Enable SPF check of every incoming message.**

3. If a message is intercepted, Kerio Connect can

    - log it in the Security log
    - reject it
    - increase/decrease spam score of the message

4. If messages are sent through backup server, create a group of IP addresses of such servers which will not be checked by SPF.

5. Confirm.



Spam Filter

☑ 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

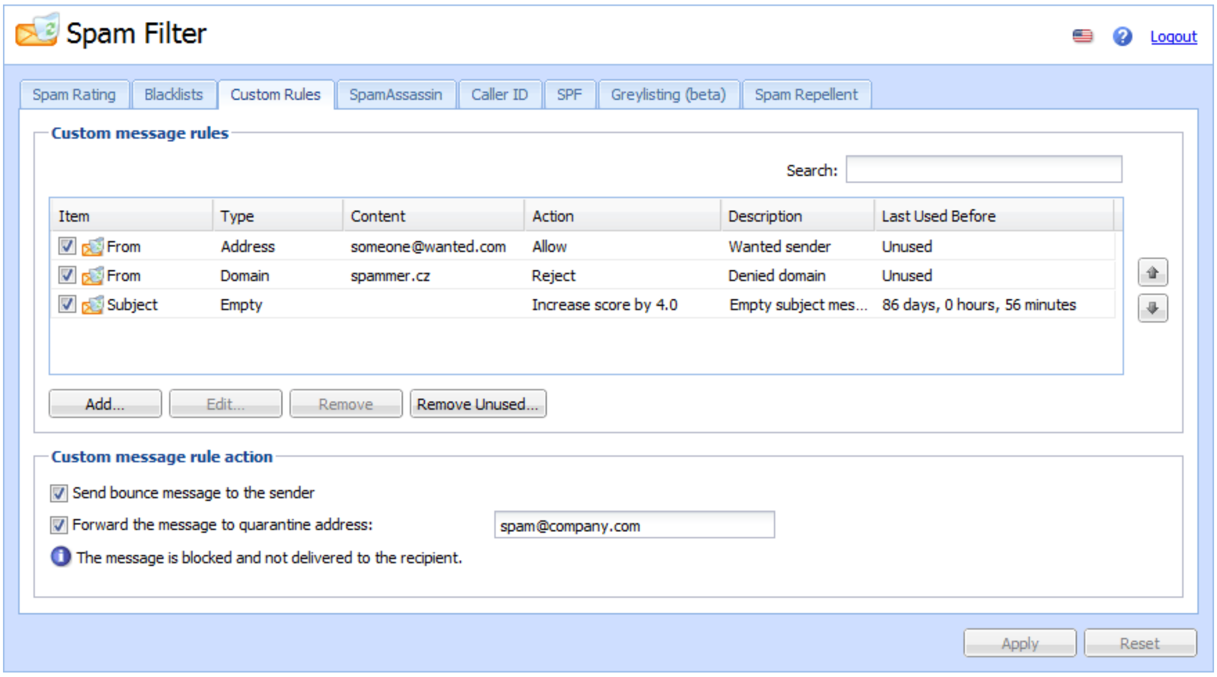
Figure 2 SPF

Creating custom rules for spam control in Kerio Connect

Why to create custom rules

Kerio Connect allows you to create your own antispam rules. Rules are based on filtering email headers and/or email bodies.

Custom rules for spam control can be created in section **Configuration** → **Content Filter** → **Spam Filter** → **tab Custom rules.**



Item	Type	Content	Action	Description	Last Used Before
☑ From	Address	someone@wanted.com	Allow	Wanted sender	Unused
☑ From	Domain	spammer.cz	Reject	Denied domain	Unused
☑ Subject	Empty		Increase score by 4.0	Empty subject mes...	86 days, 0 hours, 56 minutes

☑ Send bounce message to the sender

☑ Forward the message to quarantine address: spam@company.com

The message is blocked and not delivered to the recipient.

Figure 1 Custom rules for spam control

Creating custom rules

You can create as many rules as you wish:

1. In the administration interface, go to section **Configuration** → **Content Filter** → **Spam Filter** → **tab Custom rules.**
2. Click on **Add** and enter a name for the rule.
3. Decide whether to filter **Mail header** or **Mail body** and define the filter.

You can use * (representing any number of characters) and ? (representing max. 1 character) or regular expressions.

4. Messages which match the filter:

   - marked as non-spam
   - mark as spam and rejected
   - increase/decrease spam score

5. Confirm.

Custom rules are processed in the same order as they are listed. If a message is marked as non-spam or rejected, the following rules are not performed.

Messages rejected by tests against the `From` and `To` headers are not processed by other antispam and antivirus tests. Since this decreases the load on your server, place the tests at the top.

For further information concerning "Regular expressions", please consult the Spamassassin page.
One example for regular expressions:

- **cialis** should be blocked, but spe**cialis**t, so**cialis**t etc., not
- regular expression would look like this:

If you define a filter which blocks messages including `cialis` not in the regular expressions convention, Kerio Connect will block all messages which include this string, e.g. messages with the word `specialist`.

Defining actions for custom rules

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

- Send bounce message to the sender — this option is not recommended. Spammers usually use fake addresses and your bounce message will be undeliverable.

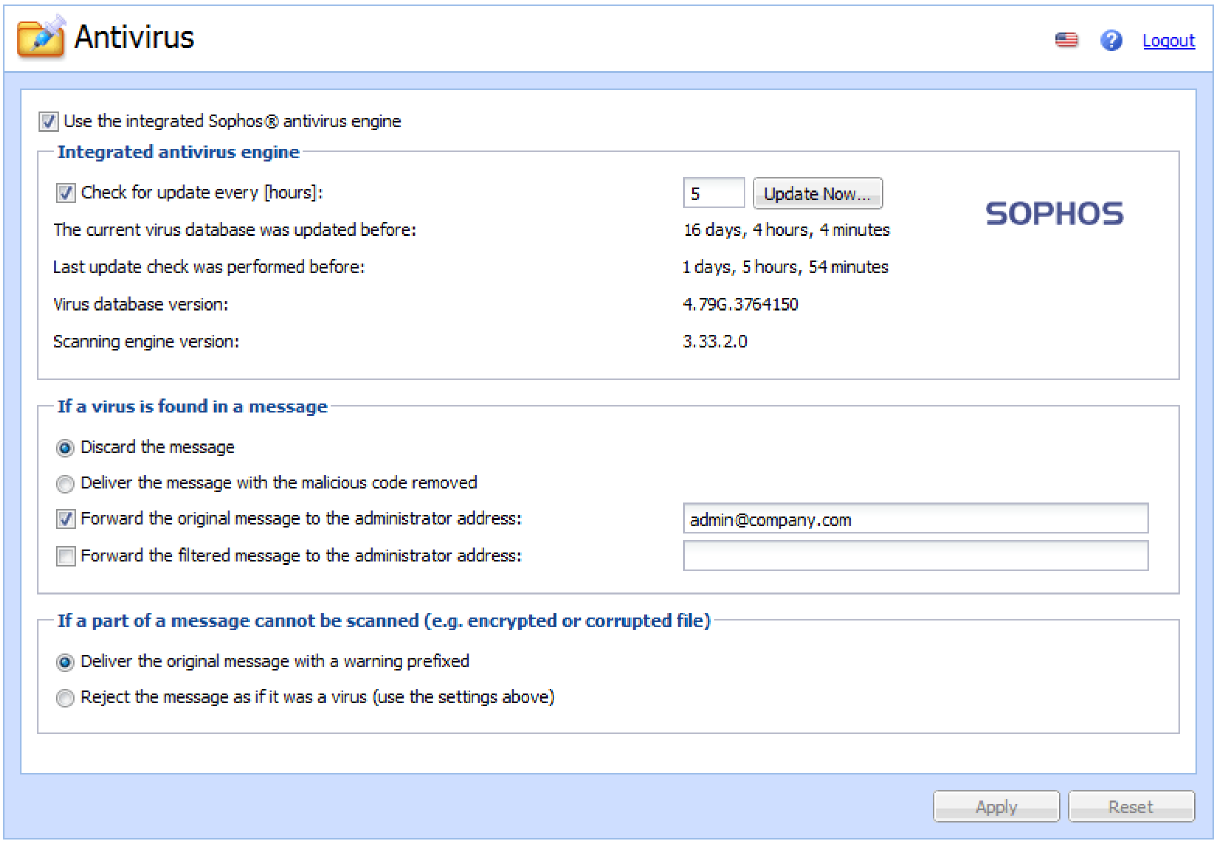
- Forward the message to quarantine address — this option is recommended due to the possibility of missing important emails by false positives.

Antivirus control in Kerio Connect

Antivirus in Kerio Connect

Kerio Connect can check all incoming messages for viruses. For this purpose, purchase Kerio Connect with the Sophos antivirus.

Immediately after the installation of Kerio Connect, the internal Sophos antivirus starts automatically.



☑ Use the integrated Sophos® antivirus engine

Integrated antivirus engine

☑ Check for update every [hours]: 5

The current virus database was updated before:	16 days, 4 hours, 4 minutes
Last update check was performed before:	1 days, 5 hours, 54 minutes
Virus database version:	4.79G.3764150
Scanning engine version:	3.33.2.0

If a virus is found in a message

● Discard the message

○ Deliver the message with the malicious code removed

☑ Forward the original message to the administrator address: admin@company.com

□ Forward the filtered message to the administrator address:

If a part of a message cannot be scanned (e.g. encrypted or corrupted file)

● Deliver the original message with a warning prefixed

○ Reject the message as if it was a virus (use the settings above)

Figure 1 Kerio Connect — antivirus section

For further information on how to secure your computer against viruses, read on filtering message attachments.

External antivirus

If you are upgrading from an earlier version (pre 8.0) and have been using an external antivirus plugin, you can still use it after the upgrade to Kerio Connect 8.0 (read this article).

Kerio Technologies has also 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.

Read our blog to get detailed information.

Configuring Sophos in Kerio Connect

To configure the integrated Sophos:

1. In the administration interface, go to section **Configuration** → **Content Filter** → **Antivirus**.
2. Check option **Use the integrated Sophos antivirus engine**.
3. Enable option **Check for update every [hour]**. Set the interval for the periodical updates of the virus database.

   Provide persistent Internet connection (automated dialing is not supported).

   The database files are downloaded via the HTTP protocol. Allow the communication on your firewall or proxy server.

   Virus database updates are not available for unregistered trial versions.

4. If virus is found, Kerio Connect will:
   - **Discard the message**
   - **Deliver the message with the malicious code removed**
5. In addition, Kerio Connect can:
   - **Forward the original message to an administrator address**
   - **Forward the filtered message to an administrator address**
6. If the message cannot be scanned, Kerio Connect will:
   - **Deliver the original message with a warning**
   - **Reject the message**
7. Confirm the settings.

Configuring HTTP proxy server

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

1. Go to section **Configuration** → **Advanced Options** → **tab HTTP Proxy**.
2. Check option **Use HTTP proxy for ...**
3. Specify the address and port of the proxy server.
4. If required, enter the authentication data.
5. Confirm the settings.

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

Troubleshooting

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

When troubleshooting consult these logs:

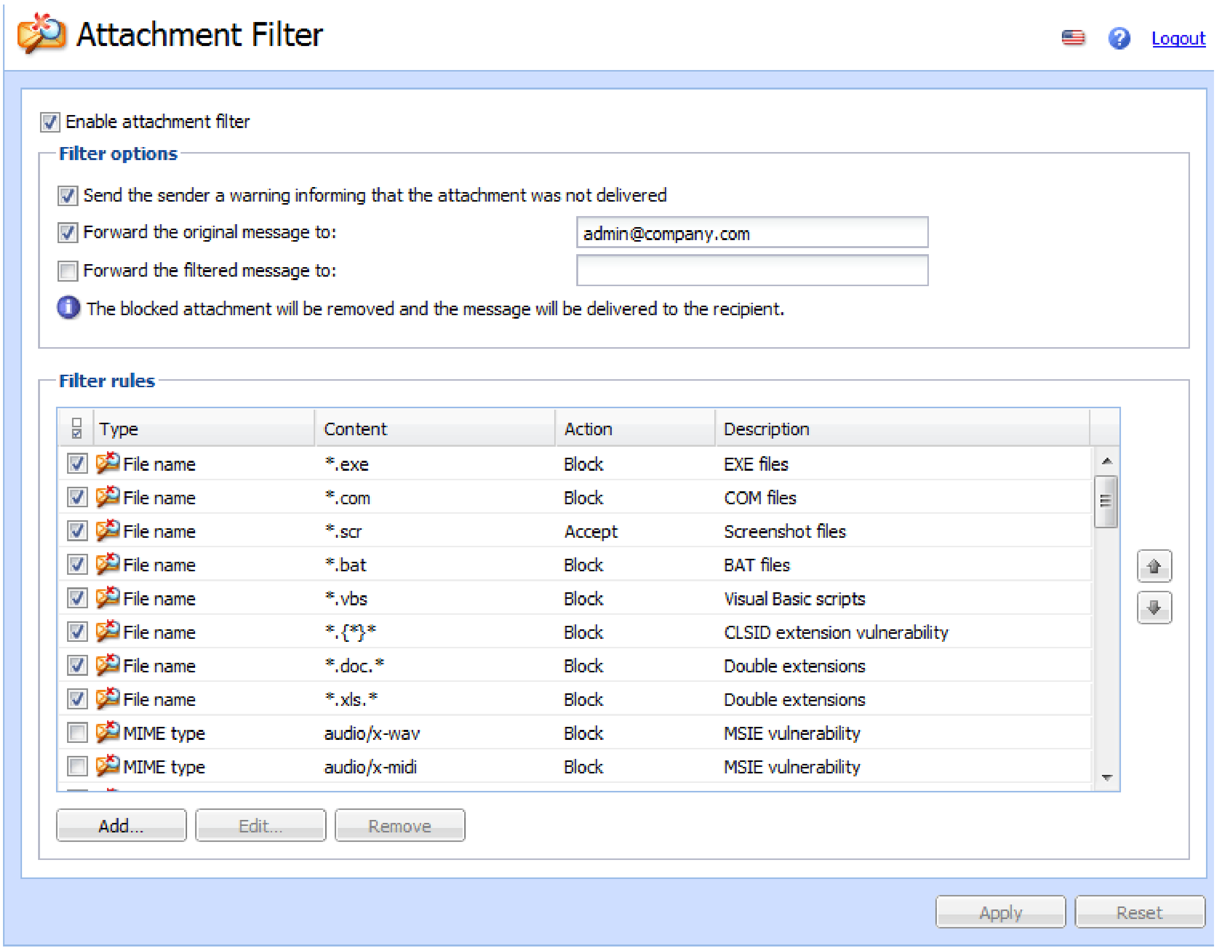
- Security — information about virus database updates
- Debug — right-click the Debug log area and enable **Messages** → **Antivirus Checking**

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

Filtering message attachments in Kerio Connect

Why to filter attachments

Many viruses are hidden as email message attachments. Kerio Connect can filter email attachments according to your settings.



☑ Enable attachment filter

Filter options

☑ Send the sender a warning informing that the attachment was not delivered

☑ Forward the original message to: admin@company.com

□ Forward the filtered message to:

The blocked attachment will be removed and the message will be delivered to the recipient.

Filter rules

☑	Type	Content	Action	Description
☑	File name	*.exe	Block	EXE files
☑	File name	*.com	Block	COM files
☑	File name	*.scr	Accept	Screenshot files
☑	File name	*.bat	Block	BAT files
☑	File name	*.vbs	Block	Visual Basic scripts
☑	File name	*.{*}*	Block	CLSID extension vulnerability
☑	File name	*.doc.*	Block	Double extensions
☑	File name	*.xls.*	Block	Double extensions
□	MIME type	audio/x-wav	Block	MSIE vulnerability
□	MIME type	audio/x-midi	Block	MSIE vulnerability

Figure 1 Kerio Connect — attachment filter

How to configure attachment filter in Kerio Connect

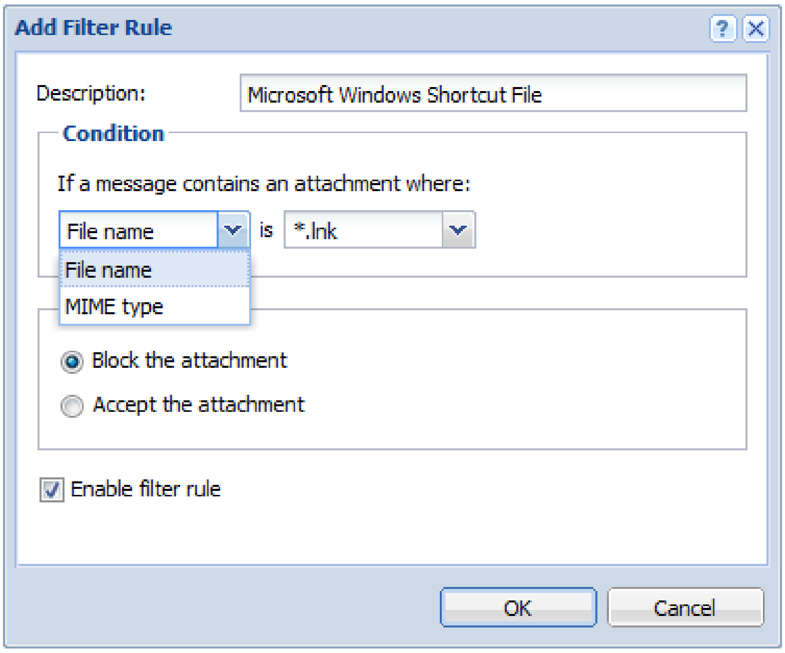
To configure the attachment filter:

1. In the administration interface, go to section **Configuration** → **Content Filter** → **Attachment Filter**.
2. Check option **Enable attachment filter**.

3. Decide whether the sender will be warned if their attachment is blocked.

4. Specify email addresses to which original and/or filtered messages will be sent (e.g. for verification of proper functionality of the attachment filter).

5. Select any of the predefined filter rules or add a new one.



Add Filter Rule

Description: Microsoft Windows Shortcut File

Condition

If a message contains an attachment where:

File name is *.lnk

● Block the attachment

○ Accept the attachment

☑ Enable filter rule

Figure 2 Filter rule

Each rule can allow or block one specific attachment.

6. Confirm the settings.

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

Troubleshooting

For information on attachment filtering, 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.

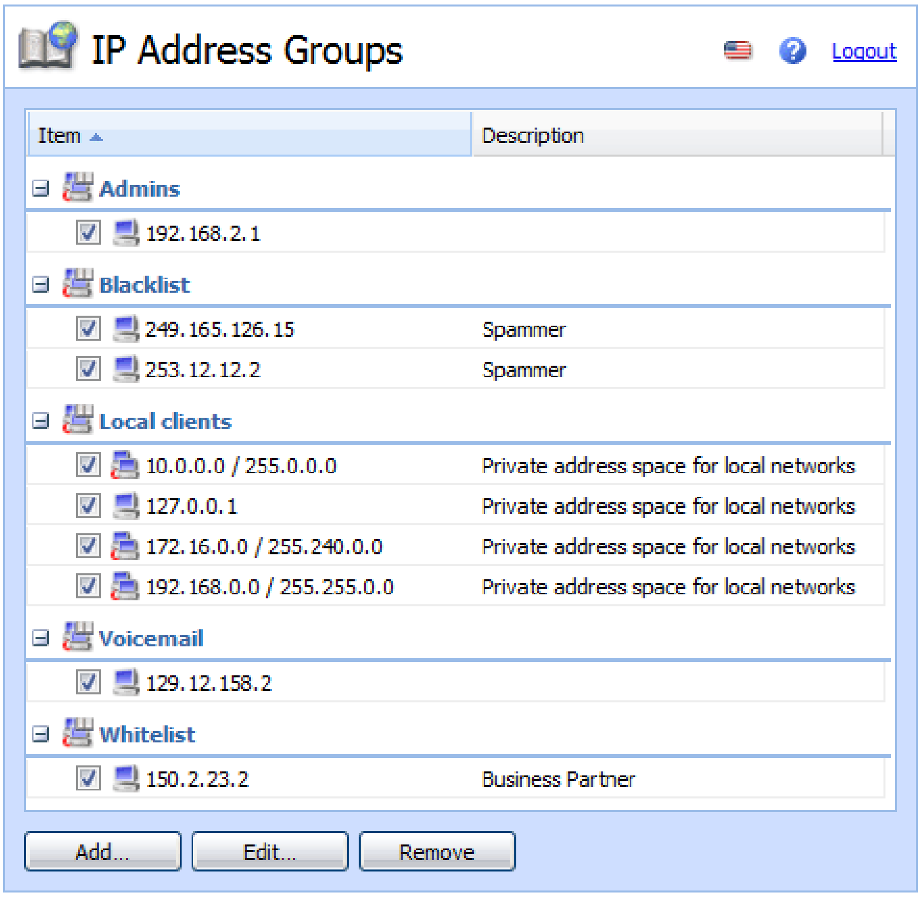
Get the SDK and read our blog to get detailed information.

Configuring IP address groups

When to use IP address groups

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

- remote administration
- Kerio Connect services
- spam (creating whitelist, blacklists, etc.)



Item ▲	Description
⊟ Admins	
☑ 192.168.2.1	
⊟ Blacklist	
☑ 249.165.126.15	Spammer
☑ 253.12.12.2	Spammer
⊟ Local clients	
☑ 10.0.0.0 / 255.0.0.0	Private address space for local networks
☑ 127.0.0.1	Private address space for local networks
☑ 172.16.0.0 / 255.240.0.0	Private address space for local networks
☑ 192.168.0.0 / 255.255.0.0	Private address space for local networks
⊟ Voicemail	
☑ 129.12.158.2	
⊟ Whitelist	
☑ 150.2.23.2	Business Partner

Figure 1 IP address groups

How to configure IP address group

Group of local IP addresses is created automatically. This group can be edited, removed or otherwise manipulated.

1. In the administration interface, go to section **Configuration** → **Definitions** → **IP Address Groups**.
2. Click on **Add** and enter a name for the group (or select an existing one).
3. Select the type and specify the address(es).The following types are available:
    - a single IP address (host)
    - range of IP addresses
    - net with corresponding mask
    - another IP address group
4. You can add a description for better reference.
5. Confirm.

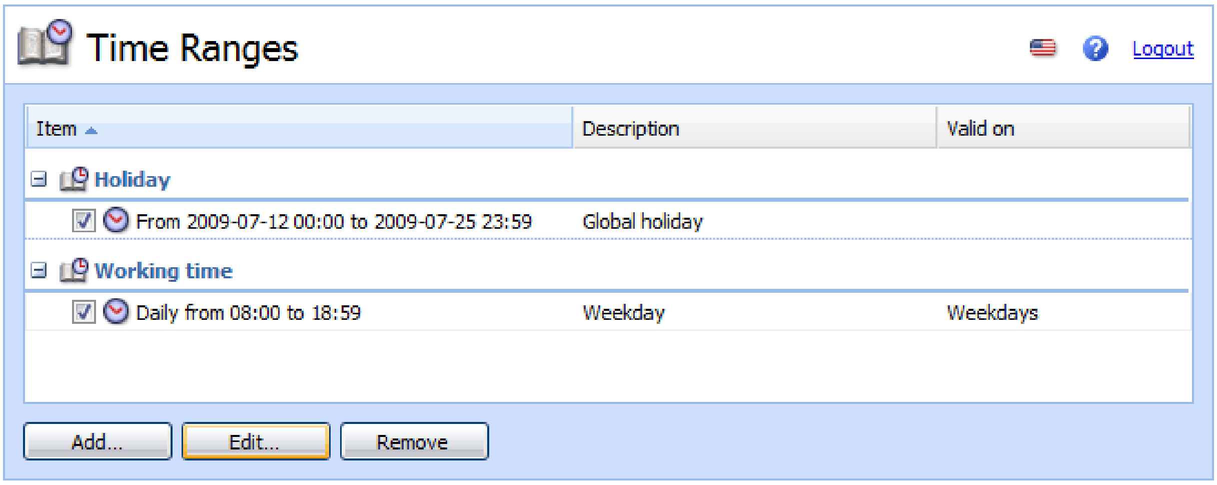
IP address groups are used in many settings in Kerio Connect. Whenever a section in the administration interface allows IP groups, you will be to configure them directly from this section.

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.



Time Ranges

Item	Description	Valid on
⊟ Holiday		
☑ From 2009-07-12 00:00 to 2009-07-25 23:59	Global holiday	
⊟ Working time		
☑ Daily from 08:00 to 18:59	Weekday	Weekdays

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.

Public folders in Kerio Connect

What are public folders

Public folders are folders (mail, calendars, contacts, tasks, notes) which are available to all users in a domain or Kerio Connect.

Creating public folders

You can create public folders in Kerio Connect client, Microsoft Outlook (with Kerio Outlook Connector), Microsoft Outlook for Mac 2011 or Microsoft Entourage.

Only users with appropriate rights can create public folders.

Global vs. domain public folders

In Kerio Connect, public folders can be

- different for each domain
- available to users of all domains

To configure the public folders:

1. Go to the administration interface to section **Configuration** → **Domains**.
2. Click on **Public Folders** (right bottom corner) and select your option.
3. Confirm.

⚠ If you change the settings when the system of public folders has already been created, you have to create new public folders — users will not be able to see the old ones.

Assigning rights to create public folders

1. In the administration interface, go to section **Accounts** → **Users**.
2. Double-click a user and go to tab **Rights**.
3. Check option **Public folders** and save the settings.

Creating public folders

To create a public folder:

1. Go to Kerio Connect client.

2. In the left folder tree, right-click on **Public folders** and create a new one.

3. By default, all newly created public folders are shared with all users of the domain (for viewing).

   To edit sharing rights, right-click the folder in Kerio Connect client and select **Sharing**.

Similar procedures in Microsoft Outlook (with Kerio Outlook Connector), Microsoft Outlook for Mac 2011 or Microsoft Entourage.

Viewing public folders

Whenever a public folder is available for a user, it is automatically displayed in Kerio Connect client (or other client).

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

Account	Email	Contacts	Calendar	Tasks	Notes
Kerio Outlook Connector (Offline Edition)	YES	YES	YES	YES	YES
Kerio Outlook Connector	YES	YES	YES	YES	YES
Kerio Connect client	YES	YES	YES	YES	YES
Microsoft Outlook for Mac 2011	YES	YES	YES	YES	YES
Exchange account in Microsoft Entourage	YES	YES[a]	YES[a]	NO	NO
Exchange account in Apple Mail[b]	YES	YES	YES	YES	YES
IMAP (any client that supports the IMAP protocol)	YES (if the client can show them)	NO	NO	NO	NO
POP3 (any client that supports the POP3 protocol)	NO	NO	NO	NO	NO

[a] Only for *Microsoft Entourage 2004 SP2*.

[b] Only if the full support for IMAP is set in the Kerio Connect's configuration file.

Table 1 Viewing public folders in individual account types

Global Address List

In Kerio Connect, all new users can be added into a public contacts folder which is used as an internal source of company contacts (full names and email addresses).

By default, this option is enabled. To disable it:

1. In the administration interface, go to section **Accounts** → **Users.**
2. Double-click the user and on tab **General** uncheck option **Publish in Global Address List.**

> If users are mapped from Active Directory or Apple Open Directory, the entire LDAP database is synchronized every hour automatically.

Configuring instant messaging in Kerio Connect

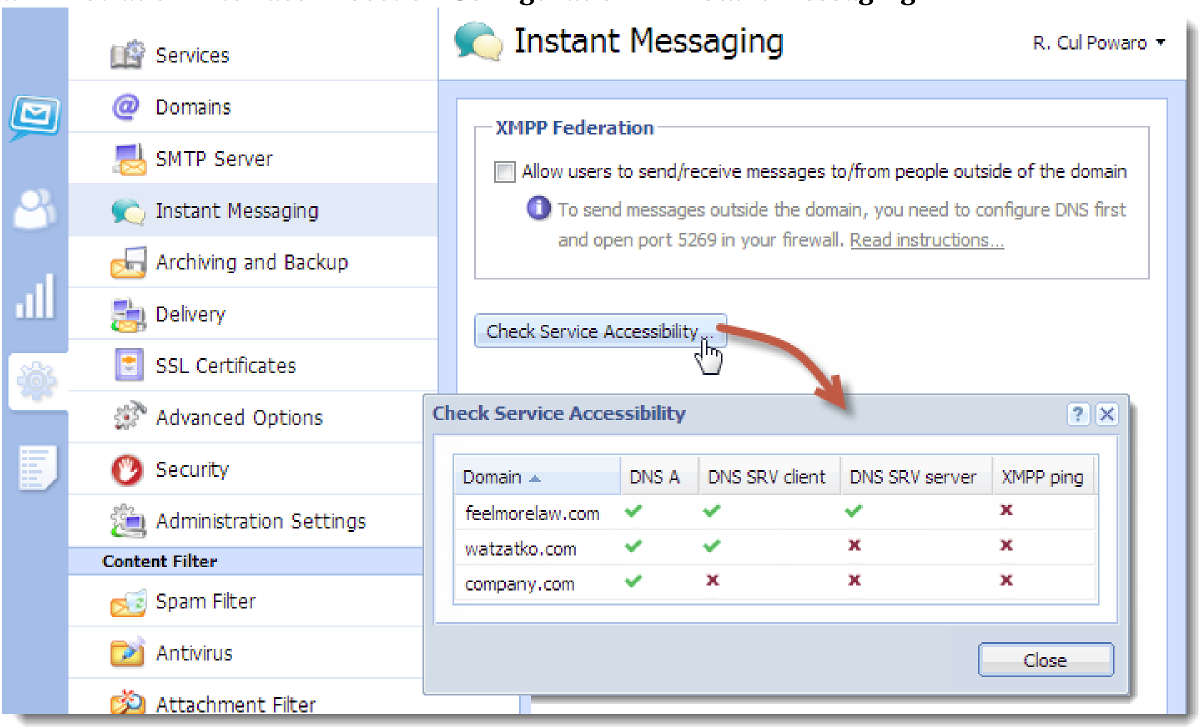
About instant messaging

New in Kerio Connect 8.1!

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**.



☐ Allow users to send/receive messages to/from people outside of the domain

To send messages outside the domain, you need to configure DNS first and open port 5269 in your firewall. Read instructions...

Domain ▲	DNS A	DNS SRV client	DNS SRV server	XMPP ping
feelmorelaw.com	✓	✓	✓	✗
watzatko.com	✓	✓	✗	✗
company.com	✓	✗	✗	✗

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**.

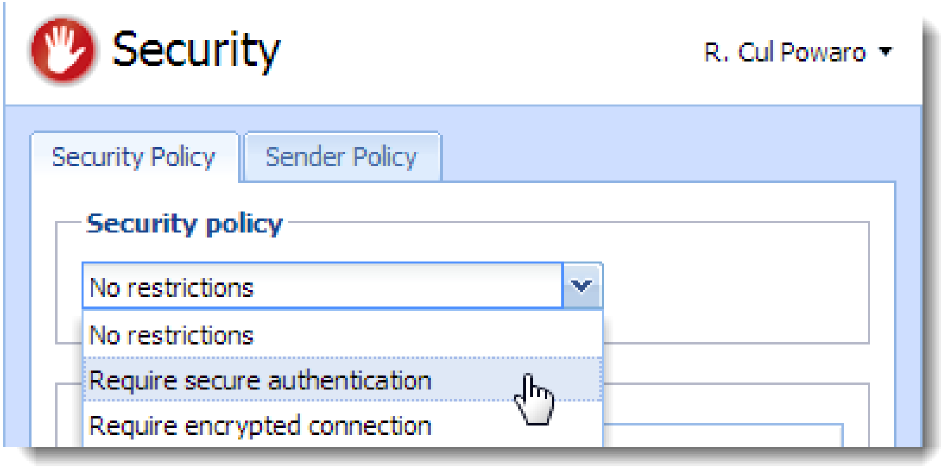
These settings are valid for all domains on the server. You can override them by individual user settings (on tab **Messages**) or group settings (tab **Rights**).

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)

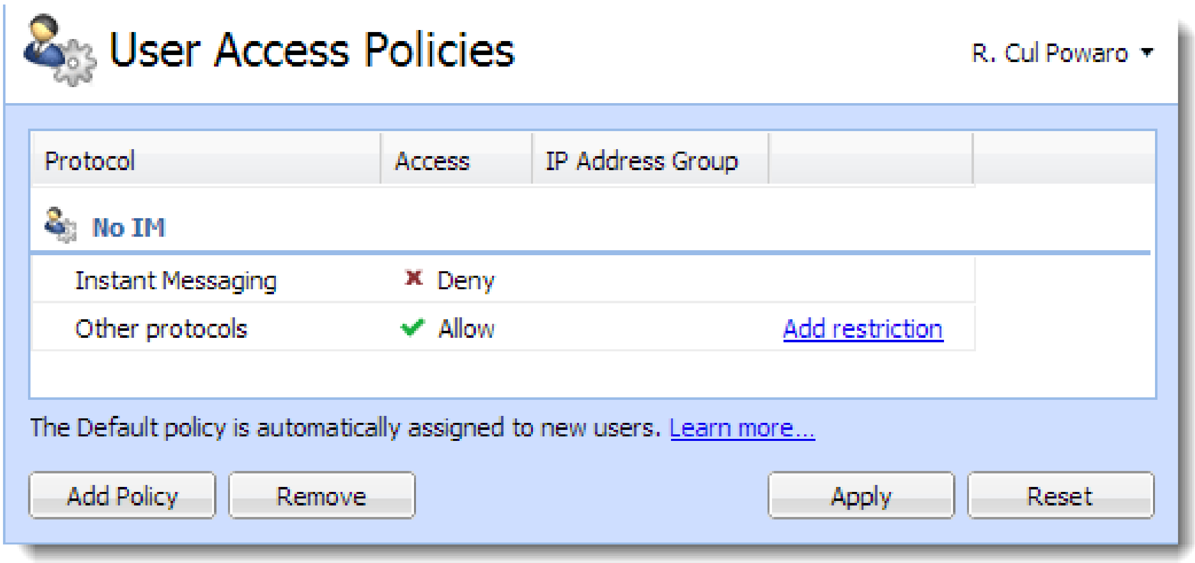
You can also enable only the secure instant messaging service (port 5223) and use SSL.

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



Protocol	Access	IP Address Group	
No IM			
Instant Messaging	✗ Deny		
Other protocols	✓ Allow		Add restriction

The Default policy is automatically assigned to new users. Learn more...

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).

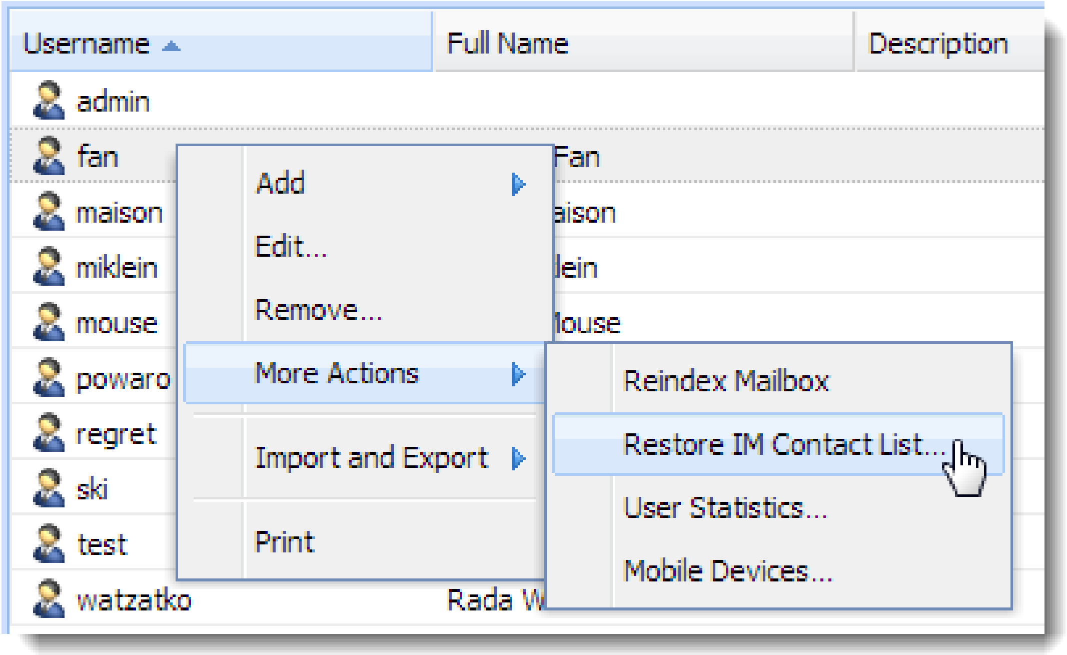
Automatic contact list

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.

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 using a management interface of your DNS registrar.

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

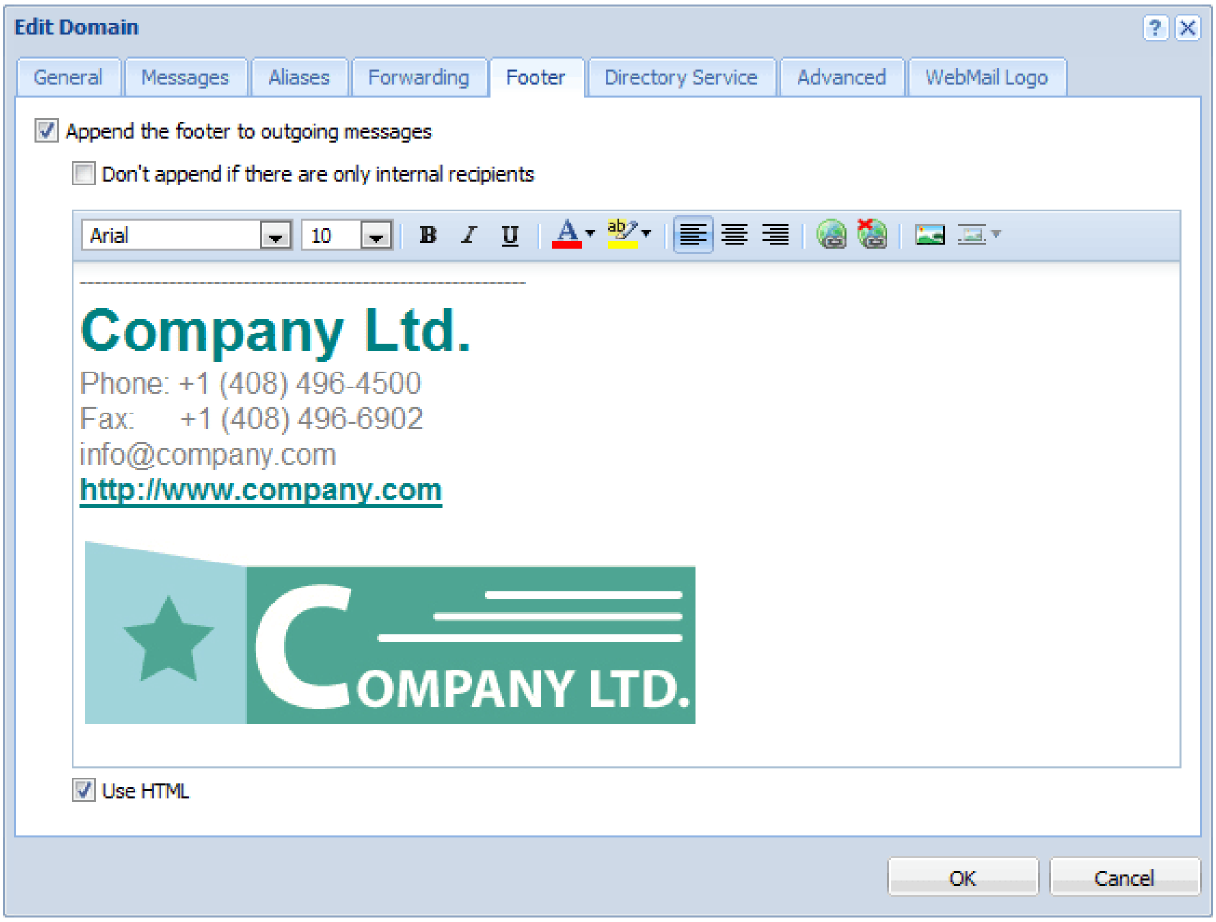
`5222` — port of the service

Customizing Kerio Connect

Defining custom email footers

For each domain, you can customize email footers which will be automatically added to all messages sent from this domain.

1. In the administration interface, go to section **Configuration** → **Domains**.
2. Double-click the domain and go to tab **Footer**.
3. Enable option **Append the footer to outgoing messages.**
4. Create the footer (in plain text or HTML).
5. If you do not want to append footers to messages for internal recipients, check the appropriate option.
6. Confirm.



☑ Append the footer to outgoing messages

□ Don't append if there are only internal recipients

Company Ltd.

Phone: +1 (408) 496-4500

Fax: +1 (408) 496-6902

info@company.com

http://www.company.com

☑ Use HTML

Figure 1 Email footers

If user defines their own email signature, this domain footer will be displayed under the user's signature.

Localizing the user interface

Kerio Connect client 8.1 and newer

For detailed information on how to localize Kerio Connect client, read article Translating Kerio Connect client into a new language.

Kerio Connect client 8.0

Kerio Connect Client is available in various languages.

In the current version of Kerio Connect, you cannot add new translations. However, you can overwrite one of the existing translations:

1. Go to the installation directory of Kerio Connect.
2. Open folder `web\webmail\translations`
3. Select 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.

Old WebMail

Kerio old WebMail is available in various languages.

The source files can be found in the Kerio Connect installation directory in folder `translations` .

To prepare a new language version:

1. Go to folder `translations` in the installation directory of Kerio Connect.
2. Copy one of the files and rename it according to your target language.

3. Open the file in a XML/text editor and translate all text to the target language.

   The XML file starts and ends with the `<translation>` tag. Make sure individual lines have the following form: `<text id=”head-user”>User</text>`.

4. Save the file and restart Kerio Connect.

The text in the language files must be coded in UTF-8.

Additional settings for old WebMail

How to add new dictionaries for spell-check

The spell-check in Kerio WebMail is based on comparing the phrases with the dictionary, and it is therefore available only for the language versions available in the folder `myspell` where language databases for Kerio Connect are stored.

These dictionaries are available on the Internet (e.g. at OpenOffice). Each dictionary includes two files, following the patterns `language_name.aff` (e.g. fr_FR.aff) and `language_name.dic` (e.g. fr_FR.dic). Copy both files to the myspell folder.

To employ the dictionary in the spellchecker, it is necessary to set it as preferred in the old WebMail settings.

1. In the old Webmail interface, click on **Settings** and go to tab **Mail composing**.
2. In the **Spell-checker dictionary** field, select your preferred dictionary.
3. Confirm.

How to add your own logo to old WebMail

Kerio Connect can display your own logo in the old Webmail interface:

- for all domains in Kerio Connect
- for individual domains separately

To display your logo for all domains:

1. In the administration interface, go to section **Configuration** → **Advanced Options**.
2. Go to tab **Kerio Connect client / WebMail**.

3. Enable option **Use custom logo in old WebMail**.

4. Specify the logo file.

> The logo must be a GIF file with size 200 x 40 pixels.

5. Confirm.

To configure custom logo for individual domains (other than the default one or other than the logo specified in **Configuration** → **Advanced Options** as described above):

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

2. Double-click the domain and go to tab **WebMail logo**.

3. Enable option **Use custom logo for this domain in old WebMail**.

4. Specify the logo file.

> The logo must be a GIF file with size 200 x 40 pixels.

5. Confirm.

> If the skin currently in use contains both the domain logos as well as the individual ones, the domain logos will be used by default.

Translating Kerio Connect client to a new language

Translating Kerio Connect client

New in Kerio Connect 8.1! For information on translating Kerio Connect client in version 8.0, read this 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

The path to data store is first configured during the installation process.

To change the data store folder:

1. Create a new folder for the data store.

   > No diacritics allowed in the folder name.
   > Make sure there is enough free space for the data store.

2. In the administration interface, go to section **Configuration** → **Advanced Options** → **tab Store Directory**.

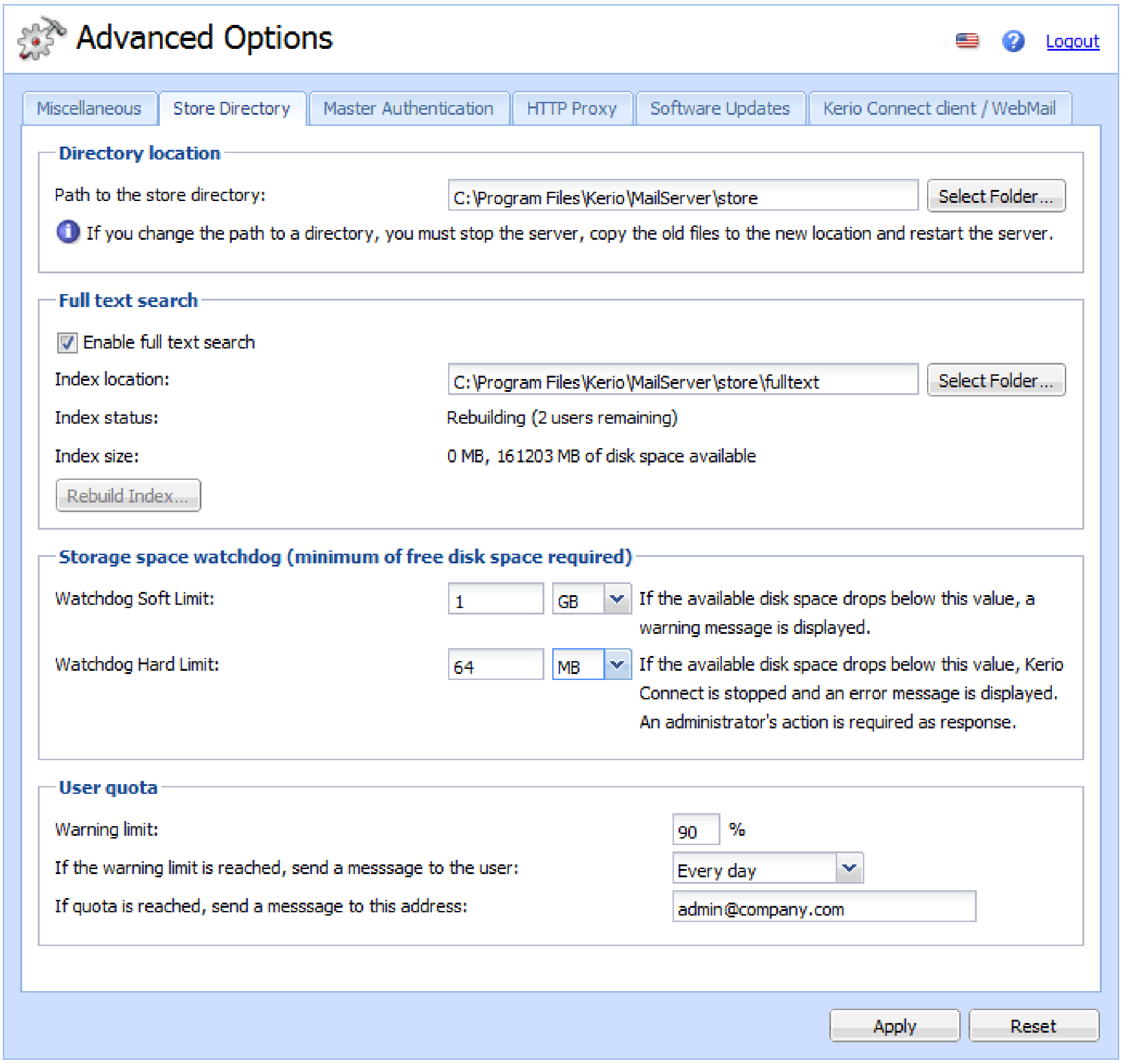
3. Select the new folder and confirm the settings.

   > 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.



Directory location

Path to the store directory: C:\Program Files\Kerio\MailServer\store

If you change the path to a directory, you must stop the server, copy the old files to the new location and restart the server.

Full text search

☑ Enable full text search

Index location: C:\Program Files\Kerio\MailServer\store\fulltext

Index status: Rebuilding (2 users remaining)

Index size: 0 MB, 161203 MB of disk space available

Storage space watchdog (minimum of free disk space required)

Watchdog Soft Limit: 1 GB If the available disk space drops below this value, a warning message is displayed.

Watchdog Hard Limit: 64 MB If the available disk space drops below this value, Kerio Connect is stopped and an error message is displayed. An administrator's action is required as response.

User quota

Warning limit: 90 %

If the warning limit is reached, send a messsage to the user: Every day

If quota is reached, send a messsage to this address: admin@company.com

Figure 1 Store directory

How to configure 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 section **Configuration** → **Advanced Options** → **tab Store Directory**.
2. **Enable full text search.**
3. Specify a folder where the fulltext search index will be stored.

Do not use a UNC path.

4. To create a new index, click on **Rebuild Index.**

   You can rebuild the index for:

   - the whole server
   - one domain
   - one user

5. Save the settings.

Fulltext search may affect the performance of your server.

Data store size

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** → **tab Store Directory**.

Watchdog Soft Limit
If the free space on disk with the data store drops below this value, a message is displayed 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 a message is displayed in the administration interface.

Information about reached limits is logged in the Error log.

Archiving in Kerio Connect

What can you archive

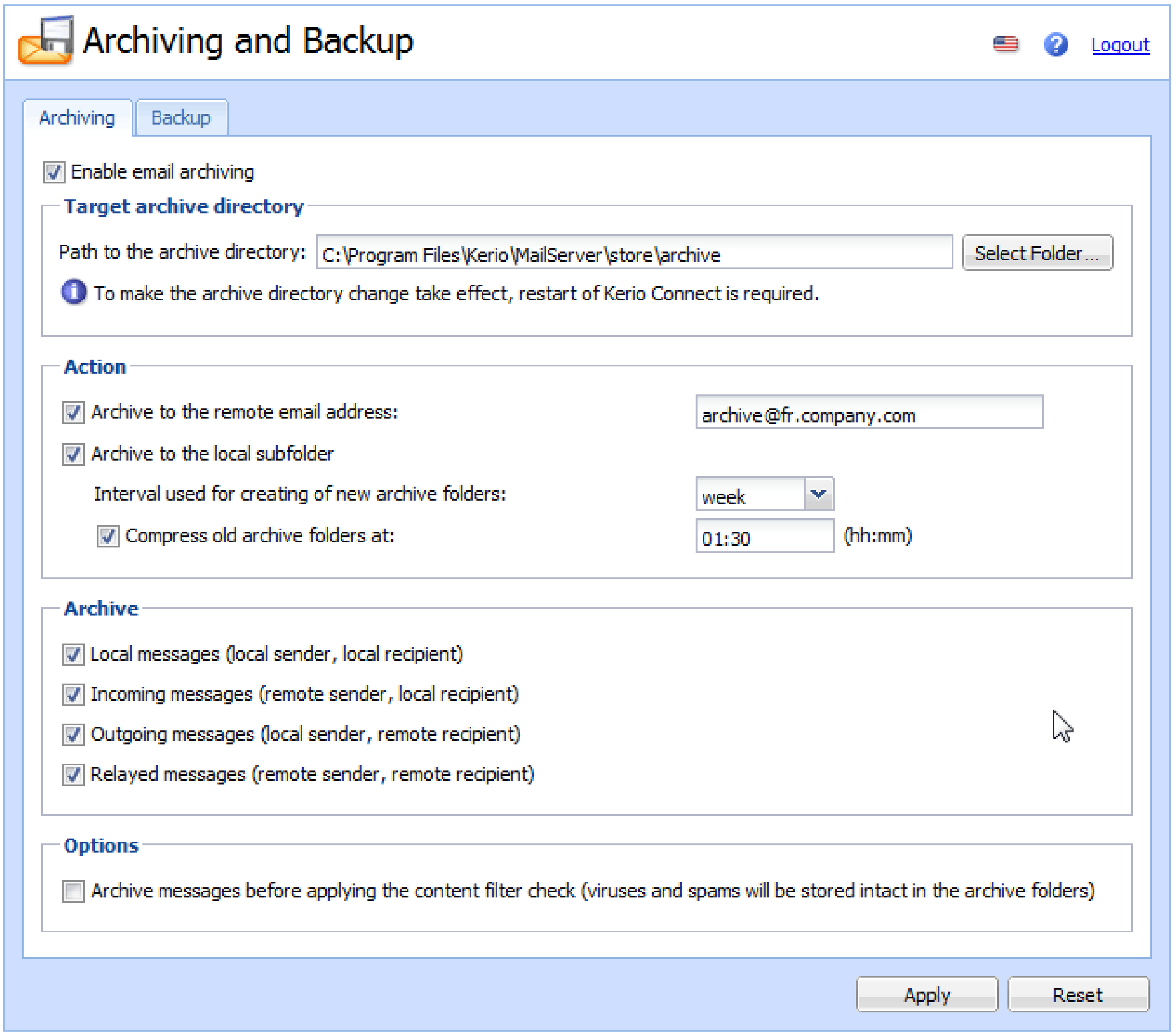
Kerio Connect can store copies of email messages. If you need a particular or deleted message, you can recover them by using email recovery.

You can archive:

- local messages — local sender, local recipient
- incoming messages — remote sender, local recipient
- outgoing messages — local sender, remote recipient
- relayed messages — remote sender, temote recipient

> As opposed to backups, archiving stores only messages (not configuration or any other administration settings).

Archiving can be configured in section **Configuration** → **Archiving and Backup**.



Archiving and Backup

☑ Enable email archiving

Target archive directory

Path to the archive directory: C:\Program Files\Kerio\MailServer\store\archive

To make the archive directory change take effect, restart of Kerio Connect is required.

Action

☑ Archive to the remote email address: archive@fr.company.com

☑ Archive to the local subfolder

Interval used for creating of new archive folders: week

☑ Compress old archive folders at: 01:30 (hh:mm)

Archive

☑ Local messages (local sender, local recipient)

☑ Incoming messages (remote sender, local recipient)

☑ Outgoing messages (local sender, remote recipient)

☑ Relayed messages (remote sender, remote recipient)

Options

□ Archive messages before applying the content filter check (viruses and spams will be stored intact in the archive folders)

Figure 1 Archiving

For archiving of mailing lists, read this article.

Configuring archiving

To configure archiving:

1. In the administration interface, go to section **Configuration** → **Archiving and Backup** → **tab Archiving.**

2. Check **Enable email archiving**.

3. **Select folder** where the archives will be stored.

No diacritics allowed in the folder name.

4. Kerio Connect can also **sent archive files to a remote email address**.

5. To archive messages also to the Kerio Connect installation directory, check option **Archive to the local subfolder**.

6. Select the types of messages you wish to archive.

7. Decide whether to check messages for spam and viruses before archiving.

8. Save the settings.

When changing the archive directory, you need to restart Kerio Connect.

Viewing archive folders

Archive folders are displayed in Kerio Connect client or in Microsoft Outlook with Kerio Outlook Connector (the online edition).

By default, only the administrator of the primary domain can view archive folders. They can also assign rights to other users:

1. In the administration interface, go to section **Accounts** → **Users**.

2. Double-click the user and go to tab **Rights**.

3. Check option **Archive folders** and confirm.

4. Save the settings.

Since messages of all users are archived, only a confidential administrators should access archive folders.

Whenever an archive folder is available for viewing, it is automatically displayed in Kerio Connect client (or other client).

Backups in Kerio Connect

What backups include

In Kerio Connect, the following items can be backed up:

- 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 confiure backups in section **Configuration** → **Archiving and Backup**.

Types of backups

In Kerio Connect, there are two types of backups — **full** backups and **differential** backups.

- **Full backup** stores all files and items.

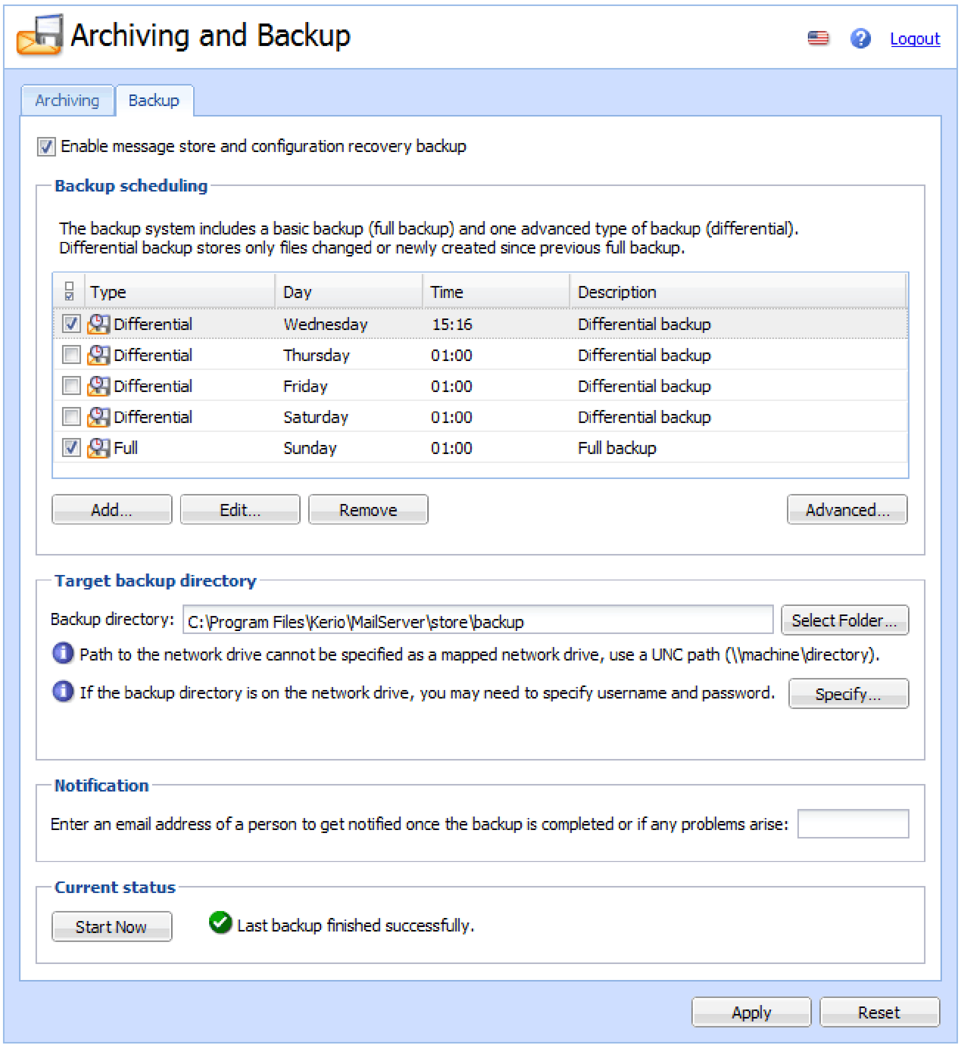
- **Differential backup** stores files that have been added or changed since the last full backup.

You can schedule any number of full and/or differential backups. The number of scheduled backups may depend on:

- size of the data store (influences the time each backup takes nad its size)

- importance of data which might be lost (backups are more frequent in companies where email communication and message storing is important)

If backups are performed frequently, minimum of data is lost if server fails.



☑ Enable message store and configuration recovery backup

Backup scheduling

The backup system includes a basic backup (full backup) and one advanced type of backup (differential). Differential backup stores only files changed or newly created since previous full backup.

	Type	Day	Time	Description
☑	Differential	Wednesday	15:16	Differential backup
□	Differential	Thursday	01:00	Differential backup
□	Differential	Friday	01:00	Differential backup
□	Differential	Saturday	01:00	Differential backup
☑	Full	Sunday	01:00	Full backup

Target backup directory

Backup directory: C:\Program Files\Kerio\MailServer\store\backup

Path to the network drive cannot be specified as a mapped network drive, use a UNC path (\\machine\directory).

If the backup directory is on the network drive, you may need to specify username and password.

Notification

Enter an email address of a person to get notified once the backup is completed or if any problems arise:

Current status

✓ Last backup finished successfully.

Figure 1 Archiving

Configuring backups

To configure the backup schedule:

1. Go to section **Configuration** → **Archiving and Backup** → **tab Backup.**

2. Check option **Enable message store and configuration recovery backup**.

3. Click **Add** and select the type and time when the backup will be performed.

4. Click on 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 diacritics allowed in the folder name.

6. Enter an email address to which messages with info about backups will be delivered.

7. Save the settings.

If you wish to make an immediate backup, click on the **Start Now** button.

Recovering data from backups

To get instructions for data recovery, read this article.

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**).

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

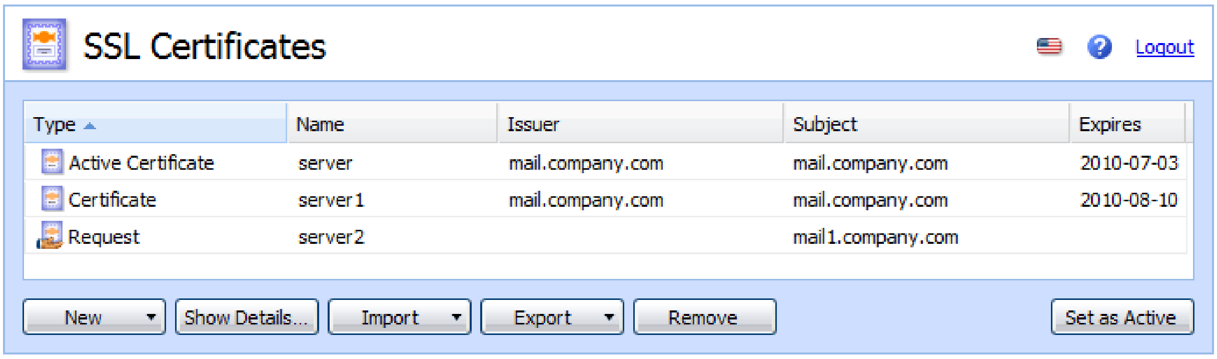
About SSL certificates

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**.



Type	Name	Issuer	Subject	Expires
Active Certificate	server	mail.company.com	mail.company.com	2010-07-03
Certificate	server1	mail.company.com	mail.company.com	2010-08-10
Request	server2		mail1.company.com	

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, it is necessary to add the certificates to Kerio Connect by using any of the following methods:

Locally on the computer where Kerio Connect is installed

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

Remotely via the administration interface

1. In a text editor, open the server certificate and the intermediate certificate.
2. Copy the intermediate certificate into the server certificate file and save.
   The file may look like this:

```
MIIDOjCCAqOgAwIBAgIDPmR/MA0GCSqGSIb3DQEBBAUAMFMxCzAJBgNVBAYTAl
MSUwIwYDVQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMR0wGwYDVQ
     ..... this is a server SSL certificate ...
```

```
ukrkDt4cgQxE6JSEprDiP+nShuh9uk4aUCKMg/g3VgEMulkROzFl6zinDg5grz
QspOQTEYoqrc3H4Bwt8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDMzCCApygAwIBAgIEMAAAATANBgkqhkiG9w0BAQUFADCBxDELMAkGA1UEBh
WkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
     ..... this is an intermediate SSL certificate which
           signed the server certificate...
5BjLqgQRk82bFi1uoG9bNm+E6o3tiUEDywrgrVX60CjbW1+yOCdMaq7dlpszRB
t14EmBxKYw==
```

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.

Managing logs in Kerio Connect

What are Kerio Connect logs for

Logs are files where information about certain events (e.g. error and warning reports, debugging information) is recorded. Each item is represented by 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.

Configuring logs

Logs are available in the Kerio Connect administration interface in section **Logs**.

There are several types of logs (see the following chapter).

When you right-click in a log, 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. See also **Log Settings** option.

Highlighting

You can save 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

Apart from immediate savings, 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.

Physically, the logs are stored in the following default folders according to the operating system:

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

Information about log settings are recorded in the **Config** log.

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

Debug log monitors various kinds of information and is used for problem-solving.

It allows you to select which information it will display.

1. Right-click in the log window and click on **Messages**.
2. Check any option you wish to monitor and confirm.

> ⚠ Too much information could be confusing and slows Kerio Connect's performance. Usually, you only need to display information relating to a particular service or function.

If a special option is necessary, you will be advised to check it in individual articles regarding Kerio Connect.

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. They can, however, indicate certain (or possible) problems. The Warning log can help if for example a user is complaining that certain services are not working.

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 does not manage to 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 pertain to: service initiation (usually due to port conflicts), disk space allocation, antivirus check initialization, improper authentication of users, etc.

Spam log

The **Spam** log displays information about all spam emails stored (or marked) in Kerio Connect.

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 mobile devices

Managing mobile devices in Kerio Connect

Beginning May 1, 2013, the support of Exchange ActiveSync in Kerio Connect is available as an add-on. For detailed information, read the Exchange ActiveSync FAQs.

Each user can synchronize their Kerio Connect account with an unlimited number of mobile devices.

To see the list of supported devices, visit Kerio Connect's product page.

Unsupported devices

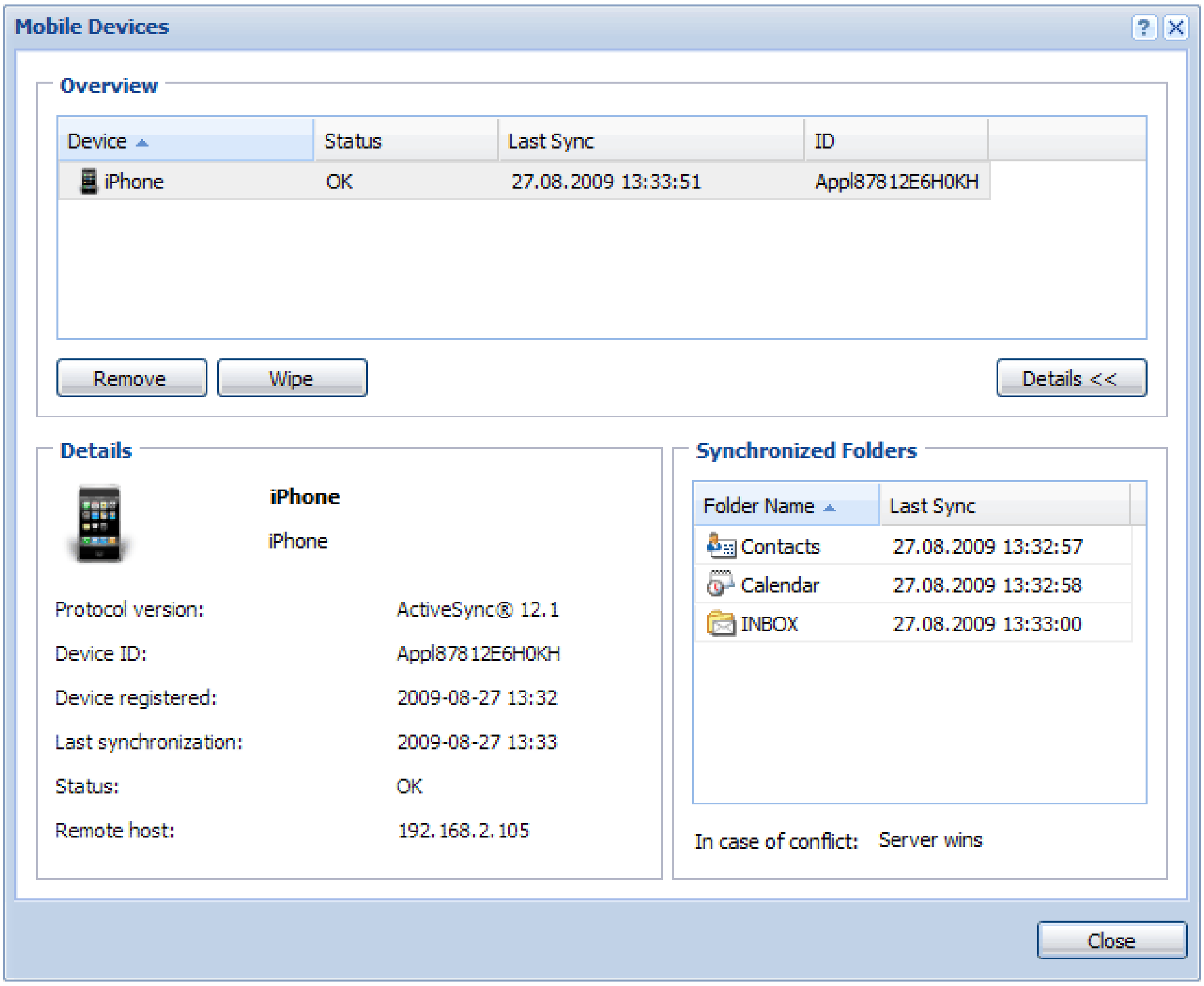
If you purchase the Exchange ActiveSync add-on, you can enable support for devices not listed as supported by Kerio Technologies.

Check option **Allow synchronization of unsupported Exchange ActiveSync devices** on tab **Miscellaneous** in section **Configuration** → **Advanced Options**.

Viewing users devices

Once a device is connected to Kerio Connect, administrators can view information about the device in the administration interface.

1. Go to the administration interface, to section **Accounts** → **Users**.
2. Select the user and click on **More Actions** → **Mobile Devices**.
3. This displays a list of devices. Select a device and
   - display details about the device.
   - click on **Remove** to delete unused devices from the list.
   - click on Wipe to delete data from the device



Overview

Device	Status	Last Sync	ID
iPhone	OK	27.08.2009 13:33:51	Appl87812E6H0KH

Details

iPhone

iPhone

Protocol version: ActiveSync® 12.1

Device ID: Appl87812E6H0KH

Device registered: 2009-08-27 13:32

Last synchronization: 2009-08-27 13:33

Status: OK

Remote host: 192.168.2.105

Synchronized Folders

Folder Name	Last Sync
Contacts	27.08.2009 13:32:57
Calendar	27.08.2009 13:32:58
INBOX	27.08.2009 13:33:00

In case of conflict: Server wins

Figure 1 Mobile devices of a user

Remotely deleting data from a device

The **Wipe** feature allows the Kerio Connect administrator to remove content of synchronized folders or even of the whole mobile device (so called hard reset) by a single click.

This feature may be helpful when the device gets lost or stolen. In addition to data clear-out, this action also disables further connections of the device to Kerio Connect (using the original user login data).

The wipe-out process will be completed the next time the device connects Kerio Connect. Users who have lost their devices should be informed that they should not run the synchronization if they find it and they should contact the administrators and ask them to cancel the wipe-out before the device is used again (the **Cancel Wipe** in user's devices).

Since the device types and operating systems are different, it depends on these conditions whether it is possible to reset the device completely or only to clear out synchronized folders.

It is not possible to use this feature to perform remote memory cards wipes. Memory cards usually store email attachments. ActiveSync supports wipe-out of any synchronized data, including the attachments. This means that the wipe removes all data on the device as well as any attachments, including those which are stored on the memory card.

Details of the wipe process are recorded in the Security log.

User confirmation of the wipe action

On Windows Mobile operating systems, users must agree that the administrator performs the wipe action. Therefore, a dialog appears which must be confirmed by the user during the first data synchronization between the device and Kerio Connect. If not confirmed, it is not possible to complete the synchronization process. This measure is applied for security reasons.

Support for BlackBerry devices in Kerio Connect

Synchronizing Kerio Connect with BlackBerry devices

⚠ From Kerio Connect 8.1, Kerio Connector for BlackBerry has been discontinued.

To synchronize BlackBerry devices with Kerio Connect, you can use:

- NotifySync — you can synchronize messages, calendars, contacts and tasks. For more info, visit the Notify Technology website.

- AstraSync — you can synchronize messages, calendars and contacts. For more info, visit the AstraSync website.

- Kerio Connector for BlackBerry

Switching between Kerio Connect client and old WebMail

Setting a default user interface

Kerio Connect offers two user interfaces — the new Kerio Connect client and old WebMail.

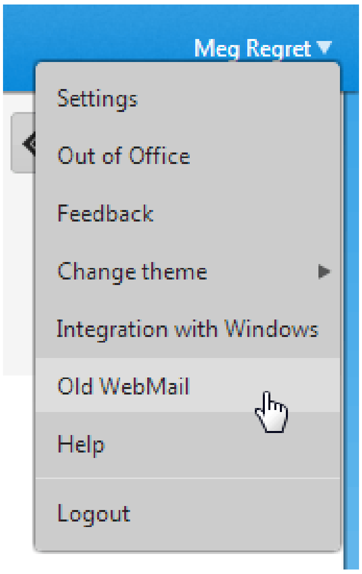
Administrators can select a default interface for their users. These settings apply to all domains within your Kerio Connect.

1. In the administration interface, go to section **Configuration** → **Advanced Options**.
2. Go to tab **Kerio Connect client / WebMail**.
3. From the **Default web client** drop-down menu, select one of the options.
    - Kerio Connect client
    - Old WebMail
    - Last used
4. Confirm the settings.

If user bookmarks, for example, Kerio Connect client and you switch the default client to old WebMail, user will be directed to Kerio Connect client when using their bookmark.

Switching from Kerio Connect client to old WebMail

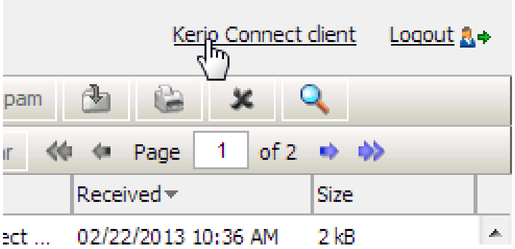
To switch from Kerio Connect client to the old WebMail interface, click your name in the top right corner and select Old WebMail



In Kerio Connect 8.0, the link to old WebMail is available in the top blue bar next to user's name.

Switching from old WebMail to Kerio Connect client

To switch from the old WebMail interface, click the **Kerio Connect client** link in the top bar of old WebMail.



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®, 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:

Apache Derby

Apache Derby is an open source relational database implemented entirely in Java.
Copyright © 2004-2009, The Apache Software Foundation
Copyright © 2004, 2005, IBM Corp.
Copyright © 1992-2003, Corel Corporation
Copyright © OSGi Alliance (2001, 2007). All Rights Reserved.
Copyright © 2002, 2003, Stefan Haustein, Oberhausen, Rhld., Germany.
Copyright © 2001-2002, Sun Microsystems.
Copyright © 2000 World Wide Web Consortium
Copyright © 1999-2002, Lotus Development Corporation.

Apache Lucene

Apache Lucene is a Java library for text searching.
Copyright © 1999-2009, The Apache Software Foundation
Copyright © 1995-2008 International Business Machines Corporation
Copyright © 2001, Dr Martin Porter
Copyright © 2002, 2003, 2004, 2005, Marc Prud'hommeaux
Copyright © 2002, Richard Boulton
Copyright © 2002-2003, Geir Landrö
Copyright © 2001-2004 Unicode, Inc.
Copyright © 2009 by www.imdict.net

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.
Copyright © 1987, 1993 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&nbsp;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.

excanvas

The ExplorerCanvas library allows 2D command-based drawing operations in Internet Explorer.

Copyright © 2006 Google Inc.

Kerio Connect Configuration Wizard for Linux

Kerio Connect Configuration Wizard for Linux is an application helping with initial configuration of Kerio Connect.

Copyright (c) Kerio Technologies, s.r.o

Kerio Connect Configuration Wizard for Linux is distributed under GNU General Public License, version 3.

To download the complete source code, please go to http://download.kerio.com/archive/

CppSQLite

A&nbsp;C++ wrapper around the SQLite embedded database library .

Copyright ©2004 Rob Groves. All Rights Reserved.

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*.

The modified source code is available at
http://download.kerio.com/archive/

Heimdal Kerberos

Heimdal Kerberos is used only in Linux-oriented Kerio Connect versions.

Heimdal is an implementation of Kerberos 5, largely written in Sweden. It is freely available under a three clause BSD style license (but note that the tar balls include parts of Eric Young’s libdes, which has a different license). Other free implementations include the one from MIT, and Shishi. Also Microsoft Windows and Sun’s Java come with implementations of Kerberos.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Copyright ©1995-1997 Eric Young. 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)

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

jabsorb

jabsorb is a simple and lightweight Ajax/Web 2.0 framework.
Copyright © 2007-2009 The jabsorb team

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.

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>

libiconv

Libiconv converts from one character encoding to another through Unicode conversion.
Copyright ©1999-2003 Free Software Foundation, Inc.
Author: Bruno Haible
Homepage: http://www.gnu.org/software/libiconv/
The *libiconv* library is distributed and licensed under GNU Lesser General Public License version 3.
Kerio Connect includes a&nbsp;customized version of this library. Complete source codes of the customized version of *libiconv* library are available at:

http://download.kerio.com/archive/

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/

libspf2

libspf2 implements the Sender Policy Framework, a&nbsp;part of the SPF/SRS protocol pair. libspf2 allows Sendmail, Postfix, Exim, Zmailer and MS Exchange check SPF records. It also verifies the SPF record and checks whether the sender server is authorized to send email from the domain used. This prevents email forgery, commonly used by spammers, scammers and email viruses/worms (for details, see http://www.libspf2.org/).
Copyright ©2004 Wayne Schlitt. All rights reserved.

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.

Copyright © 2001, 2002, 2004 Free Software Foundation, Inc.

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.

Mail-SpamAssassin

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

SpamAssassin is trademark of Apache Software Foundation.

myspell

Spellcheck library.

Copyright 2002 Kevin B. Hendricks, Stratford, Ontario, Canada And Contributors. All rights reserved.

OpenLDAP

Freely distributable *LDAP* (*Lightweight Directory Access Protocol*) implementation.

Copyright © 1998-2007 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/

sdbm

This product includes software developed by the Apache Software Foundation (http://www.apache.org/)

ScoopyNG

This product includes software developed by Tobias Klein.

Copyright ©2008, Tobias Klein. All rights reserved.

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.