

# **Kerio Connect**

## **Administrator's Guide**



# Contents

---

- Installing Kerio Connect** ..... 17
  - Product editions ..... 17
  - Windows ..... 17
  - Mac OS X ..... 18
  - Linux — RPM ..... 18
  - Linux — DEB ..... 20
  
- Performing initial configuration in Kerio Connect** ..... 22
  - About initial configuration ..... 22
  - Configuration files ..... 22
  - Configuring initial parameters ..... 23
  
- Registering Kerio Connect** ..... 29
  - Why register Kerio Connect? ..... 29
  - Registering Kerio Connect from the initial configuration wizard ..... 29
    - Registering a full version ..... 30
    - Registering a trial version ..... 32
    - Using an unregistered trial version ..... 33
  - Registering Kerio Connect in the administration interface ..... 33
    - Registering trial versions ..... 33
    - Registering a full version ..... 34
  
- Licenses in Kerio Connect** ..... 36
  - Overview ..... 36
  - Checking the number of users in your license ..... 37
  - Optional components ..... 38
  - Installing Kerio Connect licenses ..... 39
  - Updating licenses ..... 39
  
- Gathering usage statistics** ..... 40
  - Gathering information ..... 40
  - Enabling data gathering ..... 40
  
- Upgrading Kerio Connect** ..... 44
  - Overview ..... 44
  - Checking for updates ..... 44
  - Upgrading Kerio Connect server ..... 46
    - Upgrading the server remotely from the administration interface ... 46
    - Upgrading Kerio Connect manually ..... 47

---

Upgrading Kerio Outlook Connector .....	48
Troubleshooting .....	49
<b>Uninstalling Kerio Connect .....</b>	<b>50</b>
How to uninstall Kerio Connect .....	50
Windows operating system .....	50
Mac OS X operating system .....	50
Linux operating system — RPM .....	50
Linux operating system — DEB .....	50
<b>Kerio Connect VMware Virtual Appliance .....</b>	<b>52</b>
What is Kerio Connect VMware Virtual Appliance for .....	52
How to get Kerio Connect VMware Virtual Appliance .....	52
How to work with Kerio Connect VMware Virtual Appliance .....	52
Network configuration .....	53
Time zone settings .....	54
How to update Kerio Connect .....	54
<b>Adding a new disk to a virtual appliance .....</b>	<b>55</b>
Adding a new disk .....	55
Moving the existing message store to a new hard drive .....	56
<b>Switching from a 32-bit installation of Kerio Connect to 64-bit .....</b>	<b>57</b>
Overview .....	57
Microsoft Windows .....	57
64-bit Windows .....	57
32-bit Windows .....	62
Linux .....	64
64-bit Linux .....	64
32-bit Linux .....	65
Virtual appliances .....	65
<b>Accessing Kerio Connect .....</b>	<b>67</b>
What interfaces are available in Kerio Connect .....	67
Kerio Connect Client .....	67
Kerio Connect administration .....	67
How to log out .....	67
Automatic logout .....	67
<b>Accessing Kerio Connect administration .....</b>	<b>69</b>
Logging into the Kerio Connect administration .....	69
Accessing the administration interface remotely .....	70
Administrator accounts and access rights .....	71
Automatic logout .....	71
<b>Using Dashboard in Kerio Connect .....</b>	<b>73</b>

---

Dashboard overview .....	73
<b>Navigating through the Kerio Connect administration interface .....</b>	<b>75</b>
Overview .....	75
Searching for specific sections in the administration interface .....	75
<b>Domains in Kerio Connect .....</b>	<b>77</b>
Overview .....	77
Internet hostname .....	78
Primary domain .....	79
Adding new domains .....	80
<b>Creating domains in Kerio Connect .....</b>	<b>81</b>
Adding domains in Kerio Connect .....	81
Limiting the number of users per domain .....	81
Limiting the disk space per domain .....	82
Enabling message encryption with a DKIM signature .....	83
Enabling chat in Kerio Connect Client .....	83
Limiting message size and setting item clean-out to save space .....	83
Creating domain aliases .....	83
Forwarding messages to another server .....	83
Customizing Kerio Connect .....	84
Mapping users from a directory server .....	84
Archiving messages for individual domains .....	84
Additional configuration options .....	85
Deleting domains .....	85
<b>Connecting Kerio Connect to directory service .....</b>	<b>86</b>
Overview .....	86
Supported directory services .....	86
Microsoft Active Directory .....	86
Apple Open Directory .....	88
Kerberos authentication .....	89
Mapping users from directory services .....	90
Migrating user accounts from local database to directory service .....	90
Troubleshooting .....	91
<b>Migrating user accounts from local database to directory service .....</b>	<b>92</b>
Overview .....	92
Migrating users .....	92
Troubleshooting .....	93

---

<b>Authenticating users through PAM</b> .....	<b>94</b>
Overview .....	94
Configuring PAM authentication .....	94
<b>Renaming domains in Kerio Connect</b> .....	<b>95</b>
Overview .....	95
Prerequisites .....	95
Renaming domains .....	95
Post-renaming issues .....	96
<b>Distributed domains in Kerio Connect</b> .....	<b>97</b>
Distributed domains .....	97
<b>Creating user accounts in Kerio Connect</b> .....	<b>98</b>
Overview .....	98
Creating user accounts .....	98
Creating local accounts .....	99
Mapping accounts from a directory service .....	100
Templates .....	101
Disabling and deleting user accounts .....	101
Disabling users temporarily .....	101
Deleting users permanently .....	101
Troubleshooting .....	102
<b>Adding company and user contact information in Kerio Connect</b> .....	<b>103</b>
Overview .....	103
Setting company locations .....	103
Adding contact details to users .....	104
<b>Creating user groups in Kerio Connect</b> .....	<b>106</b>
About user groups .....	106
Creating user groups .....	107
Mapping groups from a directory service .....	108
Exporting group members .....	108
<b>Setting access rights in Kerio Connect</b> .....	<b>110</b>
Overview .....	110
Administrator accounts and access rights .....	110
Enabling the built-in administrator account .....	110
Assigning admin rights to individual users .....	111
Types of admin access rights .....	111
Assigning admin access rights .....	112

---

<b>Maintaining user accounts in Kerio Connect</b>	<b>113</b>
Overview	113
Deleting old items in users' mailboxes automatically	113
Recovering deleted items	115
Enabling deleted items recovery	115
Recovering deleted items	115
Limiting the size of outgoing messages	116
Per domain	117
Per user	117
From Kerio Connect Client	118
Limiting the size of incoming messages delivered via SMTP	118
Limit the size of user mailboxes	119
Notifying users about reaching their quotas	119
<b>Creating mailing lists in Kerio Connect</b>	<b>121</b>
Overview	121
Special mailing list addresses	121
Creating mailing lists	122
Accessing the mailing list archive	123
Troubleshooting	123
<b>Importing users in Kerio Connect</b>	<b>124</b>
Import options	124
Importing from CSV files	124
Creating CSV files	124
Importing from CSV files	125
Importing from a directory service	125
Windows NT domain	125
Microsoft Active Directory	125
Novell eDirectory	126
Troubleshooting	126
<b>Exporting users in Kerio Connect</b>	<b>127</b>
What can be exported	127
Exporting users from a domain	127
Exporting users from a group	127
Exporting users from a mailing list	128
<b>Creating aliases in Kerio Connect</b>	<b>129</b>
Aliases in Kerio Connect	129
Domain aliases	129
Username aliases	130

---

<b>Configuring resources in Kerio Connect</b>	<b>134</b>
Overview	134
Creating new resources	134
Assigning reservation managers	135
Removing resources	136
Using resources	136
Troubleshooting	136
<b>Monitoring Kerio Connect</b>	<b>137</b>
Overview	137
Monitoring incoming and outgoing messages	137
Viewing the message status	137
Processing message queue	138
Configuring message queue parameters	138
Traffic charts	139
Viewing statistics	139
Displaying users currently connected to Kerio Connect	140
Monitoring CPU and RAM usage	141
<b>Services in Kerio Connect</b>	<b>142</b>
Setting service parameters	142
Service types	143
SMTP	143
POP3	144
IMAP	144
NNTP	144
LDAP	144
HTTP	144
Instant Messaging	145
Restricting access to some services	145
Defining access policies	145
Assigning access policies to users	146
Troubleshooting	146
<b>Configuring the SMTP server</b>	<b>148</b>
Overview	148
Configuring the SMTP server	148
Sending outgoing messages through multiple servers	149
Securing the SMTP server	152
Troubleshooting	152



---

<b>Securing the SMTP server</b> .....	<b>153</b>
Overview .....	153
Securing the SMTP server .....	153
Troubleshooting .....	154
<b>Configuring POP3 connection</b> .....	<b>155</b>
About POP3 .....	155
Defining remote mailboxes .....	155
Sorting rules .....	158
<b>Receiving email via ETRN</b> .....	<b>160</b>
About ETRN .....	160
Configuring the ETRN account .....	160
Forwarding email .....	161
<b>Scheduling email delivery</b> .....	<b>163</b>
About scheduling .....	163
Configuring scheduling .....	163
<b>Securing Kerio Connect</b> .....	<b>165</b>
Issues to address .....	165
Configuring your firewall .....	165
Password policy .....	166
Configuring a secure connection to Kerio Connect .....	166
Securing user authentication .....	166
Encrypting user communication .....	167
<b>Configuring anti-spoofing in Kerio Connect</b> .....	<b>168</b>
About anti-spoofing .....	168
Configuring anti-spoofing in Kerio Connect .....	168
Enabling anti-spoofing per domain .....	169
<b>Password policy in Kerio Connect</b> .....	<b>171</b>
About password policy .....	171
Creating strong user passwords .....	171
Requiring complex passwords (for local users) .....	172
Enabling password expiry (for local users) .....	173
Protecting against password guessing attacks .....	174
<b>Authenticating messages with DKIM</b> .....	<b>175</b>
About DKIM .....	175
Enabling DKIM in Kerio Connect .....	175

---

<b>Configuring DNS for DKIM</b>	<b>177</b>
Adding a DKIM record to your DNS	177
Acquiring DKIM public key in Kerio Connect	178
Creating a short DKIM public key	178
<b>Configuring spam control in Kerio Connect</b>	<b>182</b>
Antispam methods and tests in Kerio Connect	182
Setting the spam score	183
Monitoring the spam filter's functionality and efficiency	184
Spam filter statistics	184
Graphical overviews	185
Logs	185
Optimizing spam protection	186
<b>Kerio Anti-spam filter</b>	<b>187</b>
Overview	187
How Kerio Anti-spam works	187
What data is sent to Bitdefender	188
Calculating the Kerio Anti-spam score	189
Configuring Kerio Anti-spam	190
Troubleshooting	192
<b>Configuring greylisting</b>	<b>193</b>
Overview	193
How greylisting works	193
What data is sent to Kerio Technologies	193
Configuring greylisting	194
Troubleshooting	195
<b>Blocking messages from certain servers</b>	<b>196</b>
Automatically blocking or allowing messages from certain servers	196
Blocking messages from spam servers — Custom blacklists	197
Blocking messages from spam servers — Public databases	197
Allowing messages from trusted servers — Custom whitelists	198
<b>Configuring Caller ID and SPF in Kerio Connect</b>	<b>199</b>
Overview	199
Configuring Caller ID	199
Configuring SPF	200
<b>Creating custom rules for spam control in Kerio Connect</b>	<b>202</b>
Overview	202
Creating custom rules	202
Example for regular expressions	203
Defining actions for custom rules	204

---

<b>Bayesian self-learning in Kerio Connect</b>	<b>206</b>
Overview	206
Terminology	206
SpamAssassin	206
Bayesian filtering	206
Bayesian self-learning	207
<b>Antivirus protection in Kerio Connect</b>	<b>208</b>
Overview	208
Configuring Kerio Antivirus	208
Updating the antivirus database	209
Configuring the HTTP proxy server	210
External antivirus	210
Filtering message attachments	210
Troubleshooting	210
<b>Filtering message attachments in Kerio Connect</b>	<b>212</b>
Overview	212
Configuring the attachment filter	213
Creating custom attachment filter rules	213
Troubleshooting	214
<b>Using an external antivirus with Kerio products</b>	<b>215</b>
Antivirus SDK for Kerio products	215
<b>Configuring IP address groups</b>	<b>216</b>
Overview	216
Configuring IP address group	217
<b>Creating time ranges in Kerio Connect</b>	<b>219</b>
Overview	219
Creating time ranges	219
<b>Filtering messages on the server</b>	<b>221</b>
Overview	221
Creating incoming rules	222
Creating outgoing rules	225
Example 1 - Forwarding messages to public folders	228
Example 2 - Prohibiting sending messages to remote recipients for individual users	230
Example 3 - Sending a copy of a message to another email address	231
Example 4 - Rejecting messages with large attachments	232
Examples 5 - Sending an auto-reply message	233

---

<b>Public folders in Kerio Connect</b>	<b>235</b>
Overview	235
Assigning administrator rights to manage public folders	235
Global vs. domain public folders	236
Configuring public folders	236
Creating public folders in Kerio Connect Client	237
Viewing public folders	238
Global Address List	239
<b>How to change from individual public folders to global public folders and keep your existing public folder data</b>	<b>241</b>
Changing to global folders	241
<b>Enabling chat in Kerio Connect Client</b>	<b>242</b>
Overview	242
Enabling chat for individual domains	242
Archiving Kerio Connect Client chat messages	243
Using Kerio Connect Client chat	243
Troubleshooting	244
<b>Configuring instant messaging in Kerio Connect</b>	<b>246</b>
Overview	246
Sending messages outside of your domain	247
Securing instant messaging	247
Limiting access to instant messaging	248
Disabling instant messaging	248
Archiving instant messages	249
Automatic contact list	249
Configuring IM clients	250
Troubleshooting	250
<b>Configuring DNS for instant messaging</b>	<b>251</b>
About SRV records	251
Configuring DNS records for server to server communication	251
Configuring DNS records for client auto-configuration	252
<b>Archiving instant messaging</b>	<b>254</b>
Overview	254
Configuring instant messaging archiving	254
Accessing the instant messaging archives	255
<b>Customizing Kerio Connect</b>	<b>256</b>
About customization	256
Defining custom email footers	256
Adding automatic user and company details to domain footers	257

---

Adding a custom logo to Kerio Connect Client .....	259
Localizing the user interface .....	261
Kerio Connect Client 8.1 and later .....	261
Kerio Connect Client 8.0 .....	261
<b>Customizing the Kerio Connect Client login page .....</b>	<b>262</b>
Overview .....	262
Customizing the login page .....	262
<b>Translating Kerio Connect Client to a new language .....</b>	<b>266</b>
Translating Kerio Connect Client for web .....	266
Upgrading Kerio Connect .....	267
<b>Configuring data store in Kerio Connect .....</b>	<b>268</b>
Setting the path to the data store directory .....	268
Configuring the full text search .....	269
Setting the data store notification limits .....	271
<b>Archiving in Kerio Connect .....</b>	<b>272</b>
Overview .....	272
Configuring archiving .....	272
Archiving the whole server .....	272
Archiving individual domains .....	273
Assigning administrator rights to view archive folders .....	275
Viewing archive folders .....	276
<b>Configuring backup in Kerio Connect .....</b>	<b>277</b>
Overview .....	277
Types of backups .....	277
Configuring backups .....	278
Recovering data from backups .....	280
Data recovery examples .....	280
Troubleshooting .....	281
<b>Examples of data recovery in Kerio Connect .....</b>	<b>282</b>
Data recovery in Kerio Connect .....	282
Examples for Microsoft Windows .....	282
Full backup recovery .....	282
Recovering a single user's mailbox .....	283
Recovering a single folder of a user .....	283
Recovering public folders of a particular domain .....	284
Examples for Mac OS X .....	285
Full backup recovery .....	285
Recovery of a single user's mailbox .....	286
Recovery of a single folder of a user .....	286

---

Recovery of public folders of a particular domain .....	287
Examples for Linux .....	287
Full backup recovery .....	287
Recovery of a single user's mailbox .....	288
Recovery of a single folder of a user .....	289
Recovery of public folders of a particular domain .....	289
<b>Data recovery in Kerio Connect .....</b>	<b>291</b>
Recovering data from backup .....	291
Advanced options of Kerio Connect Recover .....	292
Backup files .....	293
File names .....	293
File content .....	294
Data recovery examples .....	295
Troubleshooting .....	295
<b>Configuring SSL certificates in Kerio Connect .....</b>	<b>296</b>
Overview .....	296
Supported certificates .....	297
Multiple certificates .....	297
Creating certificates .....	298
Creating self-signed certificates .....	298
Creating certificates signed by certification authority .....	298
Intermediate certificates .....	298
<b>Configuring SSL/TLS in Kerio Connect .....</b>	<b>300</b>
Overview .....	300
Changing the SSL/TLS configuration .....	300
Resetting the SSL/TLS configuration .....	300
List of variables .....	301
<b>Adding trusted root certificates to the server .....</b>	<b>304</b>
Overview .....	304
Mac OS X .....	304
Windows .....	304
Linux (Ubuntu, Debian) .....	304
Linux (CentOs 6) .....	305
Linux (CentOs 5) .....	305
<b>Managing logs in Kerio Connect .....</b>	<b>306</b>
About Kerio Connect logs .....	306
Configuring logs .....	306
Types of logs .....	307
Config log .....	307
Debug log .....	307

---

Mail log .....	308
Security log .....	308
Warning log .....	308
Operations log .....	308
Error log .....	308
Spam log .....	308
Audit log .....	308
<b>Integrating Kerio Connect with Kerio Operator .....</b>	<b>310</b>
Overview .....	310
Configuring Kerio Connect .....	310
Configuring Kerio Operator .....	311
<b>Kerio Active Directory Extension .....</b>	<b>312</b>
How to use Kerio Active Directory Extension .....	312
How to install Kerio Active Directory Extension .....	312
How to create users and groups Kerio Connect in Active Directory .....	312
Troubleshooting .....	313
<b>Kerio Open Directory Extension .....</b>	<b>314</b>
How to use Kerio Open Directory Extension .....	314
How to install Kerio Open Directory Extension .....	314
Setting user account mapping in Kerio Connect .....	314
Troubleshooting .....	315
<b>Managing user mobile devices .....</b>	<b>316</b>
Managing mobile devices in Kerio Connect .....	316
Viewing users devices .....	316
Blocking specific types of devices .....	317
Remotely deleting data from users' device .....	318
<b>Setting a compatible Exchange ActiveSync version for specific mobile devices .....</b>	<b>320</b>
Overview .....	320
Editing the configuration file .....	320
<b>Changing the time zone definitions in timezones.xml file in Kerio Connect ...</b>	<b>323</b>
About time zones .....	323
Updating the timezones.xml file automatically .....	323
Updating the timezones.xml file manually .....	323
Editing the timezones.xml file .....	324
<b>Joining two servers with different domains into one server .....</b>	<b>326</b>
Details .....	326
Joining two Kerio Connect servers into one .....	327

---

<b>Providing feedback for Kerio products</b> .....	<b>329</b>
Giving feedback through Kerio Connect Client .....	329
<b>Kerio Connect — Legal notices</b> .....	<b>331</b>
Trademarks and registered trademarks .....	331
Used open source software .....	332



# Installing Kerio Connect

---

## Product editions

### Standard installation package

Kerio Connect is available as a standard installation package for:

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

### VMware Virtual Appliance

Virtual appliance for VMware products.

VMware Virtual Appliance is a software appliance edition pre-installed on a virtual host for VMware. The virtual appliance is distributed as OVF and VMX.

See [Kerio Connect VMware Virtual Appliance](#) for detailed information.

## Windows

For system requirements go to the [product pages](#).

1. Download the [Kerio Connect installation file](#).
2. Run the installation.

Kerio Connect must be installed under the user with administration rights to the system.

3. Follow the steps in the installation wizard.
4. Click **Finish** to complete the installation.



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

Kerio Connect engine starts (immediately or after restart) and runs as a service.

5. [Perform the initial configuration of Kerio Connect](#).

## Installing Kerio Connect

---

### Mac OS X

For system requirements go to the [product pages](#).

1. Download the [Kerio Connect installation file](#).
2. Run the installation.

Kerio Connect must be installed under the user with administration rights to the system.

3. Follow the steps in the installation wizard. Kerio Connect is installed in the `/usr/local/kerio/mailserver` folder.
4. Click **Finish** to complete the installation.

Kerio Connect engine starts upon the computer system startup and runs as a service.

5. [Perform the initial configuration of Kerio Connect](#).



Do not delete the Kerio Connect installation package. It includes [Kerio Connect Uninstaller](#).

### *Kerio Connect engine*

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

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

- **Stopping Kerio Connect engine:**

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

- **Running Kerio Connect engine:**

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

- **Restarting Kerio Connect engine:**

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

### Linux — RPM

For system requirements go to the [product pages](#).

1. Download the [Kerio Connect installation file](#).
2. Run the installation.

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

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

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

### ***New installation***

Start the installation using this command:

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

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

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

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

### ***Kerio Connect engine***

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

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

- **Stopping Kerio Connect engine:**  
`/etc/init.d/kerio-connect stop`
- **Running Kerio Connect engine:**  
`/etc/init.d/kerio-connect start`
- **Restarting Kerio Connect engine:**  
`/etc/init.d/kerio-connect restart`

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

- **Stopping Kerio Connect engine:**  
`systemctl stop kerio-connect.service`
- **Running Kerio Connect engine:**

## Installing Kerio Connect

---

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

### Linux — DEB

For system requirements go to the [product pages](#).

1. Download the [Kerio Connect installation file](#).
2. Run the installation.  
Kerio Connect must be installed under the user with root rights.
3. Follow the steps in the installation wizard. Kerio Connect is installed in the `/opt/kerio/mailserver` folder.
4. Click **Finish** to complete the installation.
5. [Perform the initial configuration of Kerio Connect](#).

### *New installation*

Start the installation using this command:

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

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

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

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

### *Kerio Connect engine*

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

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

- **Stopping Kerio Connect engine:**  

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

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

```
sudo service kerio-connect restart
```



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

# Performing initial configuration in Kerio Connect

---

## About initial configuration

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

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

- [Primary domain](#)
- [Administrator's account](#)
- [Data store](#)

The wizard creates special files where the [server configuration](#) is saved.

## Configuration files

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

### users.cfg

users.cfg is an XML file with the UTF-8 coding which includes information about [user accounts](#), [groups](#) and [aliases](#).

### mailserver.cfg

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

The default location of the configuration files is:

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



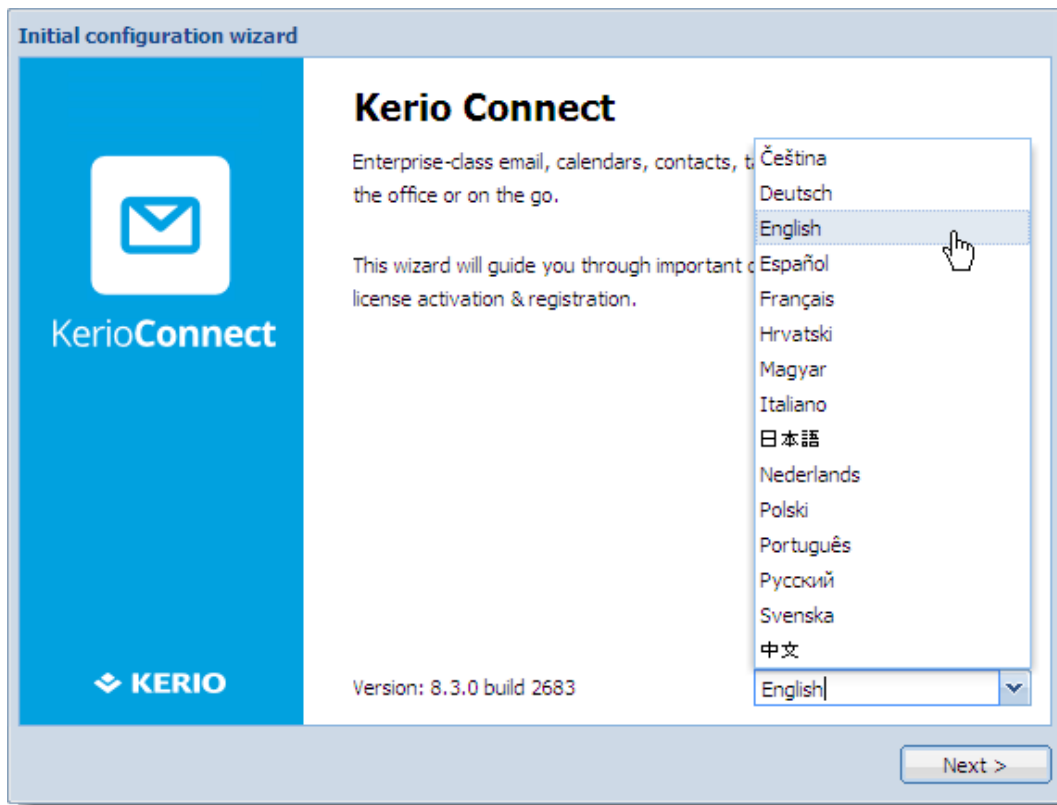
On Mac OS X and Linux systems, files can be maintained only if the user is logged in as the root user.

## Configuring initial parameters



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

1. [Install Kerio Connect](#).
2. Open the following address in your web browser:  
`https://kerio_connect_server:4040/admin`
3. Select a language for the initial configuration wizard and click **Next**.

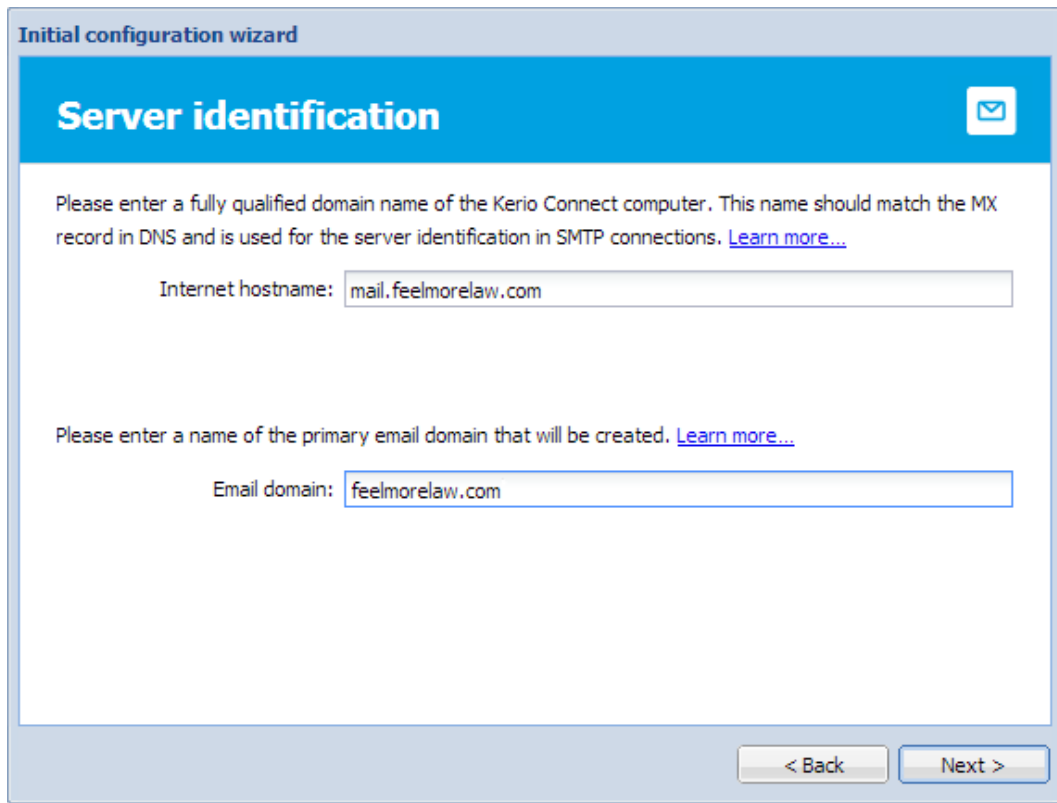


This language is also set as a default language after the first login to the administration interface.

4. Accept the **License Agreement** and click **Next**.
5. Type the **Internet hostname** and **Email domain**. Click **Next**.

## Performing initial configuration in Kerio Connect

---




The screenshot shows a window titled "Initial configuration wizard" with a blue header bar containing the text "Server identification" and an envelope icon. Below the header, there is instructional text: "Please enter a fully qualified domain name of the Kerio Connect computer. This name should match the MX record in DNS and is used for the server identification in SMTP connections. [Learn more...](#)". A text input field labeled "Internet hostname:" contains the text "mail.feelmorelaw.com". Below this, another instruction reads: "Please enter a name of the primary email domain that will be created. [Learn more...](#)". A second text input field labeled "Email domain:" contains the text "feelmorelaw.com". At the bottom right of the window, there are two buttons: "< Back" and "Next >".

For more information about domains, read the [Domains in Kerio Connect](#) article.


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



The screenshot shows a window titled "Initial configuration wizard" with a blue header bar containing the text "Administrator password" and a mail icon. Below the header, a message reads: "Please provide username and password for an account which will have full access to the administration." There are three input fields: "Username:" with the text "Admin", "Password:" with 12 black dots, and "Confirm password:" with 12 black dots. At the bottom left, an information icon is followed by the text: "The password cannot be empty and should be at least 8 characters long." At the bottom right, there are two buttons: "< Back" and "Next >".

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

7.

 New in Kerio Connect 9.2!

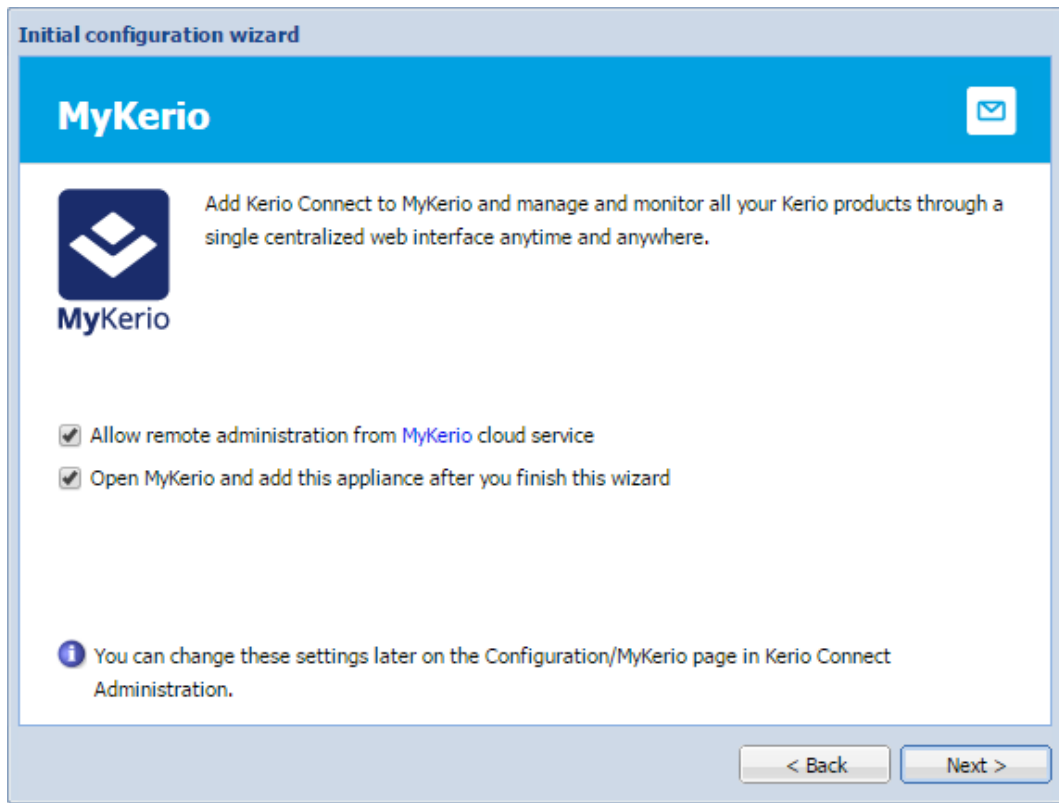
To manage your Kerio Connect from the [MyKerio cloud service](#), select **Allow remote administration from MyKerio** and click **Next**.

To go to MyKerio immediately after you finish the wizard, select **Open MyKerio and add this appliance...**

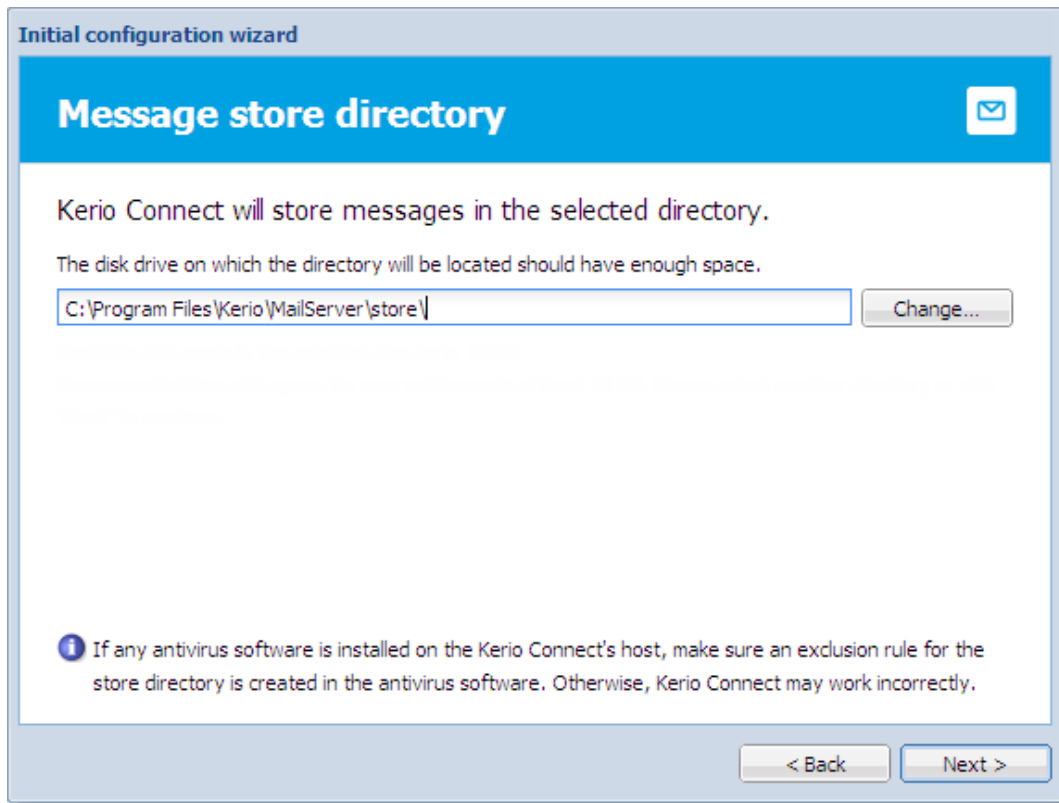
For more information about MyKerio, read [Adding Kerio Connect to MyKerio](#).

## Performing initial configuration in Kerio Connect

---



8. Set a directory for the message store and click **Next**.



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

For more information about the message store, read the [Configuring data store in Kerio Connect](#) article.



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

9. [Register the product or continue without the registration.](#) Click **Next**.

## Performing initial configuration in Kerio Connect

---

The screenshot shows a window titled "Initial configuration wizard" with a blue header bar containing the word "Licensing" and a mail icon. Below the header, the text "How do you plan to use Kerio Connect?" is displayed. There are two radio button options: "I will use a commercial or NFR license" with a "License" button, and "I want to try it free for 30 days" with a "Trial" button. At the bottom of the window, there are "< Back" and "Next >" buttons.

10. Finish the wizard.

When you finish the wizard, [log in to Kerio Connect administration](#) using the administrator username and password from the wizard or log in to [MyKerio](#).

# Registering Kerio Connect

---

## Why register Kerio Connect?

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

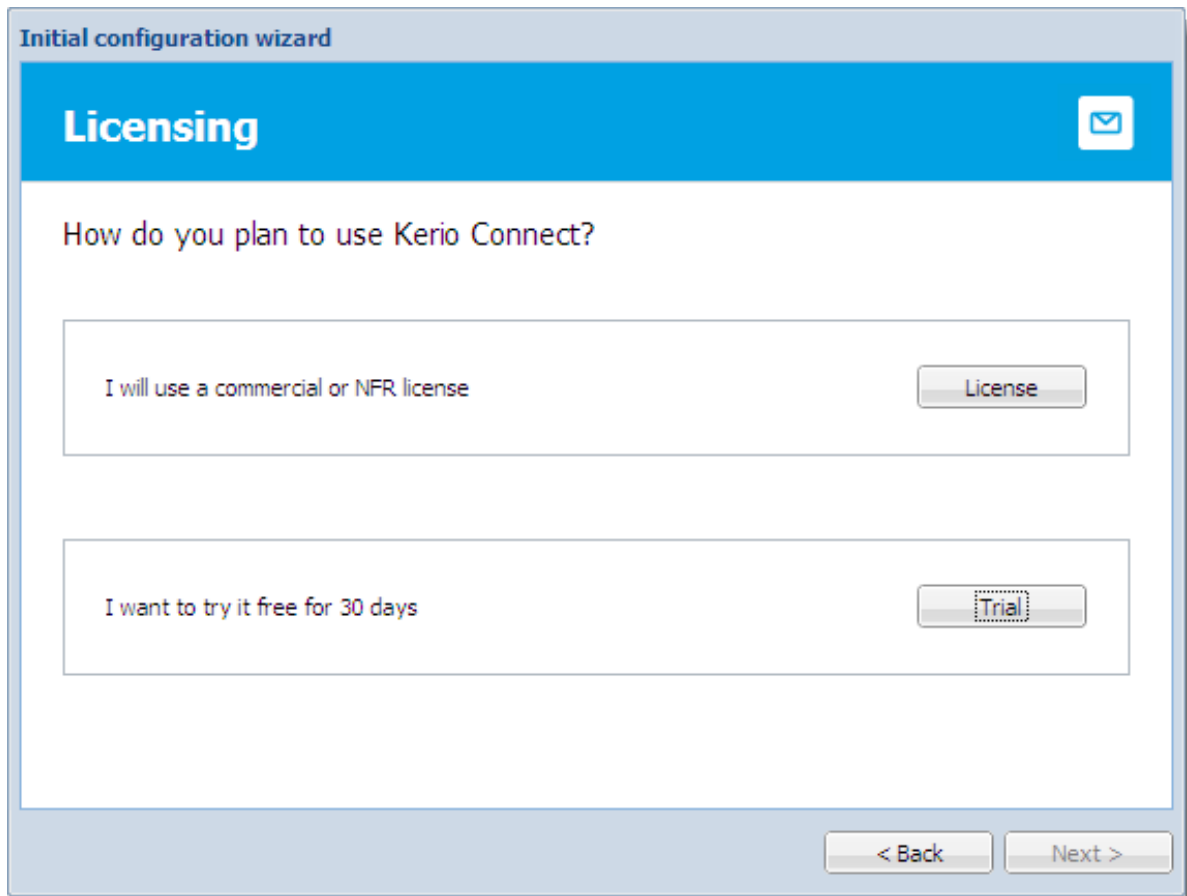
- Thirty days after installation, Kerio Connect Engine will be disabled.
- [Kerio Antivirus engine](#) cannot be updated for unregistered trial versions.
- Synchronization of mobile devices via Exchange ActiveSync is disabled.
- [Greylisting antispam protection](#) is not available.
- Technical support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

If you [register](#) a trial version, you will receive technical support during the entire trial period.

You can register Kerio Connect when you [run the initial configuration wizard](#) or in the administration interface.

## Registering Kerio Connect from the initial configuration wizard

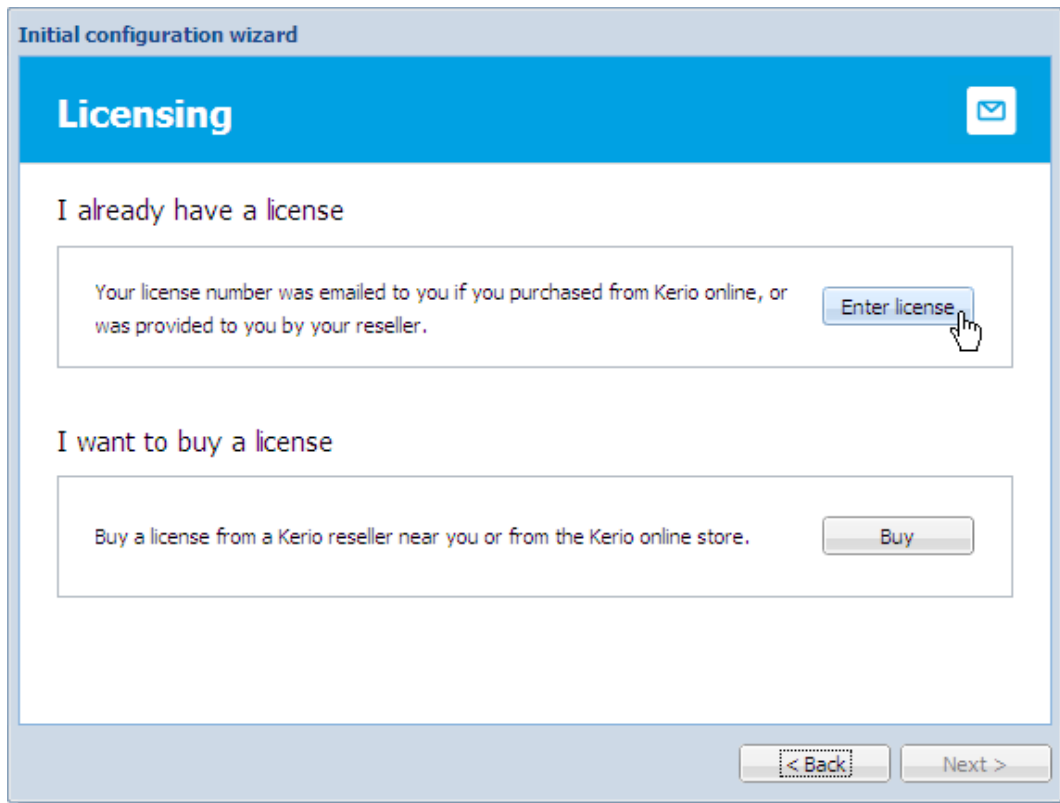
You can register Kerio Connect when you [run the initial configuration wizard](#).



### Registering a full version

1. On the **Licensing** tab of the configuration wizard, click the **License** button.
2. Prepare to type your license number:  
If you have a license number, click **Enter license**.  
If you don't have a license number, click the **Buy** button.

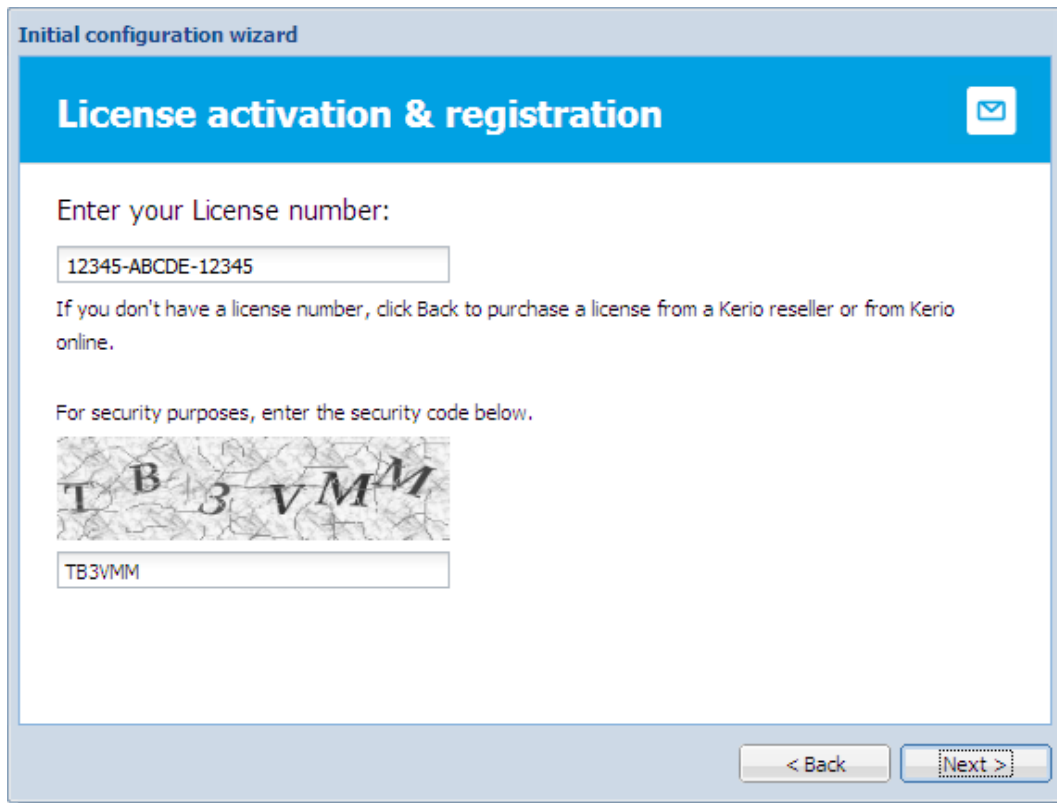
### 3.2 Registering Kerio Connect from the initial configuration wizard



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

## Registering Kerio Connect

---



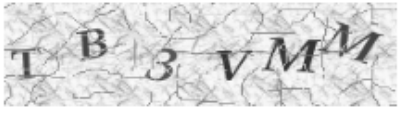
Initial configuration wizard

### License activation & registration

Enter your License number:

If you don't have a license number, click Back to purchase a license from a Kerio reseller or from Kerio online.

For security purposes, enter the security code below.



< Back    Next >

4. Decide if you want to grant Kerio Technologies permission to [gather usage statistics](#), and click **Next**.
5. Click **Finish** to close the wizard.

### Registering a trial version

1. On the **Licensing** tab of the initial configuration wizard, click the **Trial** button.
2. Type your trial license number and security code, and click **Next**.  
If you don't have a trial license number, click **Get a Trial License number**.



Initial configuration wizard

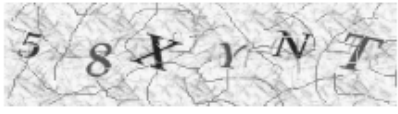
## Registered trial activation

Enter your Trial License number:

 [Get a Trial License number](#)

An email with your Trial License number has been sent to you when you requested the trial. Enter that here.

For security purposes, enter the security code below.



[Activate in unregistered mode](#)

< Back      Next >

3. Decide if you want to grant Kerio Technologies permission to [gather usage statistics](#), and click **Next**.
4. Click **Finish** to close the wizard.

#### Using an unregistered trial version

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

The limitations of the unregistered trial versions are described above, in the [Why register?](#) section.

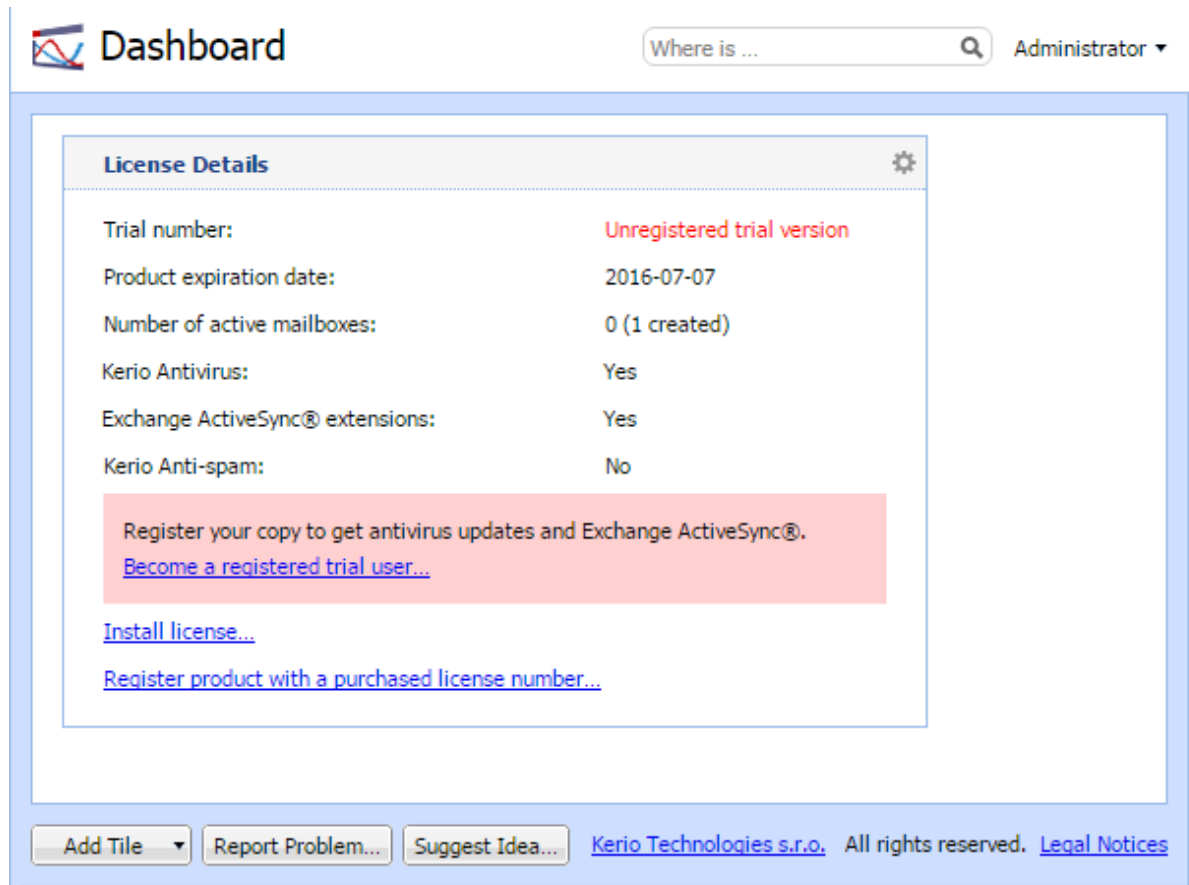
### Registering Kerio Connect in the administration interface

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



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

#### Registering trial versions



1. Log in to the administration interface and on the **Dashboard** click **Become a registered trial user**.
2. Type your trial license number and security code and click **Next**.  
If you don't have a trial license number, click **Get a Trial License number**.
3. Confirm.

### Registering a full version

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

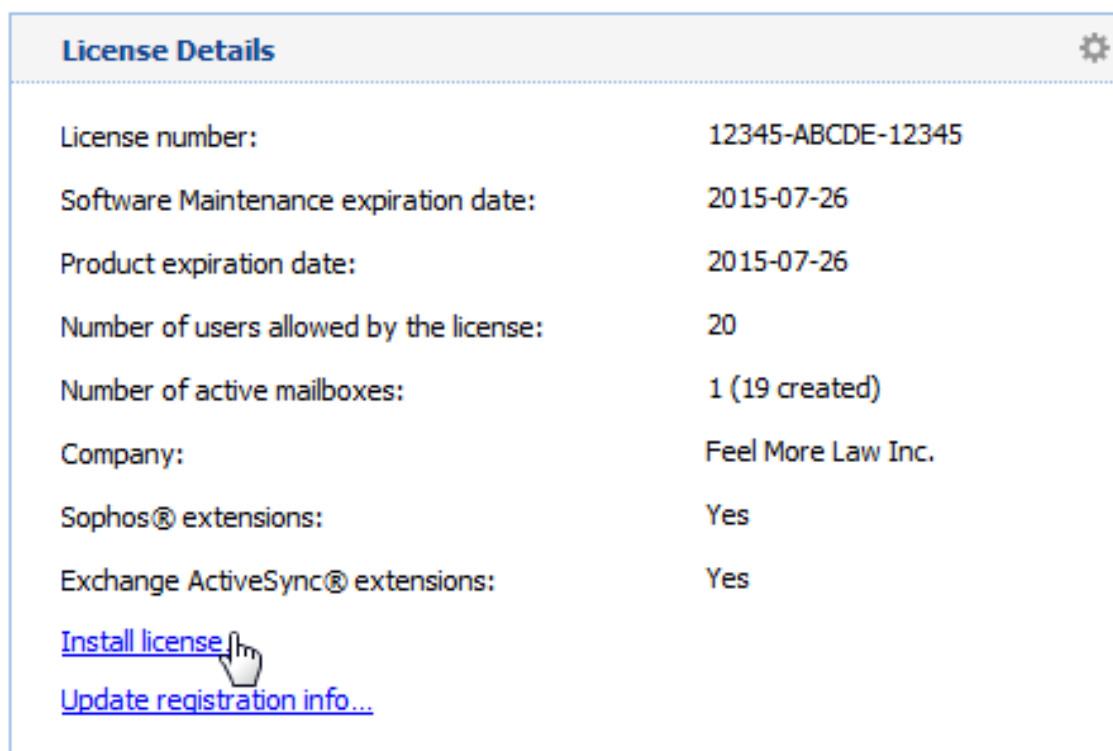
If you haven't registered your trial version:

1. In the Kerio Connect **Dashboard**, click **Register product with a purchased license number**.
2. Type the information required, including the license number you acquired on purchase.

3. Kerio Connect contacts the registration server, checks the validity of the data you entered, and automatically downloads the license file (digital certificate).
4. Click **Finish** to close the installation wizard.

#### *Installing your license manually*

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



License Details	
License number:	12345-ABCDE-12345
Software Maintenance expiration date:	2015-07-26
Product expiration date:	2015-07-26
Number of users allowed by the license:	20
Number of active mailboxes:	1 (19 created)
Company:	Feel More Law Inc.
Sophos® extensions:	Yes
Exchange ActiveSync® extensions:	Yes
<a href="#">Install license</a>	
<a href="#">Update registration info...</a>	

The default location of the license file varies by platform:

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

# Licenses in Kerio Connect

---

## Overview

Licenses are counted by number of users.

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

- [Created and enabled in Kerio Connect](#)
- [Mapped from a directory service](#)  
All users created in this database count as a licenses.
- [Imported from a domain](#)

The following don't count as licenses:

- [Disabled accounts](#)
- [Mailing lists](#)
- [Resources](#)
- [Aliases](#)
- [Domains](#)
- [Internal administrator account](#)

If you want to increase the number of users allowed by your license, visit the [Kerio Connect](#) website.

### ***Users mapped from a directory service***

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

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

## Checking the number of users in your license

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

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

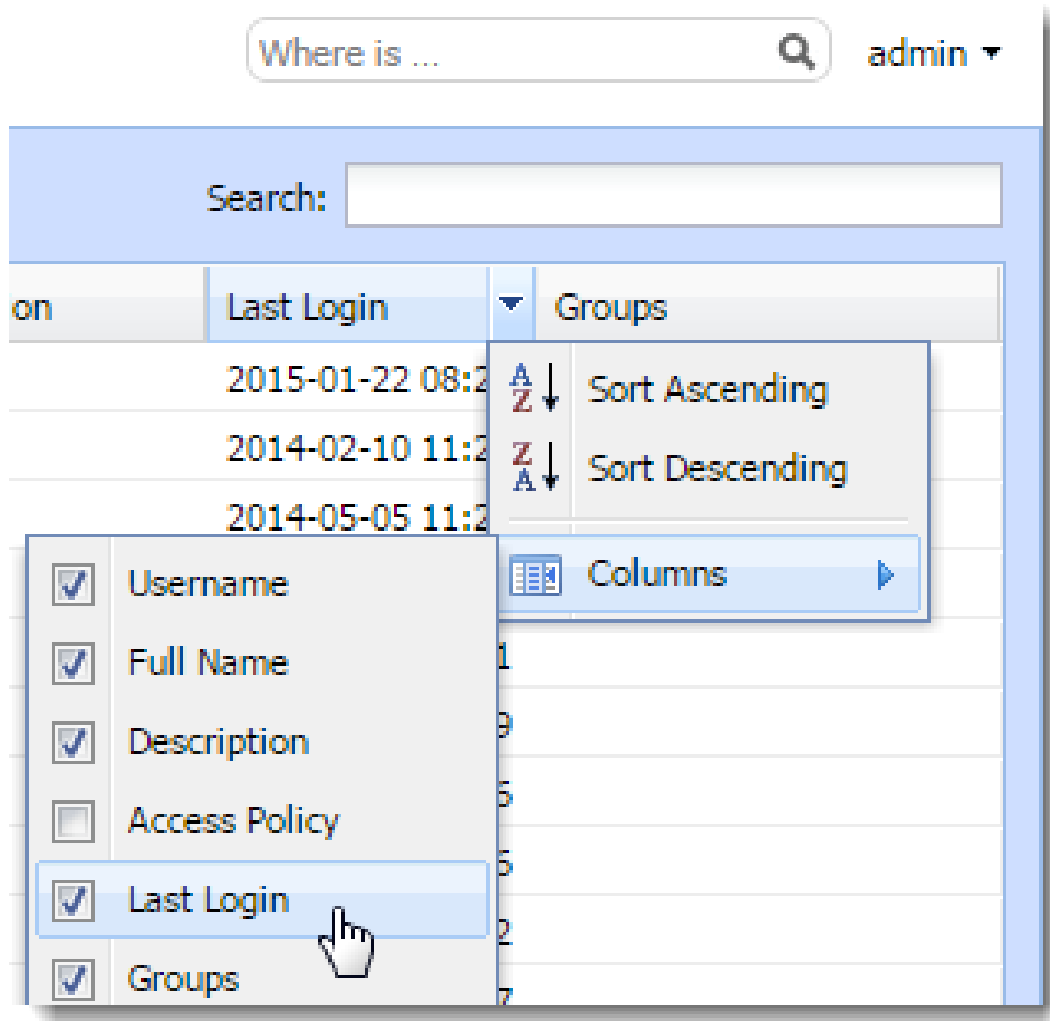
The screenshot shows the Kerio Connect Administration interface. At the top, there is a 'Dashboard' header with a search bar and a user profile 'R. Cul Powaro'. Below this is the 'License Details' tile, which contains the following information:

License number:	12345-12345-12345
Software Maintenance expiration date:	2014-07-26
Product expiration date:	2014-07-26
Number of users allowed by the license:	20
Number of active mailboxes:	12 (18 created)
Company:	Feel More Law Inc.
Sophos® extensions:	Yes
Exchange ActiveSync® extensions:	Yes

Below the table are two links: [Install license...](#) and [Update registration info...](#). Two callout boxes with arrows point to the 'Number of users active from the last server restart' and 'Number of users created and enabled' fields in the 'Number of active mailboxes' row.

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

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



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

Now you can [remove users](#) who do not use Kerio Connect.

### Optional components

Kerio Connect has the following optional components:

- [Kerio Antivirus](#)
- Exchange ActiveSync
- [Kerio Anti-spam](#)

These components are licensed individually. Visit the [product pages of Kerio Connect](#) for additional information.

### **Installing Kerio Connect licenses**

For information on registrations and license installations, read [Registering Kerio Connect](#).

### **Updating licenses**

If you, for example, purchase additional users or components, your license will be updated automatically within 24 hours.

# Gathering usage statistics

---

## Gathering information

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

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

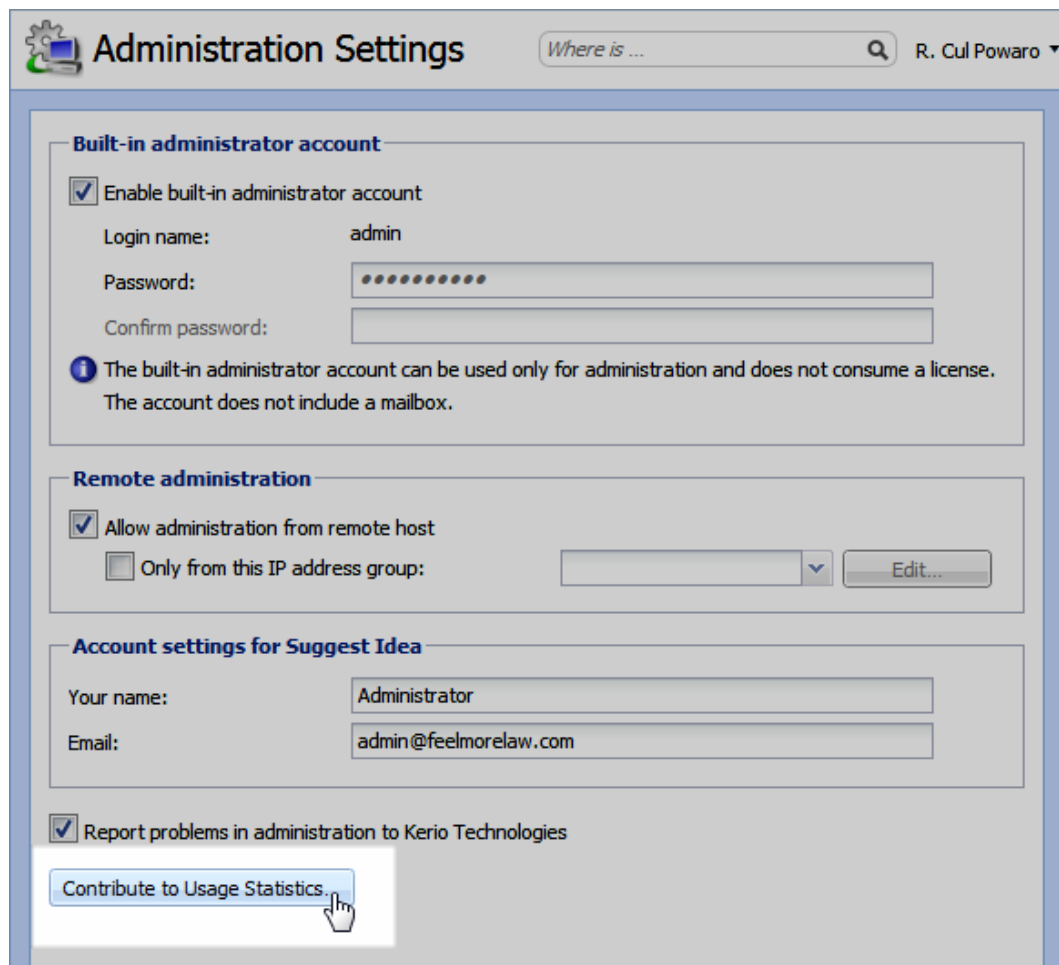
## Enabling data gathering

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

To change the settings later, follow these steps:

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





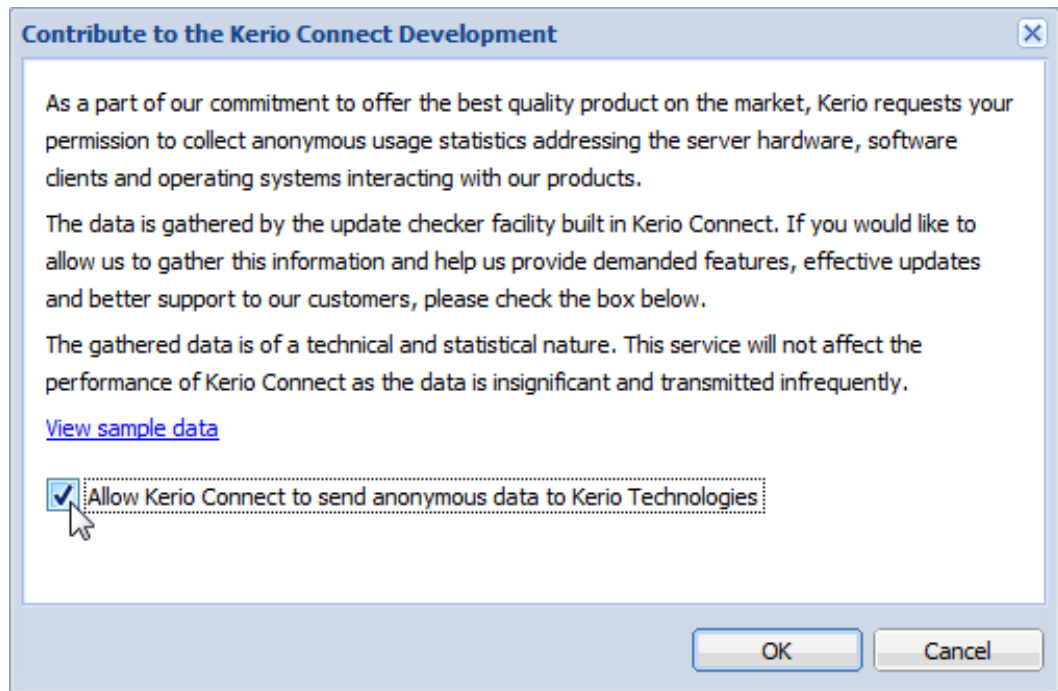
The screenshot shows the 'Administration Settings' window. The title bar includes a gear icon, the text 'Administration Settings', a search box with 'Where is ...', and a user name 'R. Cul Powaro'. The main content area is divided into several sections:

- Built-in administrator account:** This section has a checked checkbox for 'Enable built-in administrator account'. Below it, the 'Login name' is 'admin'. The 'Password' field contains ten dots, and the 'Confirm password' field is empty. An information icon (i) is followed by the text: '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:** This section has a checked checkbox for 'Allow administration from remote host'. Below it, there is an unchecked checkbox for 'Only from this IP address group:' followed by an empty text box, a dropdown arrow, and an 'Edit...' button.
- Account settings for Suggest Idea:** This section has two text input fields: 'Your name:' with the value 'Administrator' and 'Email:' with the value 'admin@feelmorrelaw.com'.
- At the bottom, there is a checked checkbox for 'Report problems in administration to Kerio Technologies' and a button labeled 'Contribute to Usage Statistics.' with a mouse cursor pointing to it.

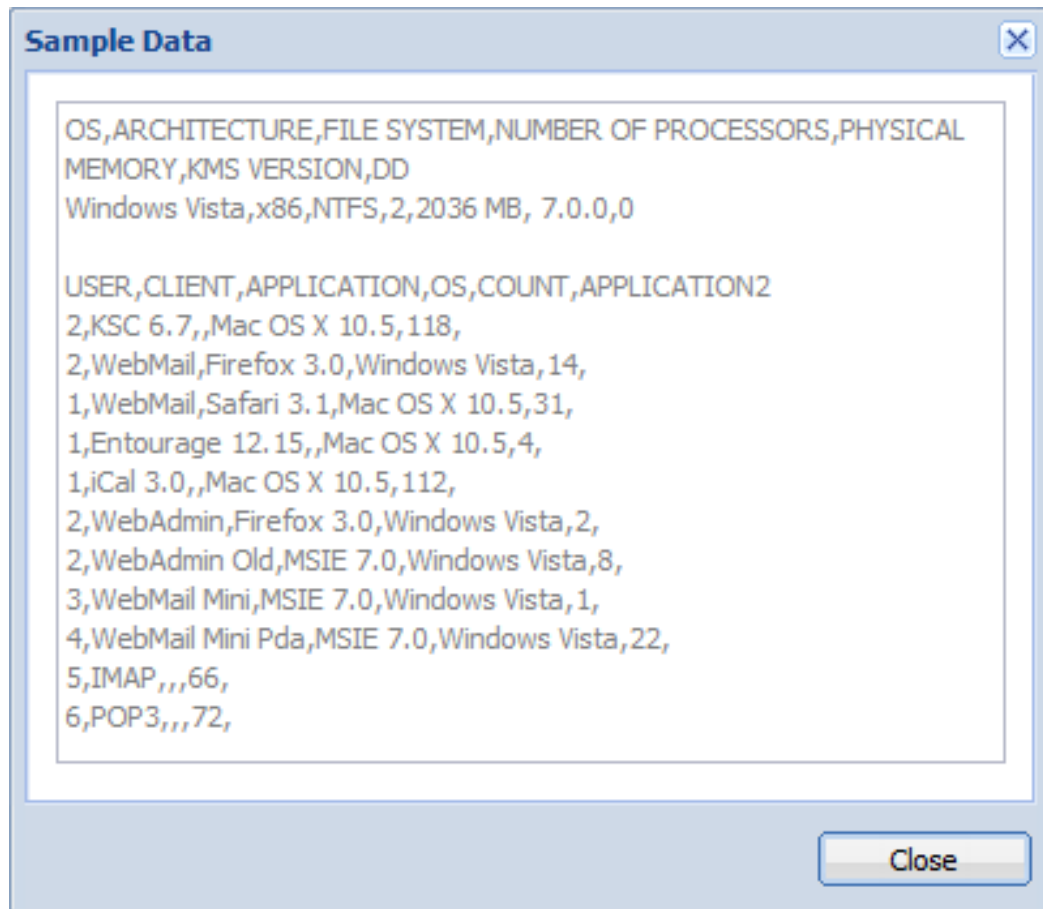
4. Check the **Allow Kerio Connect to send anonymous data to Kerio Technologies** option.

## Gathering usage statistics

---



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



6. Click **OK**.

# Upgrading Kerio Connect

---

## Overview

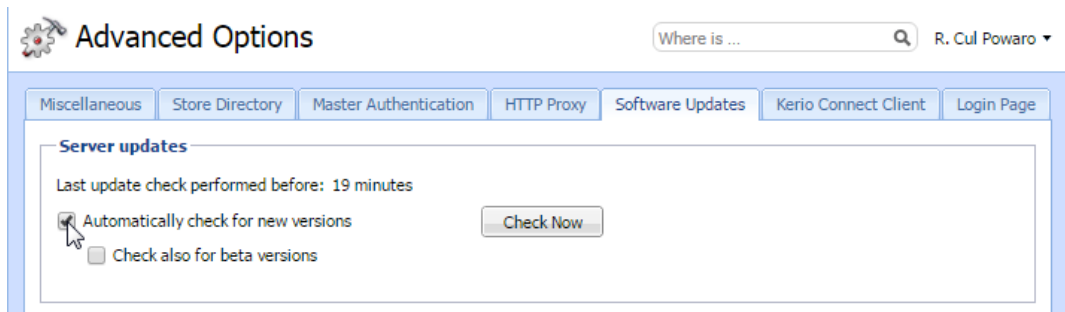
When you purchase Kerio Connect or extend your [Software Maintenance](#), you are eligible to receive new versions of Kerio Connect and its components as soon as they are available.

## Checking for updates

Kerio Connect can periodically check for new versions available:



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

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



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

If a new version is available, Kerio Connect displays a notification on the **Dashboard** and in the **Advanced Options** → **Server Updates** section.

 **Dashboard** Where is ...  R. Cul Powaro ▾

Kerio Connect 9.0.2 is available. Go to [Software Updates](#) to install the new version.

---

**System**

Version:	9.0.1 (394)
Operating system:	Ubuntu 15.10, x86_64
Hostname:	mail.feelmorelaw.com

---

**License Details**

License number:	12345-ABCDE-12345
Software Maintenance expiration date:	2017-12-09
Product expiration date:	2017-12-09
Number of users allowed by the license:	20
Number of active mailboxes:	2 (7 created)
Company:	Feel More law Inc.
Sophos® extensions:	Yes
Exchange ActiveSync® extensions:	Yes

[Install license...](#)  
[Update registration info...](#)


Add Tile ▾ Technical Support... Suggest Idea...
[Kerio Technologies s.r.o.](#) All rights reserved. [Legal Notices](#)

**Server updates**

Last update check performed before: 12 hours, 30 minutes

Automatically check for new versions

Check also for beta versions

 A new version is available for download: [Kerio Connect 9.0.2](#)

## Upgrading Kerio Connect

---

### *Configuring HTTP proxy server*

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

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

### Upgrading Kerio Connect server

You can upgrade your Kerio Connect:

- Remotely from the administration interface
- Manually on the server



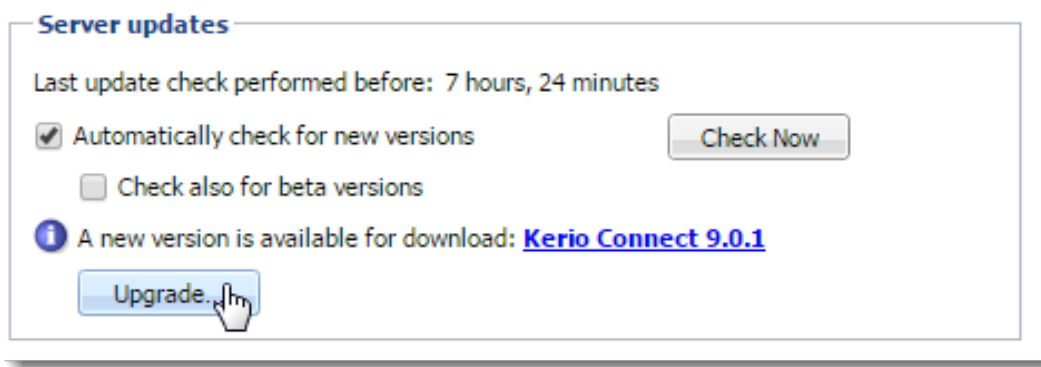
Kerio Connect saves a backup of the configuration files from the previous version in the installation folder in UpgradeBackups.

### Upgrading the server remotely from the administration interface



New in Kerio Connect 9!

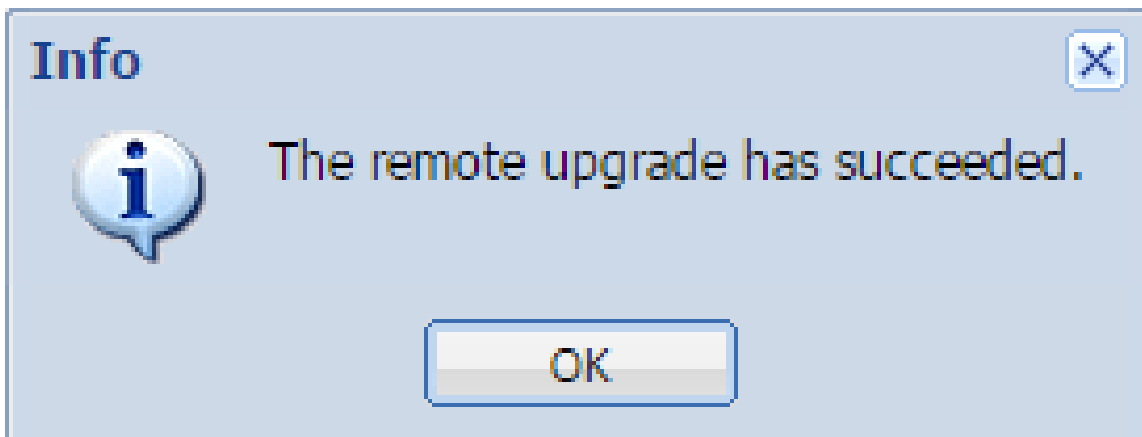
1. In the administration interface, go to the **Configuration** → **Advanced Options** section.  
You can upgrade from any device which can access the Kerio Connect administration interface.
2. Switch to the **Software Updates** tab.
3. Click **Upgrade** in the **Server Updates** section.



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

Kerio Connect starts downloading and upgrading your Kerio Connect server.

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



### Upgrading Kerio Connect manually

#### *Microsoft Windows*

To upgrade Kerio Connect on Microsoft Windows, download and run the installation package. The program detects the installation directory, stops all running components (Kerio Connect engine and Kerio Connect Monitor) and replaces existing files with new ones automatically.

## Upgrading Kerio Connect

---

### *Mac OS X*

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

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

### *Linux — RPM*

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

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

### *Linux — DEB*

To upgrade Kerio Connect on Linux Debian, use the same command as for [installation](#):

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

### *Kerio Connect VMware Virtual Appliance*

See the article [Kerio Connect VMware Virtual Appliance](#) for information on upgrading the appliance.

## Upgrading Kerio Outlook Connector

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

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





4. Click **Apply**.

## Troubleshooting

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

# Uninstalling Kerio Connect

---

## How to uninstall Kerio Connect

### Windows operating system

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



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

### Mac OS X operating system

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



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

### Linux operating system — RPM

Uninstall Kerio Connect using this command:

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



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

### Linux operating system — DEB

Uninstall Kerio Connect using this command:

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



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

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

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

# Kerio Connect VMware Virtual Appliance

---

## What is Kerio Connect VMware Virtual Appliance for

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

For supported VMware product versions, check the [product pages](#).

## How to get Kerio Connect VMware Virtual Appliance

Download the [Kerio Connect installation package](#) according to your VMware product type:

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

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



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

## How to work with Kerio Connect VMware Virtual Appliance

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

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

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

- DNS name of the server,
- data store.

This console provides several actions to be taken:

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



**Figure 1** Console — network configuration



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

### Network configuration

The network configuration allows you to:

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

## Kerio Connect VMware Virtual Appliance

---

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



If you use a DHCP service on your network, the server will be assigned an IP address automatically and will connect to the network. If you do not use or do not wish to use DHCP for Kerio Connect, you have to set the IP address manually.

If the IP address is assigned by the DHCP server, we recommend to reserve an IP address for Kerio Connect so that it will not change.

If you run Kerio Connect VMware Appliance in the local network, check that an IP address has been assigned by the DHCP server. If not, restart the appliance.

### Time zone settings

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

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

### How to update Kerio Connect



A terminal is available for product and operating system updates. You can switch it by pressing the standard **Alt+Fx** combination (for example, **Alt+F2**) for running a new console.

Before the first SSH connection to the terminal, it is necessary to enable the latter.

To update Kerio Connect:

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

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

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



To upgrade the console, go to the [Kerio Connect download page](#) and download the **Virtual Appliance Console Upgrade Package**.

# Adding a new disk to a virtual appliance

---

## Adding a new disk



Please run a backup first. Some of these commands are potentially destructive and may cause damage to your system if not carried out correctly.

If you want to increase the available disk space for your message store in a Debian virtual appliance, you can add a second virtual hard drive to the appliance.

1. Using your VM Hypervisor, add a new hard drive to your VM and start the appliance.
2. Log in to the system console.
3. Run this command to check if the Debian installed and recognized the new hard drive:

```
fdisk -l
```

If installed correctly, the hard drive is recognized at `/dev/sdb/` and has no partitions.

4. Create a new partition on the new hard drive.
5. In the `fdisk` controller, select **New** → **Primary** → **Size in MB**.
6. Select **Write** and **Quit**.

A new partition is created at `/dev/sdb/`.

7. Format the new disk:

```
mkfs.ext3 /dev/sdb1
```

This command formats the partition with the ext3 filesystem.

8. Mount the hard drive with these commands:

```
mkdir /store
```

to create a directory for the hard drive

```
mount -t ext3 /dev/sdb1 /store
```

to mount the hard drive to this directory.

The new hard drive is prepared.

## Adding a new disk to a virtual appliance

---

### *Adding the drive to the fstab file*

If you want the new hard drive to mount automatically when the server reboots, follow these steps:

1. Open the fstab file with this command:

```
vi /etc/fstab
```

2. Add the following line to the end of the file:

```
/dev/sdb1 /store ext3 defaults,errors=remount-ro 0 1
```

3. Save the file.

### **Moving the existing message store to a new hard drive**

If you want to move your Kerio Connect message store to a new drive, follow these steps:

1. Stop the Kerio Connect server with this command:

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

2. Copy all data from the old message store to the new hard drive:

```
cp -R -p /opt/kerio/mailserver/store/* /store
```

3. Change the message store directory path in the Kerio Connect configuration file:

```
sed -i -e "s/\/opt\/kerio\/mailserver\/store/\/store/"  
/opt/kerio/mailserver/mailserver.cfg
```

4. Start Kerio Connect.



# Switching from a 32-bit installation of Kerio Connect to 64-bit

---

## Overview

Use these links to find instructions for your operating systems:

- [Microsoft Windows](#)
- [Linux](#)
- [Virtual appliances](#)

## Microsoft Windows

The steps for switching from a 32-bit version of Kerio Connect to a 64-bit installation differ for [32-bit systems](#) and [64-bit systems](#).



Perform a [full backup](#) of Kerio Connect before proceeding.

## 64-bit Windows

On a 64-bit Windows system, you can:

- [Upgrade to a newer version of Kerio Connect](#) (for example, upgrade from the 32-bit version of Kerio Connect 8.5.3 to the 64-bit version of Kerio Connect 9.0.0)
- [Install the 64-bit version of the same Kerio Connect](#) (for example, switch from the 32-bit version of Kerio Connect 8.5.3 to the 64-bit version of Kerio Connect 8.5.3)

### *Upgrading to a newer version of Kerio Connect*

To upgrade your Kerio Connect, you can run the 64-bit installation file of a newer version of Kerio Connect. In that case, your message store and configuration files stay in the Program Files (x86) folder.

You can also uninstall the 32-bit version first and then install the 64-bit version of Kerio Connect. In that case, you move your message store and configuration files to the Program Files folder as described below.

1. Uninstall the 32-bit version of your Kerio Connect.

## Switching from a 32-bit installation of Kerio Connect to 64-bit

---

Kerio Connect created several files while it was running. These files can be removed during the uninstallation.

**Remove Message Store**

This option will remove message store including archive folder, backup folder, all user message folders and log files.

**Remove Configuration Files**

This option will remove all user specific configuration data, including licenses, configuration files and their backup made during the upgrades, SSL certificates, statistics and WebMail customizations.



**DO NOT** remove the configuration files and data store during the process.

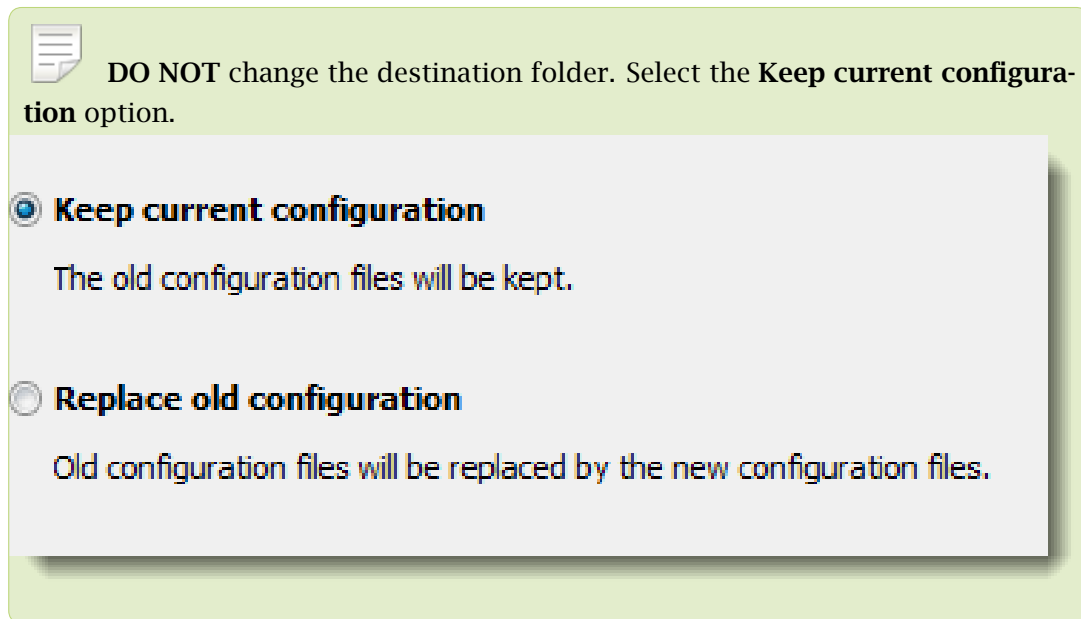
2. Move the **Kerio/MailServer** directory with the configuration files and the data store to the **Program Files** folder — the default installation folder for 64-bit programs.

## Switching from a 32-bit installation of Kerio Connect to 64-bit

---



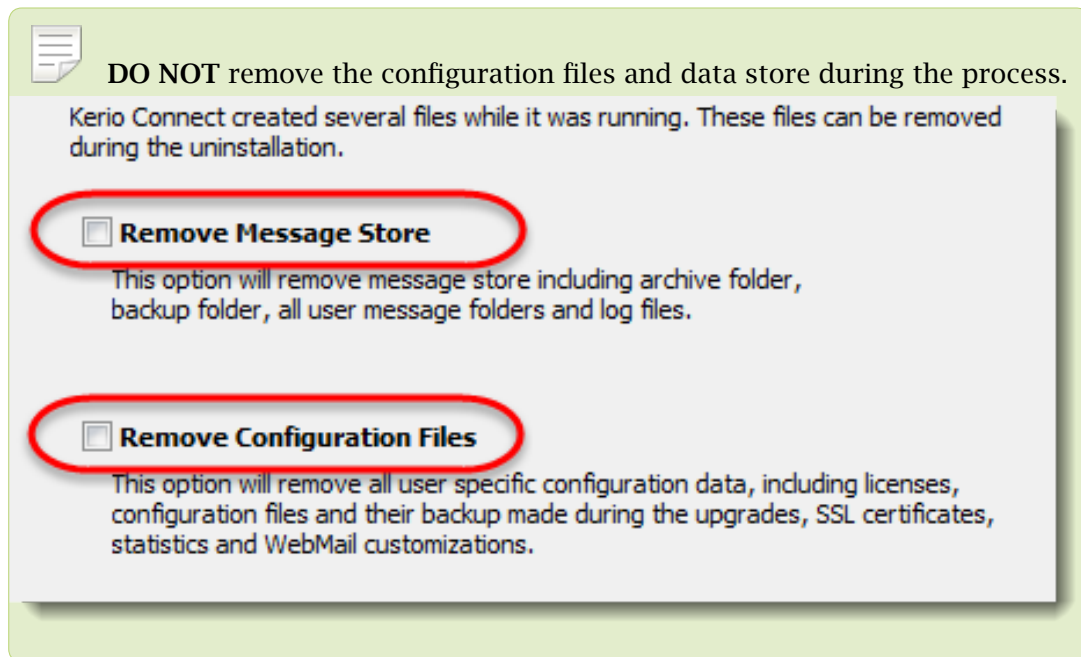
3. Open the **mailserver.cfg** file and change all paths from **C:\Program Files (x86)\** to **C:\Program Files\**.
4. Install the 64-bit version of a newer version of Kerio Connect.



A 64-bit version of a newer Kerio Connect is installed in the **Program Files** folder.

### ***Installing the 64-bit version of the same Kerio Connect***

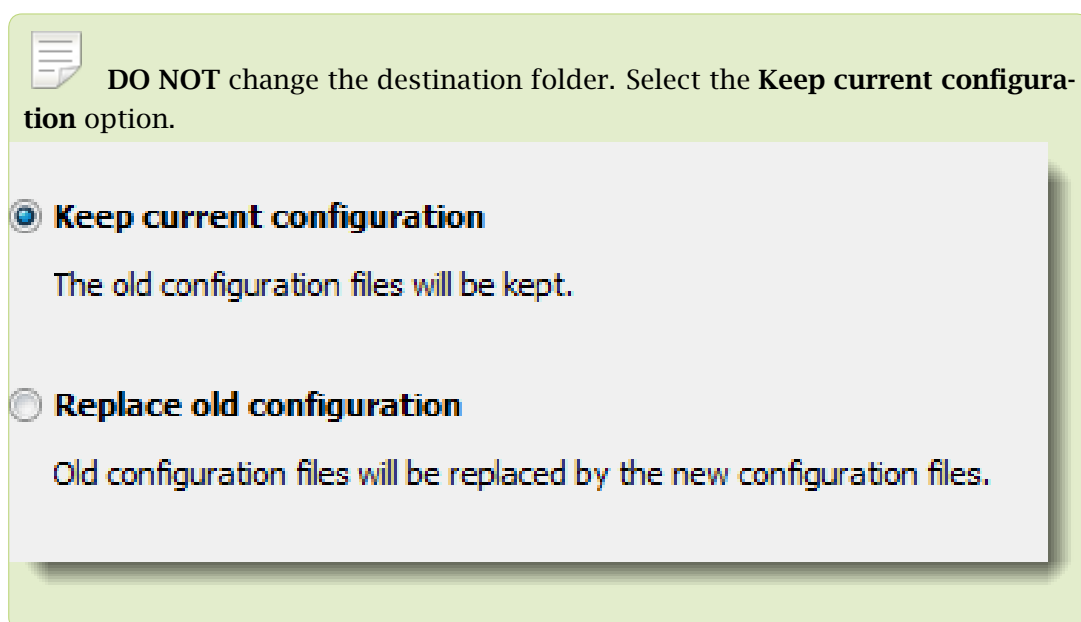
1. Uninstall the 32-bit version of your Kerio Connect.



2. Move the **Kerio/MailServer** directory with the configuration files and the data store to the **Program Files** folder — the default installation folder for 64-bit programs.

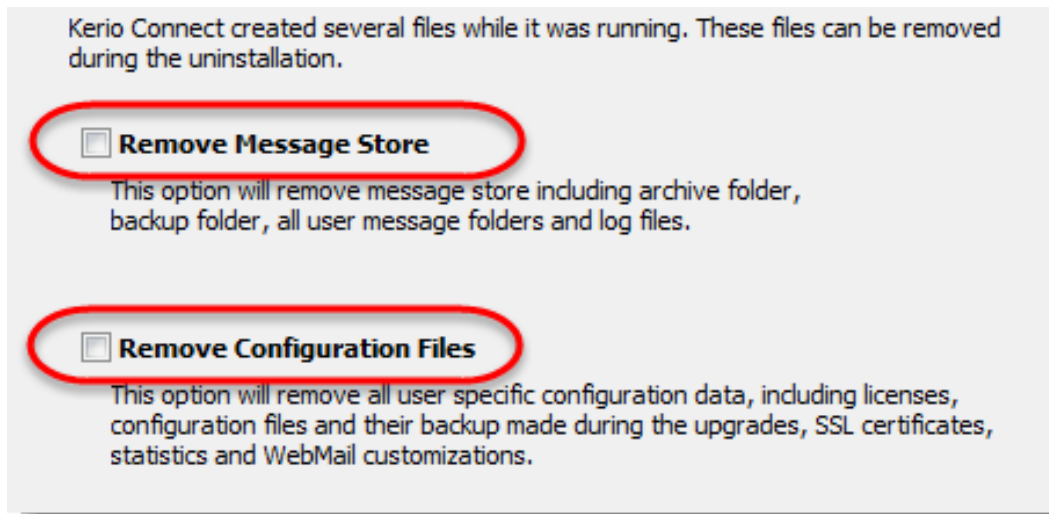


3. Open the **mailserver.cfg** file and change all paths from **C:\Program Files (x86)\** to **C:\Program Files\**.
4. Install the 64-bit version of the same Kerio Connect.



## Switching from a 32-bit installation of Kerio Connect to 64-bit

---



A 64-bit version of the same Kerio Connect is installed in the **Program Files** folder.

### 32-bit Windows

1. Uninstall the 32-bit version of your Kerio Connect.



**DO NOT** remove the configuration files and data store during the process.

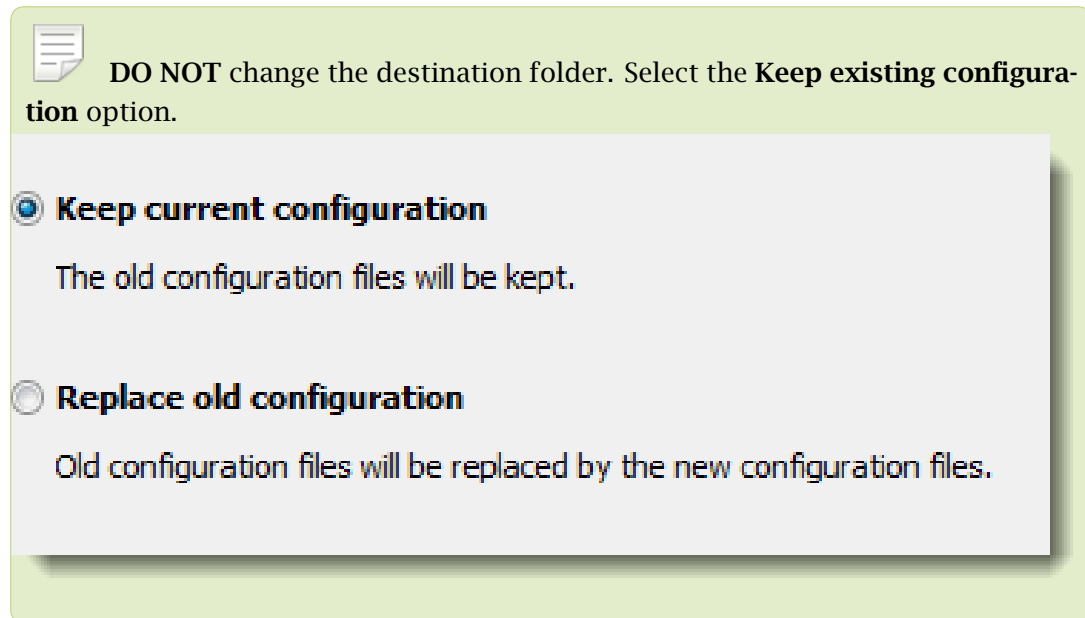
2. Copy the **Kerio/MailServer** directory from the **Program Files (x86)** folder of your 32-bit system to the **Program Files** folder on your 64-bit system.
3. Open the **mailserver.cfg** file and change all paths from **C:\Program Files (x86)\** to

## Switching from a 32-bit installation of Kerio Connect to 64-bit

---

C:\Program Files\.

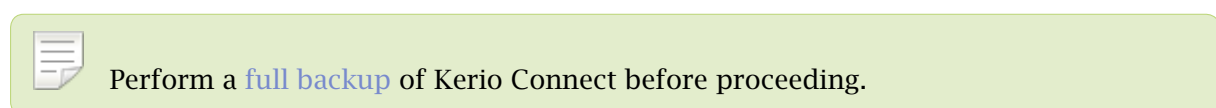
4. On your 64-bit system, install the 64-bit version of Kerio Connect.



A 64-bit version of a Kerio Connect is installed in the **Program Files** folder on your 64-bit Microsoft Windows system.

## Linux

The steps for switching from a 32-bit version of Kerio Connect to a 64-bit installation differ for [32-bit systems](#) and [64-bit systems](#).



### 64-bit Linux

1. Uninstall the 32-bit version of your Kerio Connect.

Debian — `apt-get remove <package name>`

RPM — `rpm -e <package name>`

2. Install the 64-bit version of Kerio Connect.

You can now start using the 64-bit version of Kerio Connect.



### 32-bit Linux

1. Install the 64-bit Linux.
2. On the 32-bit system, uninstall the 32-bit version of Kerio Connect.  
Debian — `apt-get remove <package name>`  
RPM — `rpm -e <package name>`
3. Copy the contents of the **opt/kerio/mailserver** folder on the 32-bit system to the same folder on the 64-bit system.
4. Install Kerio Connect on the 64-bit system.

You can now start using the 64-bit version of Kerio Connect.

### Virtual appliances

Use these steps to move from a 32-bit virtual appliance to the 64-bit Kerio Connect virtual appliance.



Perform a [full backup](#) of Kerio Connect before proceeding.

1. Deploy the 64-bit version of the Kerio Connect VMware appliance.
2. Stop Kerio Connect on both appliances.
3. Use SSH to connect to the appliances.
4. Use SCP to copy the following items from **opt/kerio/mailserver** on the 32-bit appliance to the same folder on the 64-bit appliance:
  - **license** folder
  - **mailserver.cfg** file
  - **users.cfg** file
  - **cluster.cfg** file
  - **sslcert** folder
  - **store** folder

## Switching from a 32-bit installation of Kerio Connect to 64-bit

---



Pack the whole store before copying.

If you have the store folder on an external hard drive, this step is not required.

- **ldapmap** folder if you have edited any files
- **fulltext** folder if you have enabled the full text search feature



Pack the fulltext folder before copying.

If you have the fulltext folder on an external hard drive, this step is not required.

5. Start the 64-bit Kerio Connect appliance.

You can now start using the 64-bit version of Kerio Connect virtual appliance.

# Accessing Kerio Connect

---

## What interfaces are available in Kerio Connect

Kerio Connect includes two interfaces:

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

Use the [officially supported browsers](#) to access the interfaces.

Kerio Connect Administration and Kerio Connect Client are available in several languages. The default language is the language of your browser.

## Kerio Connect Client

For information about the end-user interfaces, see [Accessing Kerio Connect Client](#).

## Kerio Connect administration

For information about the administration interface, see [Accessing Kerio Connect administration](#).



You can also manage Kerio Connect through MyKerio. See [Adding Kerio Connect to MyKerio](#) for more information.

## How to log out

After you finish your work in the administration interface, log out. Disconnecting from Kerio Connect increases the security of data stored on the server.

## Automatic logout

If Kerio Connect Client for web or the administration are idle for a certain time, you are automatically disconnected.

To set the period for automatic logout:

1. In the administration interface, go to **Configuration** → **Advanced options** → **Kerio Connect Client**.
2. In the **Session security** section, set the timeout for:

## Accessing Kerio Connect

---

- **Session expiration** is the time without any activity in an interface after which Kerio Connect ends the session.



The timeout is reset each time user performs an action.

- **Maximum session duration** is the time after which users are be logged out even if they actively use the interface.
3. As a protection against session hijacking you can force logout after Kerio Connect user changes their IP address. Select **Force logout from Kerio Connect Client....**



Do not use this option, if your ISP changes IP addresses during the connection (for example, in case of GPRS or WiFi connections).

4. Click **Apply**.

### 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)



These session security settings apply to both the administration interface and Kerio Connect Client for web.

# Accessing Kerio Connect administration

---

## Logging into the Kerio Connect administration

Only users with [appropriate rights](#) can access the Kerio Connect administration interface.

You can access the Kerio Connect administration only via secured connections (HTTPS). You can use either the IP address or the DNS name of Kerio Connect.

1. In your browser, type the URL of your Kerio Connect in the following format:

`https://server_name:4040/admin`

For example: `https://mail.feelmorelaw.com:4040/admin`

Use only the [officially supported browsers](#).



If Kerio Connect is behind firewall, you must allow the [HTTPS](#) service on port 4040.

Type `server_name/admin` and the browser automatically redirects you to the secured connection and port 4040.

2. In the login dialog, type your admin username and password.

If your account does not belong to the [primary domain](#), type your email address in the username field.

3. Click **Login**.



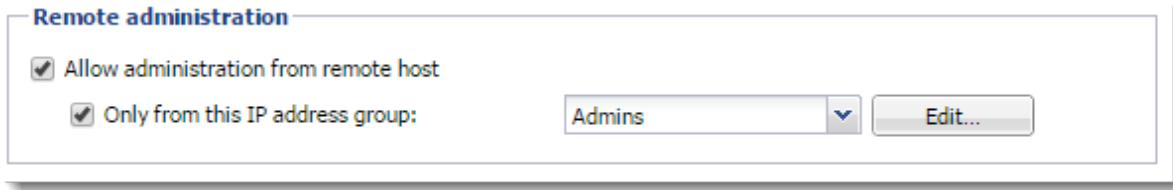
### Accessing the administration interface remotely

Administrators can access the administration interface:

- From the computer where Kerio Connect is installed
- From remote computers

To allow access to Kerio Connect Administration from a remote computer:

1. Go to **Configuration** → **Administration Settings**.
2. Select **Allow administration from remote host**.
3. (Optional) Specify a [group of IP addresses](#) from which administrators can access the administration.
4. Click **Apply**.



## Administrator accounts and access rights

For information about administration access rights, see [Setting access rights in Kerio Connect](#)

## Automatic logout



These session security settings apply to both the administration interface and Kerio Connect Client for web.

If Kerio Connect Client for web or the administration interfaces are without any activity, you are automatically disconnected.

To set the period for automatic logout:

1. In the administration interface, go to **Configuration** → **Advanced options** → **Kerio Connect Client**.
2. In the **Session security** section, set the timeout.
  - **Session expiration** is the time without any activity in an interface after which Kerio Connect ends the session.



The timeout is reset each time user performs an action.

- **Maximum session duration** is the time after which users are logged out even if they actively use the interface.
3. To protect against session hijacking, select **Force logout from Kerio Connect Client...** Kerio Connect then logs out users after their IP address changes.



Do not use this option, if your ISP changes IP addresses during the connection (for example, in case of GPRS or WiFi connections).


4. Click **Apply**.

## Accessing Kerio Connect administration


---

### 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)

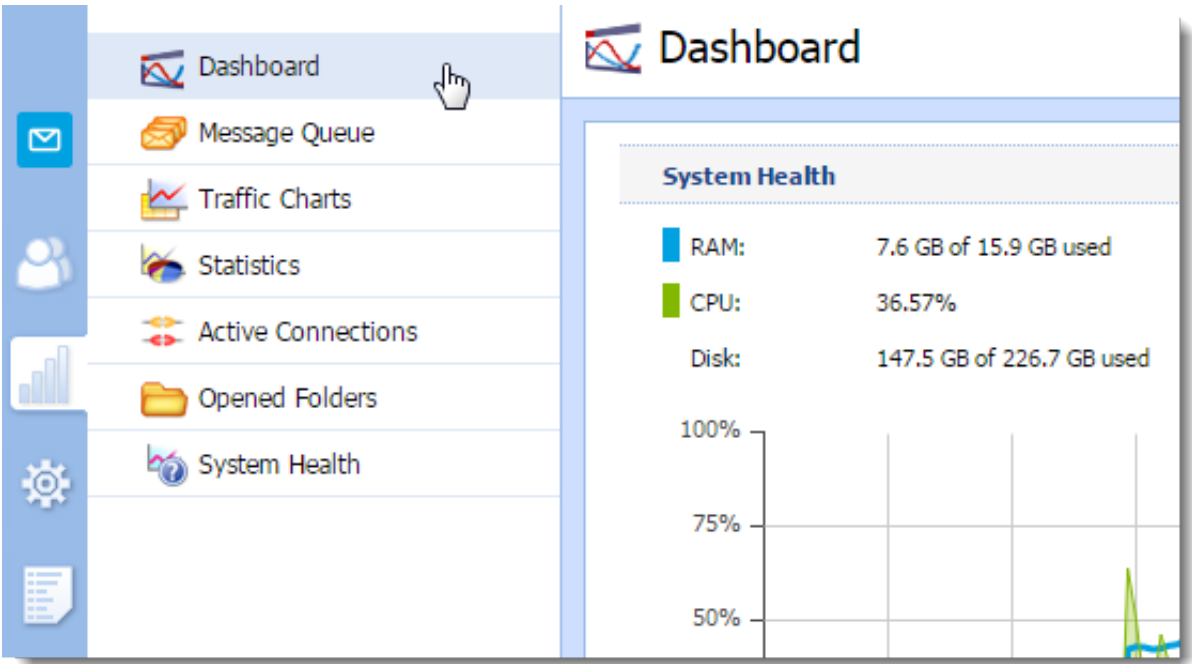


# Using Dashboard in Kerio Connect

## Dashboard overview

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

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



# Using Dashboard in Kerio Connect

The screenshot shows the Kerio Connect Dashboard interface. Annotations with red boxes and arrows point to various features:

- Tiles:** A box labeled "Tiles" has arrows pointing to the "System Health" and "System Status" tiles.
- Add new tiles:** A box labeled "Add new tiles" points to the "Add Tile" button at the bottom left.
- Remove this tile:** A box labeled "Remove this tile" points to the trash icon in the top right corner of the "License Details" tile.
- To change the tile order, drag the tile to another place:** A box labeled "To change the tile order, drag the tile to another place" points to the drag handle icon in the top left corner of the "License Details" tile.

The dashboard content includes:

- System Health:** RAM (1.8 GB of 3.8 GB used), CPU (2.86%), and Disk (9.6 GB of 454.5 GB used) usage. A graph shows usage over time from 11:05 to Now.
- System:** Version 9.2.0 (2250), Operating system Ubuntu 15.10, x86\_64, and Hostname mail.feelmorelaw.com.
- System Status:** Uptime (15 days, 0 hours, 54 minutes), Antivirus (Enabled), Antispam (Enabled), Greylisting (Enabled), Exchange ActiveSync (Enabled), Last backup (2016-10-21 01:00), Messages in the queue (0), and MyKerio (Enabled).
- License Details:** License number (12345-12345-12345), Software Maintenance expiration date (2017-12-10), Product expiration date (2017-12-10), Number of users allowed by the license (20), Number of active mailboxes (3 (11 created)), Company (Feel More Law Inc.), Sophos® extensions (Yes), Exchange ActiveSync® extensions (Yes), and Kerio Anti-spam (Yes). Links for "Install license..." and "Update registration info..." are provided.

# Navigating through the Kerio Connect administration interface

---

## Overview

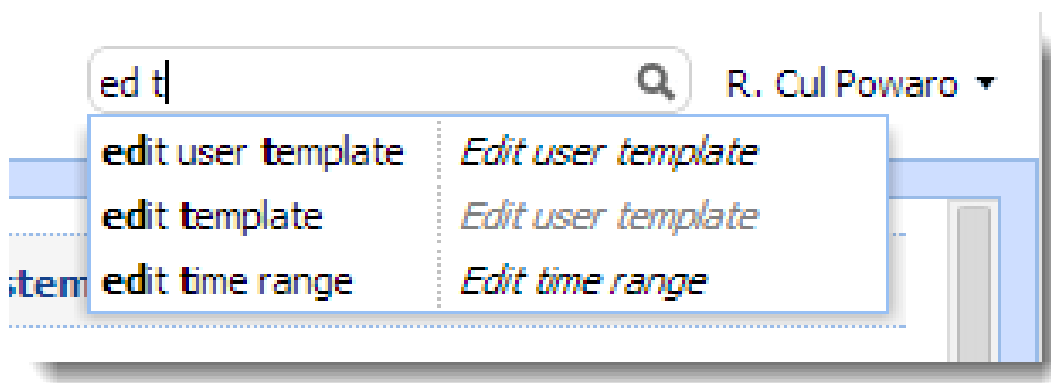
Using keywords, you can easily search for the location of any section or dialog in the Kerio Connect administration interface.

## Searching for specific sections in the administration interface

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

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

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



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

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

## Navigating through the Kerio Connect administration interface

The screenshot shows the 'Advanced Options' page in the Kerio Connect administration interface. A search bar at the top right contains the text 'message'. Below the search bar, a list of options is displayed, with a search filter applied. The options are:

- maximum **message** size
- delete **messages**
- sending **messages** outside domain
- message** footer
- message** prefix
- uuencoded **messages**
- decoding TNEF **messages**
- message** size limit
- reject **message**
- archive local **messages**
- archive incoming **messages**
- archive outgoing **messages**
- archive relayed **messages**
- leave a copy of **message** on the server
- high priority **message**
- send **messages** from outgoing queue

Annotations in the image point to:

- highlighted section:** The 'Miscellaneous' tab is highlighted with a red box.
- keywords and phrases:** The word 'message' in the search bar and the word 'message' in the search results.
- names of sections and dialogs:** The names of the sections and dialogs listed on the right side of the search results, such as 'Edit user', 'Edit mailing list', 'Miscellaneous settings', etc.



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

# Domains in Kerio Connect

---

## Overview

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, for example:

- Domain name — `feelmorrelaw.com`
- Email domain name — `mail.feelmorrelaw.com`
- User email address — `user@feelmorrelaw.com`

Kerio Connect may include [any number](#) of email domains.



[User accounts](#) are defined separately in each domain. Therefore, domains must be defined before you create user accounts.

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

To display various information in the columns, right-click any column name and select the items you want to display.

Internet hostname: mail.feelmorrelaw.com

Name ▲	Description	Aliases	Forward to Host
@ feelmorrelaw.com (primary)	Primary company domain	feelmorrelaw.cz	
@ company.com			
@ somewhere.com	Forward domain		smtp.fr.company.com

Buttons: Add, Edit..., Remove, Set as Primary, Distributed Domains..., Internet Hostname..., Public Folders...

### Internet hostname

To make messages deliverable, you must specify a DNS name of the server with Kerio Connect installed — the Internet hostname.

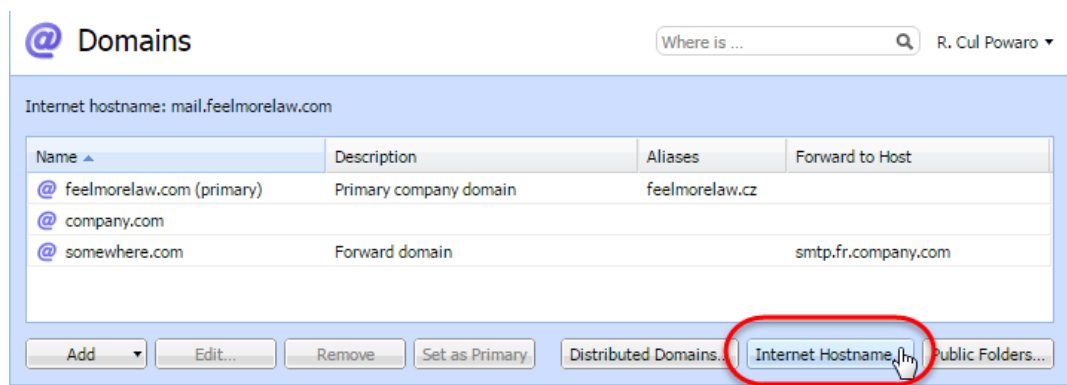
Kerio Connect also uses the Internet hostname when establishing the SMTP traffic. When the SMTP connection is established, the EHLO command is used for retrieving the reverse DNS record. The server that communicates with Kerio Connect can perform checks of the reverse DNS record.



If Kerio Connect is running behind NAT, use the Internet hostname of the firewall.

To change the internet hostname:

1. In the administration interface, go to **Configuration** → **Domains**.
2. Click the **Internet hostname** button.

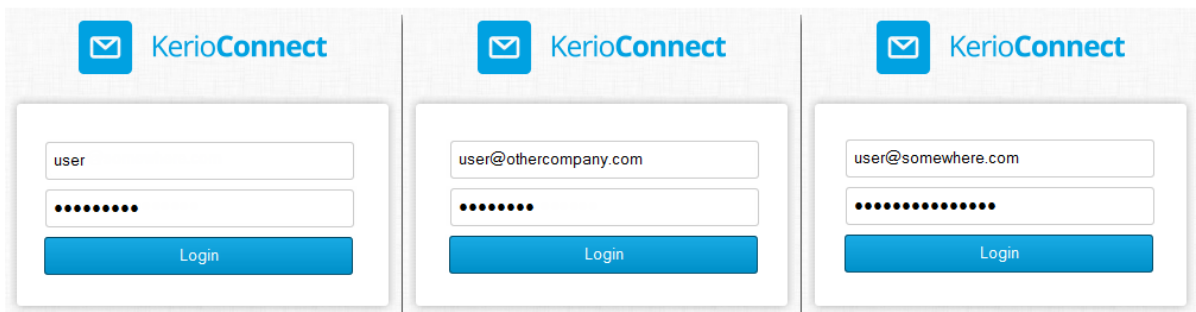
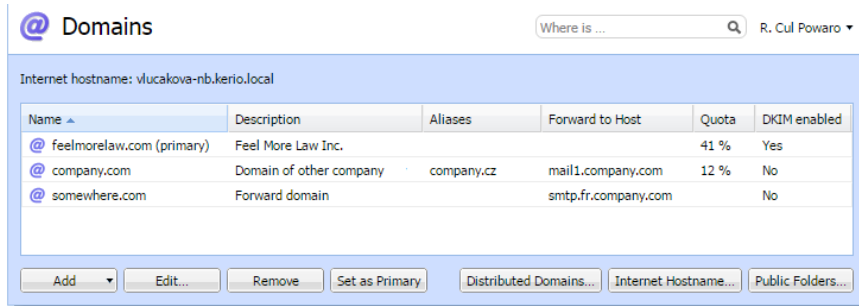


3. Type the server name and click **OK**.



## Primary domain

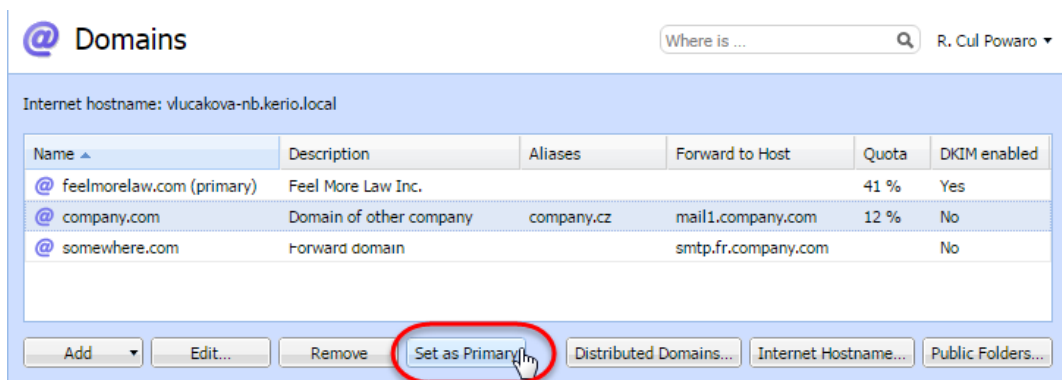
One domain in Kerio Connect must be set as **primary**. Users defined in a primary domain use only their username for authentication, not the whole email address.



By default, the first domain you create is set as primary automatically.

To change the primary domain:

1. In the administration interface, go to **Configuration** → **Domains**.
2. Select a domain and click the **Set as Primary**.



### Adding new domains

For information about adding new domains to Kerio Connect, read [Creating domains in Kerio Connect](#).

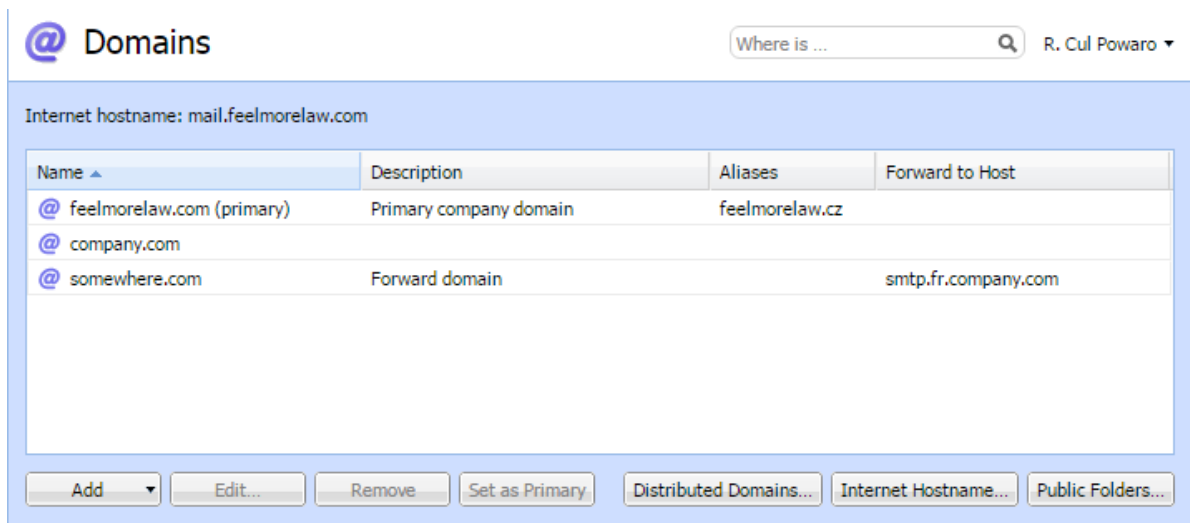


# Creating domains in Kerio Connect

---

## Adding domains in Kerio Connect

You can add any number of email domains in Kerio Connect. One domain must be set as a [primary domain](#).



To add a new domain to Kerio Connect:

1. In the administration interface, go to **Configuration** → **Domains**.
2. Click **Add** → **Local Domain**.
3. (Optional) Add a description for better reference.
4. Click **OK**.

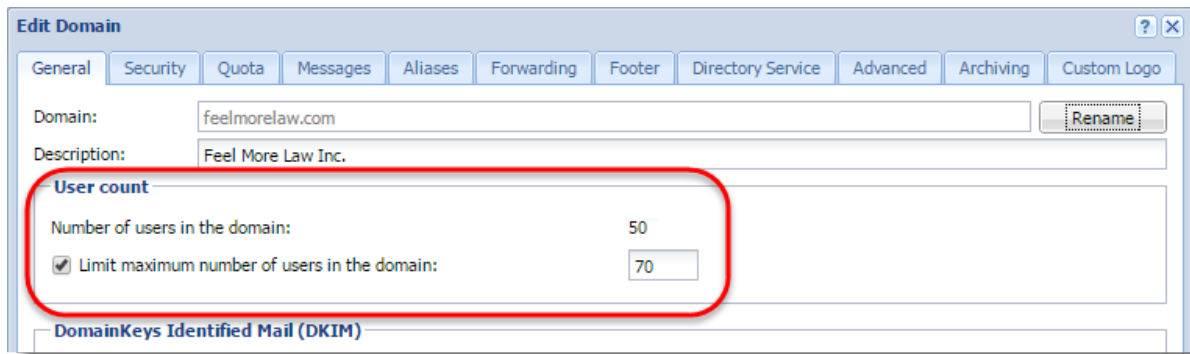
The domain is ready to use. Additional settings are available, as described below.

## Limiting the number of users per domain

You can limit the maximum number of domain [users](#) who can connect to Kerio Connect at a time.

1. Double-click a domain.
2. On the **General** tab, in the **User count** section, select **Limit maximum number of users in the domain**.
3. Set the number of users.
4. Click **OK**.

## Creating domains in Kerio Connect



The screenshot shows the 'Edit Domain' window with the following details:

- Domain: feelmorelaw.com
- Description: Feel More Law Inc.
- User count** (highlighted):
  - Number of users in the domain: 50
  - Limit maximum number of users in the domain: 70
- DomainKeys Identified Mail (DKIM)



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

## Limiting the disk space per domain



New in Kerio Connect 9.1!

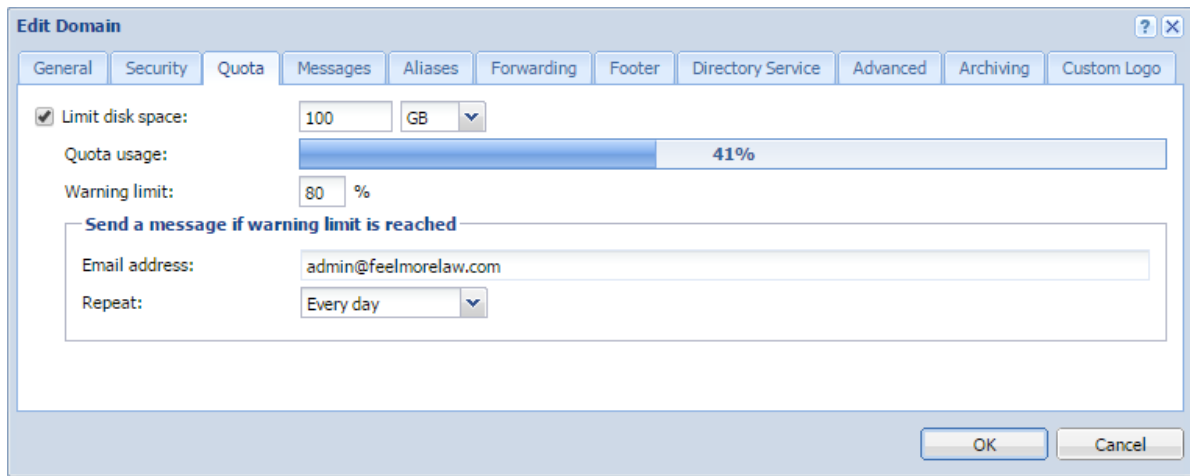
You can limit the disk space occupied by a domain and have Kerio Connect send you an email when a specified percentage of that space is filled (the warning limit).

Archive and global public folders are excluded from the quota.

If a domain fills up the disk space:

- Kerio Connect blocks all incoming messages
- Users cannot create any new items, such as calendar events, tasks, and notes

1. Double-click a domain.
2. Go to the **Quota** tab.
3. Select **Limit disk space** and set the quota.
4. Set **Warning limit** percentage.
5. Specify **Email address** that will be sent a message when the domain reaches the limit.
6. Specify how often the warning is repeated.
7. Click **OK**.



### Enabling message encryption with a DKIM signature

For information on DKIM signatures, see [Authenticating messages with DKIM](#).

### Enabling chat in Kerio Connect Client



New in Kerio Connect 9.1!

For information on chat, see [Enabling chat in Kerio Connect Client](#).

### Limiting message size and setting item clean-out to save space

For information on keeping your data manageable, see [Maintaining user accounts in Kerio Connect](#).

### Creating domain aliases

For information on domain aliases, see [Creating aliases in Kerio Connect](#).

### Forwarding messages to another server

You can forward messages to another server, if the recipient is not from your domain.

1. Double-click a domain.
2. Go to the **Forwarding** tab.
3. Enable **If the recipient was not found in this domain**

## Creating domains in Kerio Connect

---

4. Specify the server and port.

5. Set the delivery option.

Messages can be forwarded immediately, by the scheduler, or by ETRN command.

6. (Optional) Disable forwarding for messages sent to domain alias addresses.



To forward messages, you can also create a message filter on the server - see [Filtering messages on the server](#).

The screenshot shows the 'Edit Domain' dialog box with the 'Forwarding' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: General, Security, Quota, Messages, Aliases, Forwarding (selected), Footer, Directory Service, Advanced, Archiving, and Custom Logo. The main content area contains the following options:

- If the recipient was not found in this domain, forward the message to another host
- Forward to:  Port:
- i** Consider using **distributed domains** instead of forwarding. [Learn more...](#)
- Delivery options**
- Online - deliver the messages immediately
- Offline - delivery is started by scheduler
- Offline - delivery is triggered by ETRN command from remote host
- Forwarding**
- If the domain in recipient's address is one of this domain's aliases:
- Forward this message
- Don't forward such message (prevent loops in multiple server scenarios)

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

### Customizing Kerio Connect

For information on custom domain footers and custom logos for Kerio Connect Client, see [Customizing Kerio Connect](#).

### Mapping users from a directory server

For information on directory services and mapping users, see [Connecting Kerio Connect to directory service](#) and [Mapping accounts from a directory service](#).

### Archiving messages for individual domains



New in Kerio Connect 9.1!

For information on per-domain archiving, see [Archiving in Kerio Connect](#).

### Additional configuration options

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

- Set a new [Internet hostname](#).
- Manage [public folders](#).
- Create [distributed domains](#).

### Deleting domains

If you want to delete a domain in Kerio Connect, that domain must not:

- Be a [primary domain](#).
- Contain any [users](#).
- Have any [aliases](#) assigned to it.

# Connecting Kerio Connect to directory service

---

## Overview

Mapping accounts from a directory service provides these benefits:

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



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

## Supported directory services

Kerio Connect supports:

- [Microsoft Active Directory](#)
- [Apple Open Directory](#)

## Microsoft Active Directory

To connect Kerio Connect to Microsoft Active Directory:

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

4. Select **Map user accounts and groups from a directory service**.
5. As a **Directory service type**, select **Microsoft Active Directory** from the drop-down menu.
6. In the **Hostname** field, type the DNS name or IP address of the Microsoft Active Directory server.  
If you enable secure connection in step 8, use the DNS name.  
If a non-standard port is used for communication between Kerio Connect and Microsoft Active Directory, add the port number to the hostname.
7. Type the **Username** and **Password** of a Microsoft Active Directory administrator with full access rights to the administration.
8. To protect data, such as user passwords, sent from Microsoft Active Directory to Kerio Connect and vice versa, select **Enable secured connection (LDAPS)**.
9. Click **Test connection** to verify you typed the correct data.
10. On the **Advanced** tab, specify the Kerberos realm.  
See the [Kerberos authentication](#) section below.
11. Save the settings.

Now you can [map users](#) to Kerio Connect.

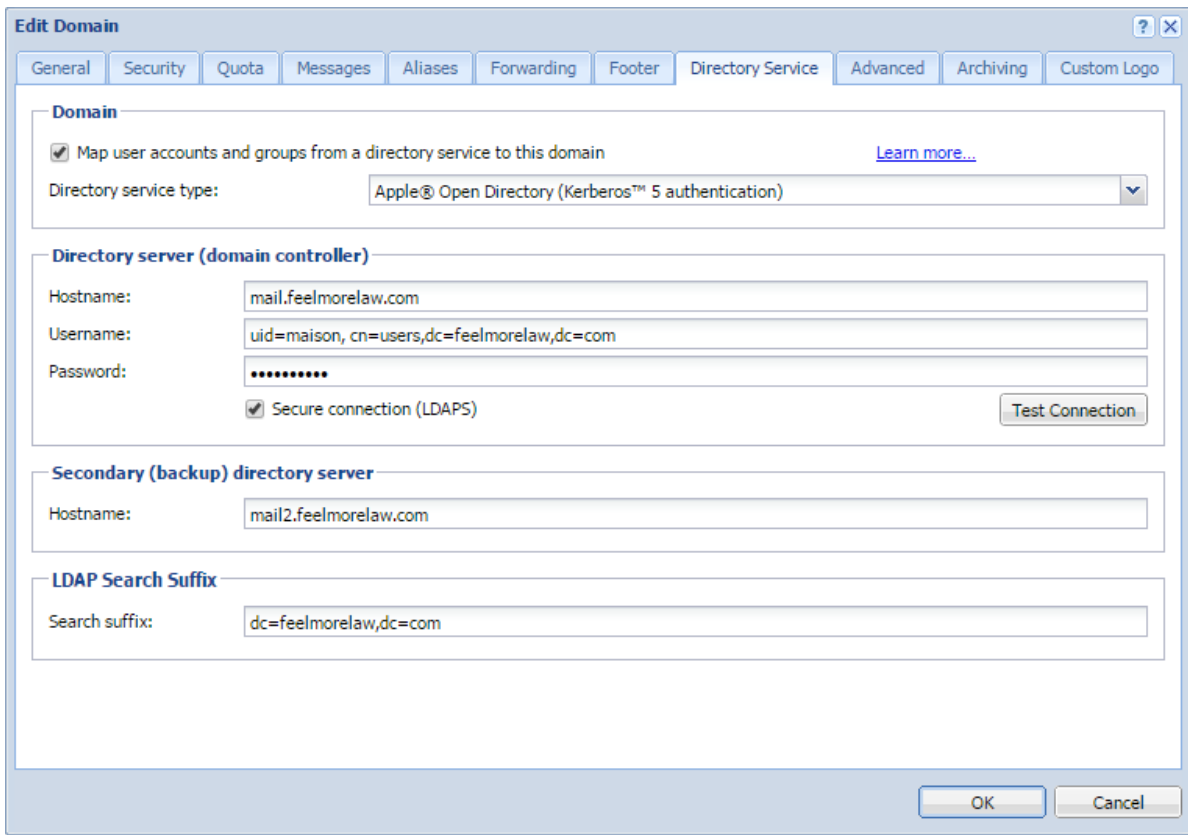
The screenshot shows the 'Edit Domain' dialog box with the 'Advanced' tab selected. The 'Directory Service' sub-tab is active. The 'Domain' section has the checkbox 'Map user accounts and groups from a directory service to this domain' checked. The 'Directory service type' dropdown is set to 'Microsoft® Active Directory®'. The 'Directory server (domain controller)' section has the following fields: Hostname: mail.feelmorelaw.com, Username: maison@feelmorelaw.com, Password: [masked], and the 'Secure connection (LDAPS)' checkbox is checked. A 'Test Connection' button is visible. The 'Secondary (backup) directory server' section has Hostname: mail2.feelmorelaw.com. The 'Microsoft® Active Directory® Domain Name' section has the checkbox 'Different from this mail domain name:' unchecked and the domain name field set to feelmorelaw.com. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

### Apple Open Directory

1. On the Apple Open Directory server, install the [Kerio Open Directory Extension](#).
2. In the Kerio Connect administration interface, go to **Configuration** → **Domains**.
3. Double-click the domain and switch to the **Directory Service** tab.
4. Select **Map user accounts and groups from a directory service**.
5. As a **Directory service type**, select **Apple Open Directory** from the drop-down list.
6. In the **Hostname** field, type the DNS name or IP address of the Microsoft Active Directory server.  
  
If you enable secure connection in step 8, use the DNS name.  
  
If a non-standard port is used for communication between Kerio Connect and Microsoft Active Directory, add the port number to the hostname.
7. Type the **Username** and **Password** of an Apple Open Directory administrator with full access rights to the administration.
8. To protect data, such as user passwords, sent from Microsoft Active Directory to Kerio Connect and vice versa, select **Enable secured connection (LDAPS)**.
9. Click **Test connection** to verify you entered the correct data.
10. On the **Advanced** tab, specify the Kerberos realm.  
  
See the [Kerberos authentication](#) section below.
11. Save the settings.

Now you can [map users](#) to Kerio Connect.





## Kerberos authentication

To use the Kerberos authentication:

1. Verify that Kerio Connect belongs to the Active Directory or Open Directory domain.
2. In the administration interface, go to **Configuration** → **Domains**.
3. Double-click a domain and switch to the **Advanced** tab.
4. (For Linux installations only) Type the PAM service name.

For additional information, see [Authenticating users through PAM](#).

5. Type the **Kerberos realm name**.

The Kerberos realm name is your domain name and Kerio Connect specifies it automatically upon domain creation.

6. If you are using the Windows NT domain, type the domain name.
7. (Optional) Select **Bind this domain to specific IP address** and type the IP address .

Users accessing Kerio Connect from this IP address use only their username (without the domain name) to log in.

8. Click **OK**.

## Connecting Kerio Connect to directory service

**Edit Domain**

General Security Quota Messages Aliases Forwarding Footer Directory Service Advanced Archiving Custom Logo

**Kerberos™ 5**

For users in this domain authenticated through Kerberos™ 5 (Microsoft® Active Directory® or Apple® Open Directory), use this Kerberos realm (Microsoft® Active Directory® domain or Apple® Open Directory) name:

FEELMORELAW.COM

**Windows NT® domain**

For users in this domain authenticated through Windows NT domain use this NT domain name:

FEELMORELAW

Bind this domain to specific IP address: 192.168.92.1

**i** This IP address will be used for sending outgoing messages from this domain.  
If a user connects to the server via an interface with this IP address, this domain name is appended to the username by default.

OK Cancel

You can display a column with the Kerberos info in **Configuration** → **Domains**.

**@ Domains**

Internet hostname: vlucakova-nb.kerio.local

Name ▲	Description	Aliases	Kerberos™
@ feelmorelaw.com (primary)	Feel More Law Inc.		FEELMORELAW.COM
@ company.com	Domain of other company	company.cz	COMPANY.COM
@ feelmorelaw.eu	Feel More Law Inc. Europe		FEELMORELAW.EU
@ firma.cz	Lokální primární doména	nasprodukt.cz, firmicka.cz	FIRMA.CZ

## Mapping users from directory services

For information on activating users, read article [Creating user accounts in Kerio Connect](#).

## Migrating user accounts from local database to directory service

For detailed information, read article [Migrating user accounts from local database to directory service](#).

## Troubleshooting

All information about directory service can be found in the [Debug](#) and [Warning](#) logs.

# Migrating user accounts from local database to directory service

---

## Overview

You can connect your Kerio Connect to [Microsoft Active Directory](#) or [Apple Open Directory](#). To migrate the users accounts from a local database to a directory service:

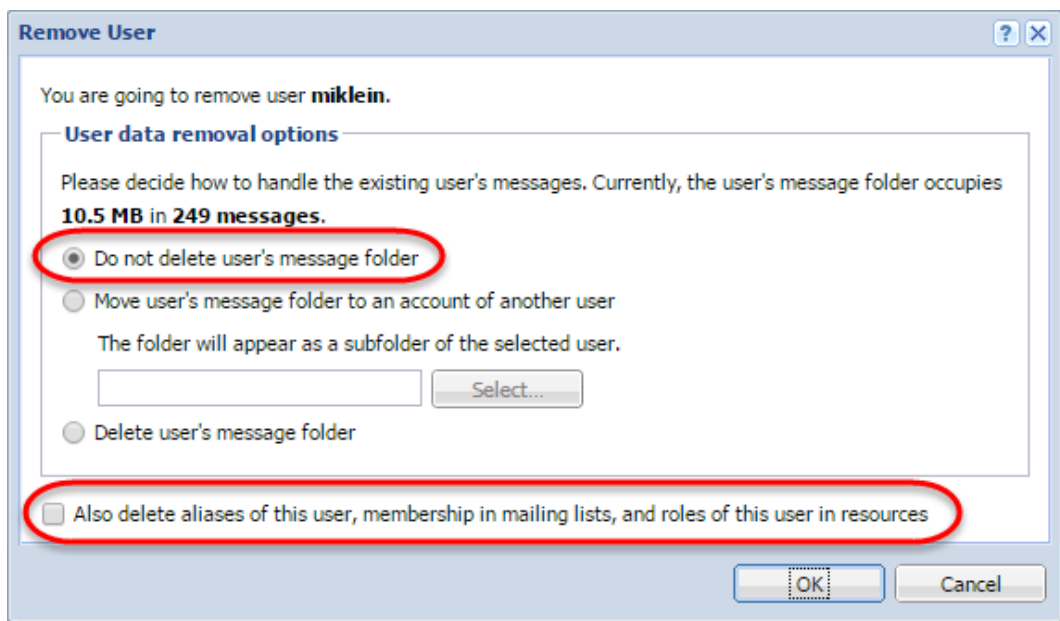
1. Remove the local accounts from Kerio Connect.
2. Connect your domain to a directory service.
3. Create new accounts in the directory service with identical usernames as before.

## Migrating users

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



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



3. Connect your domain to a directory service.

See [Connecting Kerio Connect to directory service](#) for details.

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

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

See [Mapping accounts from a directory service](#) for details.

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

### **Troubleshooting**

All information about directory service can be found in the [Debug](#) and [Warning](#) logs.

# Authenticating users through PAM

---

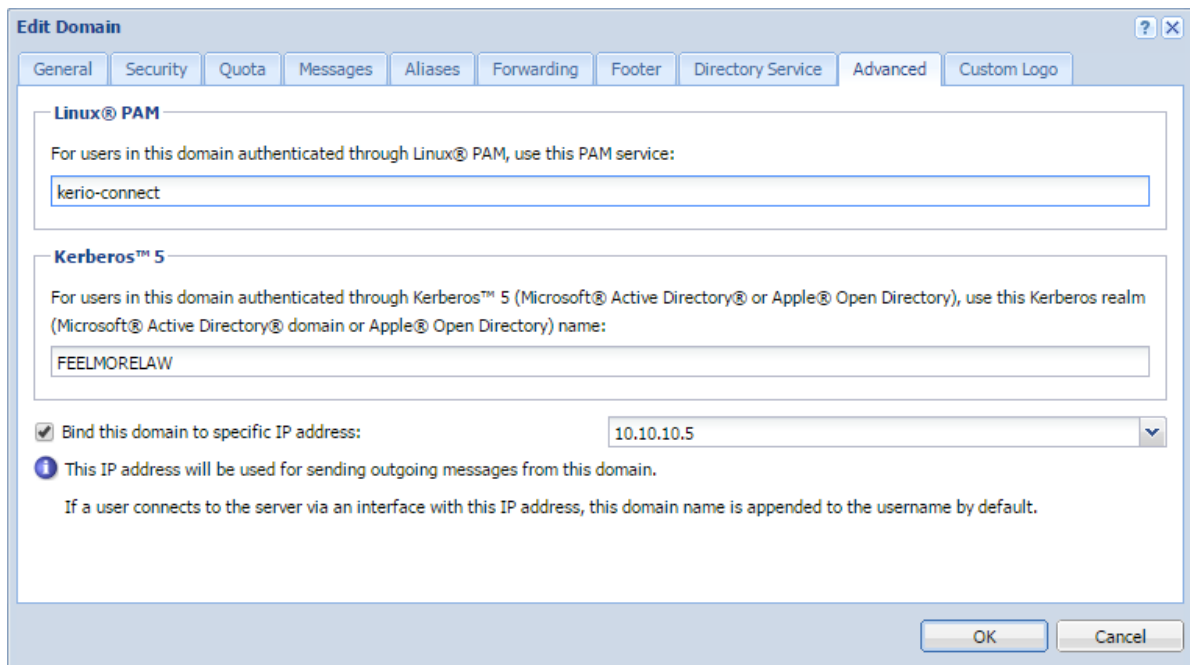
## Overview

On Linux, you can authenticate users from a specific domain against the Linux system.

The Kerio Connect installation package includes a configuration file for the `kerio-connect` PAM service. You can locate the file under `/etc/pam.d/kerio-connect`.

## Configuring PAM authentication

1. In the administration interface, go to **Configuration** → **Domains**.
2. Double-click the domain.
3. On the **Advanced** tab, type the name of the PAM service.
4. Click **OK**.



# Renaming domains in Kerio Connect

---

## Overview

In Kerio Connect, you can rename your domain in the administration interface. 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
<i>domain name</i>	old_domain.com	new_domain.com
<i>names_of_aliases</i>	alias.com	old_domain.com alias.com

Table 1 Rename Domain

The domain configuration does not change after renaming.



Any calendar events created before renaming cannot be edited or removed after the domain is renamed.

## Prerequisites

Before you start the renaming process:

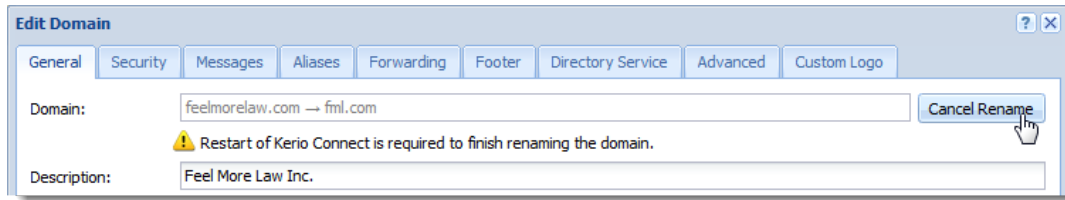
- Purchase a domain from your provider and make sure the DNS records are updated. Test the new domain.
- Make a [full backup of your message store](#) before and after the renaming process

## Renaming domains

1. In the administration interface, go to **Configuration** → **Domains**.
2. Double-click the domain you want to rename.
3. On the **General** tab, click **Rename**.
4. Type a new name for the domain.

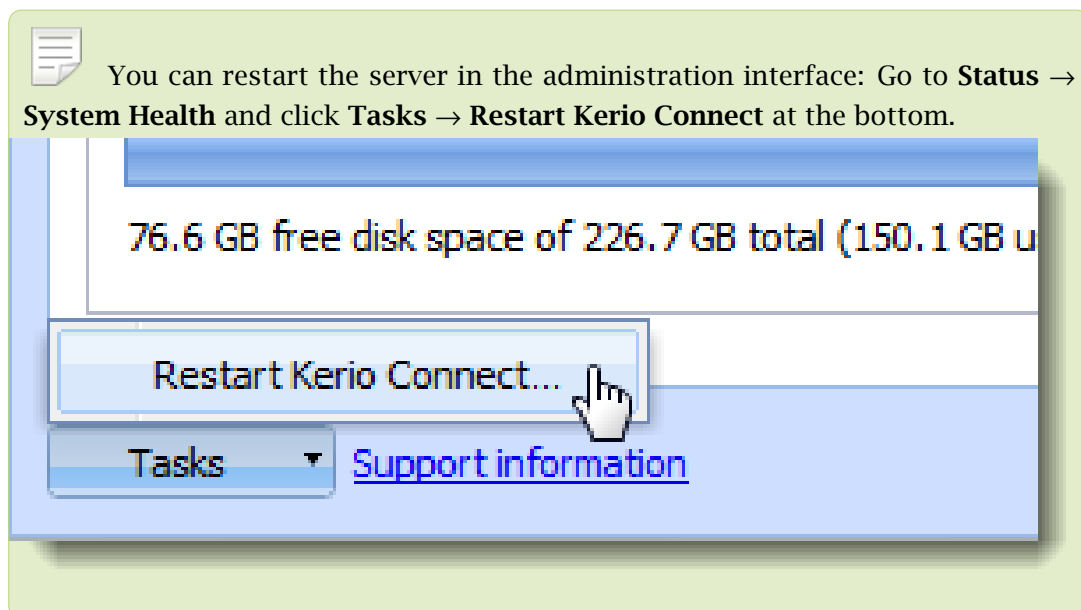
You can cancel the renaming process before you restart the server. Click **Cancel Rename** in the domain's configuration.

## Renaming domains in Kerio Connect



### 5. Restart the server.

Before the restart, all operations are performed using the original name. During the restart, Kerio Connect automatically replaces the original name 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 a distributed domain.

### Post-renaming issues

If users have email filters with addresses of users from a renamed domain, they must change the rules.

If users use Kerio Outlook Connector (Offline Edition), they must empty the cache after the domain is renamed.



# Distributed domains in Kerio Connect

---

## Distributed domains

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

Distributed domain connects the servers together and moves all users across all servers into a single email [domain](#).

Distributed domain requires users mapped from a [directory service](#).

For details read the [Distributed domains](#) manual.

# Creating user accounts in Kerio Connect

## Overview

In Kerio Connect, user accounts represent physical email boxes.

With user accounts you:

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

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

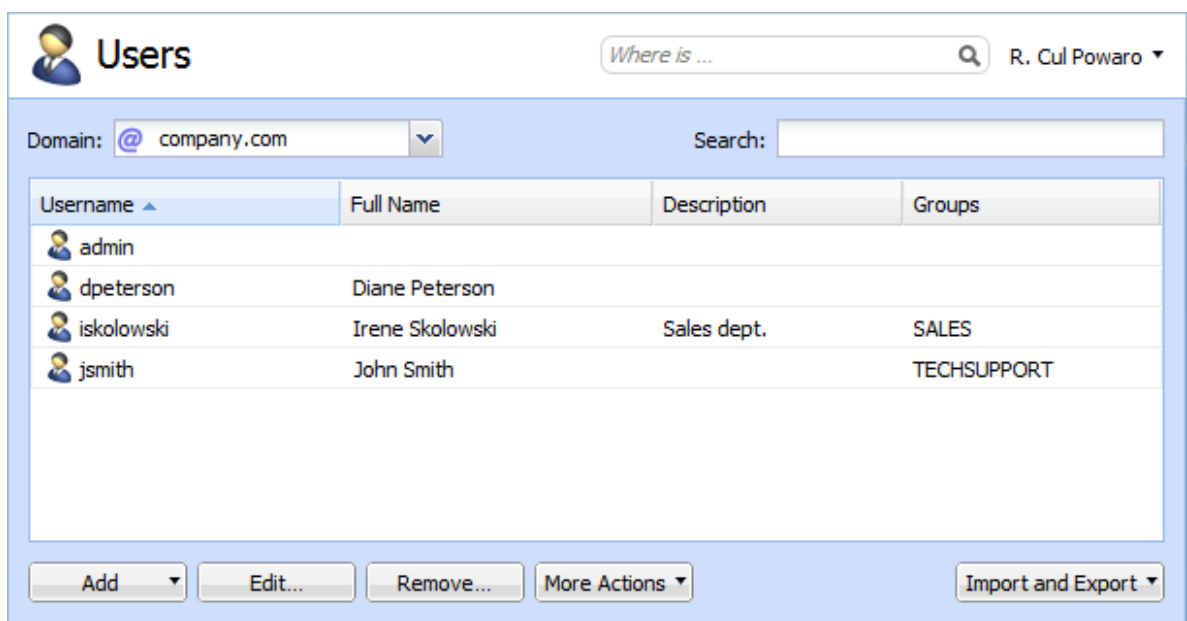


Figure 1 Users

## Creating user accounts

You can create either [local users](#) or [map existing users](#) from a [directory service](#).

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

Local accounts can also be imported to Kerio Connect. Read [Importing users in Kerio Connect](#) for more information.

### Creating local accounts

You can create and manage local accounts in the Kerio Connect administration interface.

1. Go to **Accounts** → **Users** and select a domain for the new account.
2. Click **Add** → **Add Local User**

You can also use a [template](#).

3. On the **General** tab, type a new username and password for the user.

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



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

4. Click **OK**.

**Add User**

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

Username: powaro

Full name: R. Cul Powaro

Description: Vice President

Authentication: Internal user database

Password: ..... Generate

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)

OK Cancel

Figure 2 Adding users

## Creating user accounts in Kerio Connect

---

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

### *Additional configuration*

For each user account, you can:

- Create email address [aliases](#).
- Forward messages to another mailbox within or outside Kerio Connect.
- [Add the user to groups](#).
- Set space [quotas](#).
- Configure [access rights](#) to the administration interface.
- Manage [account limits](#) (message count, sending outgoing messages, etc.)
- [Maintain accounts](#) (for example, message clean-out)
- [Restrict access to services](#)
- [Add personal and contact information](#)



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 for the account.
2. Click **Add** → **Add From a Directory Service**.
3. Select users you want to map to Kerio Connect.  
You can add users later.
4. Click **Next**.
5. Click **Finish**.

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

## Templates

If you plan to create multiple local accounts with similar settings, create a template:

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

## Disabling and deleting user accounts

You can temporarily disable user accounts or delete user accounts permanently. Both disabling and deleting free up your license.

You cannot disable/delete the following user accounts:

- Your own account
- User with a higher level of [administration rights](#)

### Disabling users temporarily

When you disable user accounts temporarily, users cannot login to Kerio Connect. However, all messages and settings of this user remain available in Kerio Connect.

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

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

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



This action is different from blocking when a [password guessing attack](#) occurs.

### Deleting users permanently

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

## Creating user accounts in Kerio Connect

---

3. In the **Remove Users** dialog box, you can:

- Delete the user's mailbox
- Keep the user's mailbox

When you create a account with the same username later, Kerio Connect automatically associates the new account with the old mailbox.

- Transfer it to another account in Kerio Connect
- Delete other settings of the user (aliases, roles, and so on)

4. Click **OK**.



Instant messaging files are always deleted.

## Troubleshooting

All information about users can be found in the [Config log](#).

Information about deleting users is logged in the [Warning log](#)

# Adding company and user contact information in Kerio Connect

---

## Overview

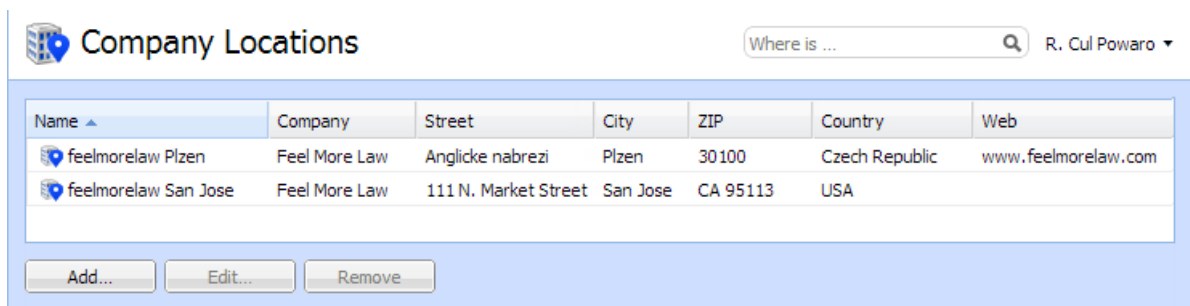
In Kerio Connect, you can add detailed contact information for your [company](#) or for [individual users](#).

Kerio Connect:

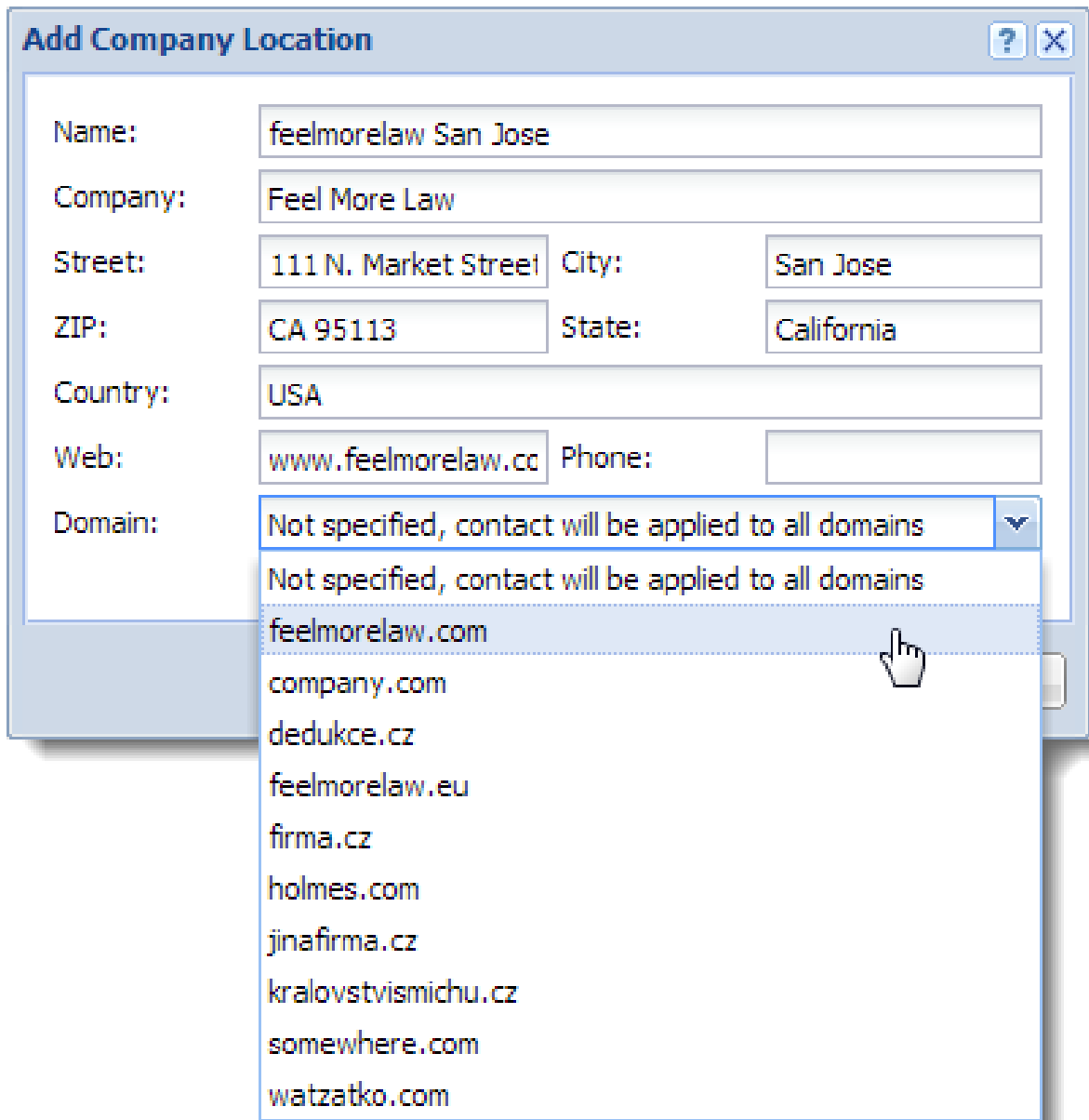
- displays this information in [users' contact details](#)
- uses this information when appending automatic domain footers (See [Customizing Kerio Connect](#) for more on footers.)

## Setting company locations

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



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



**Add Company Location**

Name:

Company:

Street:  City:

ZIP:  State:

Country:

Web:  Phone:

Domain:  ▼

- Not specified, contact will be applied to all domains
- feelmorelaw.com
- company.com
- dedukce.cz
- feelmorelaw.eu
- firma.cz
- holmes.com
- jinafirma.cz
- kralovstvimichu.cz
- somewhere.com
- watzatko.com

### Adding contact details to users

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



## 23.3 Adding contact details to users

**Edit User**

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

**Personal**

First name: R. Middle name: Cul  
Last name: Powaro Prefix:  
Phone: +123456789 Suffix:  
Mobile:

**Work**

Office: Job title: Vice President  
Department:  
Company location: Not specified Edit...  
Not specified  
feelmorelaw Plzen  
feelmorelaw San Jose

OK Cancel

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

# Creating user groups in Kerio Connect

## About user groups

You can use user groups in Kerio Connect to:

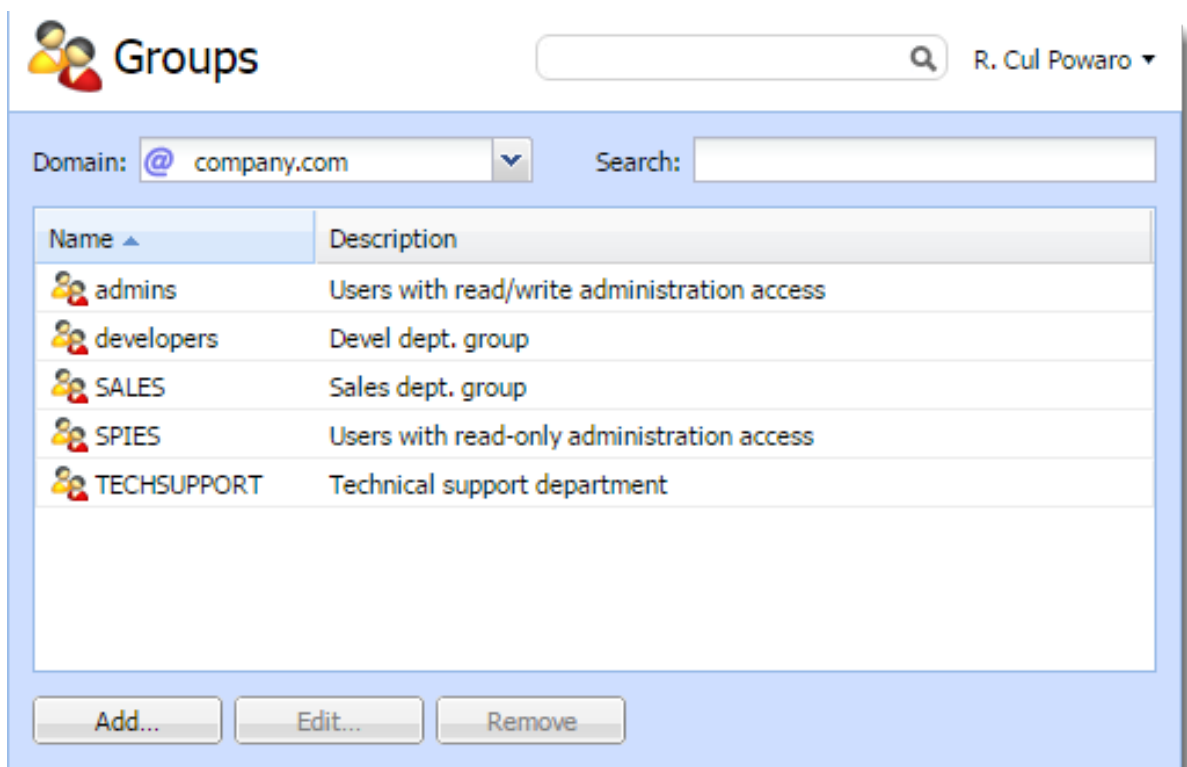
- Set [access rights](#) to Kerio Connect administration for multiple users
- Deliver a single message to multiple users via a single email address (see also [mailing lists](#))

You can:

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

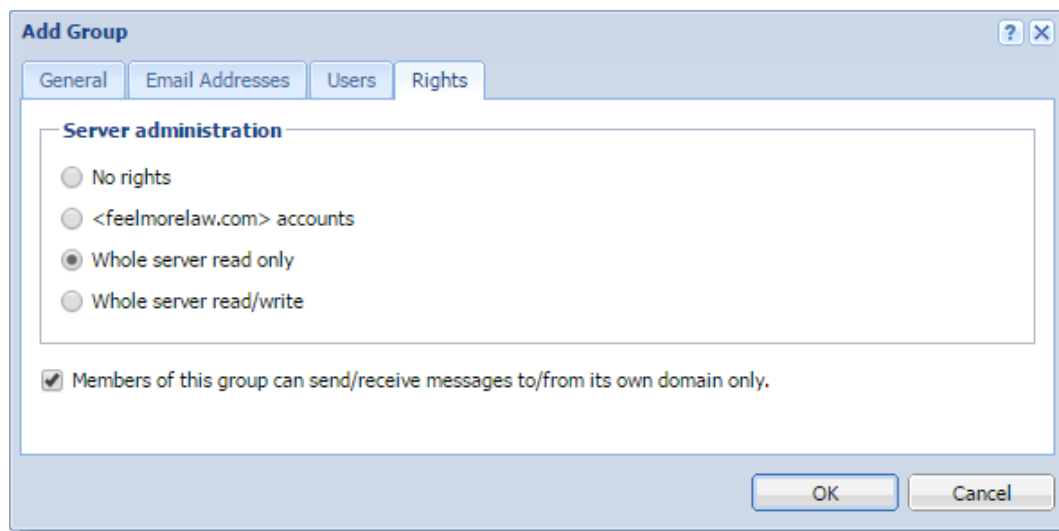
User groups belong to a [domain](#). Each domain may include any number of local and mapped groups. The number of groups is **not** limited by [your license](#).

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



## Creating user groups

1. Go to section **Accounts** → **Groups**.
2. Select a domain in which you want to create a group.
3. Click **Add**.
4. On the **General** tab, type a name for the group and description.
5. On the **Email Address** tab, add email addresses for the user group.  
You can add any number of email addresses. You can also use an existing username as the email address — any messages sent to the group email address will also be delivered to the original user.
6. On the **Userstab**, click **Add**.
7. Select the local users you want to add to the group and click **OK**.  
You can also go to **Accounts** → **Users** and select a group in user's settings.
8. On the **Rights** tab, set the access right to the administration interface (see [Setting access rights in Kerio Connect](#) for more details).



9. Click **OK**.

### Mapping groups from a directory service

To add groups from a directory service, you must:

1. Connect Kerio Connect to a directory service.  
See [Connecting Kerio Connect to directory service](#) for more details.
2. Activate groups in the administration interface

To activate groups:

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



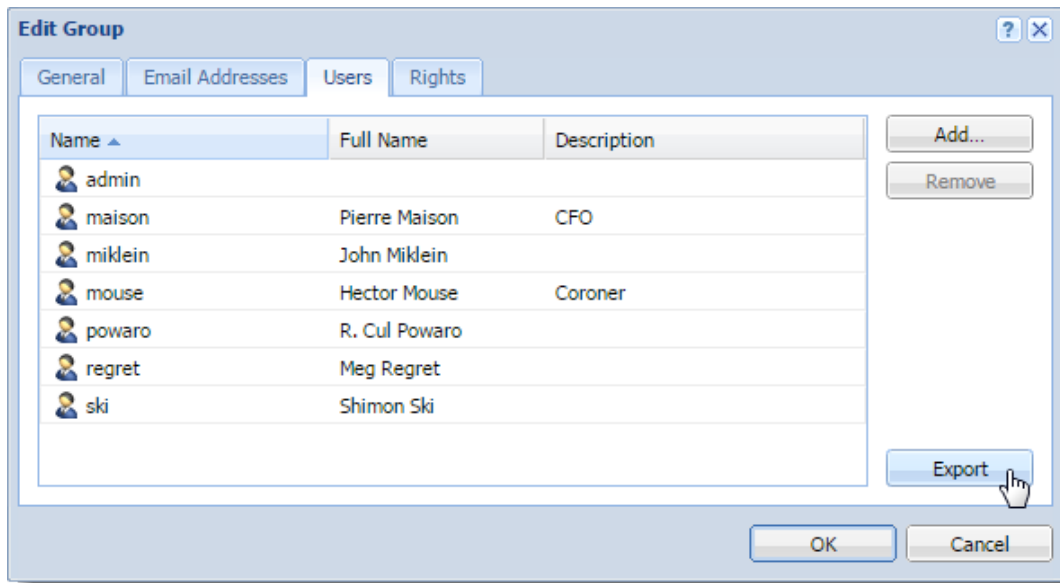
Kerio Connect does not map nested groups and users.

### Exporting group members

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

The data in the CSV file is organized as follows:

- Individual items are separated by semicolons
  - Multiple information within individual items are separated by commas
1. In the administration interface, go to the **Accounts** → **Groups** section.
  2. Double click a group.
  3. On the **Users** tab, click **Export**.



Kerio Connect saves the CSV file to your hard drive.

The filename has the following format:

users\_<domain\_name>\_<group\_name>\_<date>.csv (for example,  
users\_company.com\_TECHSUPPORT\_2015-09-09.csv)

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

# Setting access rights in Kerio Connect

---

## Overview

In Kerio Connect, you can set access rights to:

- **Kerio Connect Administration** (see below)
- **Public folders** (For details, see [Public folders in Kerio Connect](#))
- **Archive folders** (For details, see [Archiving in Kerio Connect](#))

## Administrator accounts and access rights

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

- [Built-in administrator](#)
- Users with special [access rights](#) to the administration



For more information about Kerio Connect Administration, see [Accessing Kerio Connect administration](#).

## Enabling the built-in administrator account

In Kerio Connect, you can enable a special administrator account. This account is available only for accessing the administration interface.

The built-in admin 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. Select **Enable built-in administrator account**

3. Type a password for this administrator.

The username is set to Admin and cannot be changed.

4. Click **Apply**.

The screenshot shows the 'Administration Settings' window. At the top, there is a search bar with the text 'Where is ...' and a magnifying glass icon, and a user profile 'R. Cul Powaro' with a dropdown arrow. The main content area is titled 'Built-in administrator account' and contains the following elements:

- A checked checkbox labeled 'Enable built-in administrator account'.
- A 'Login name:' field with the value 'Admin'.
- A 'Password:' field with a masked password of ten dots.
- A 'Confirm password:' field with a masked password of ten dots.
- An information icon (i) followed by the text: 'The built-in administrator account can be used only for administration and does not consume a license. The account does not include a mailbox.'



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 the **Enable built-in administrator account** option in **Configuration** → **Administration Settings**.

The same rules as for [disabling other admin accounts](#) apply.

## Assigning admin rights to individual users

### Types of admin access rights

You can assign users and groups the following administration access rights:

#### Whole server read/write

Admins can view and edit the whole administration interface.

#### Whole server read only

Admins can view the whole administration interface.

#### Domain accounts

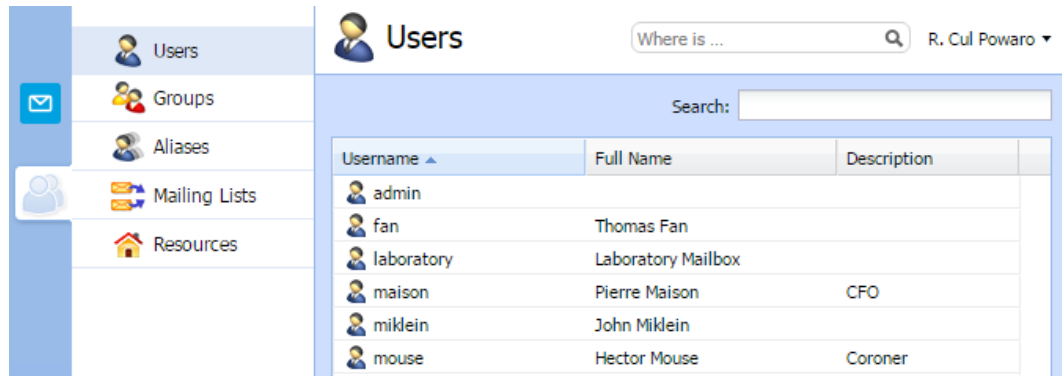
Admins can view and edit their own domain settings:

- **Users** (see [Creating user accounts in Kerio Connect](#))
- **User groups** (see [Creating user groups in Kerio Connect](#))
- **Aliases** (see [Creating aliases in Kerio Connect](#))

## Setting access rights in Kerio Connect

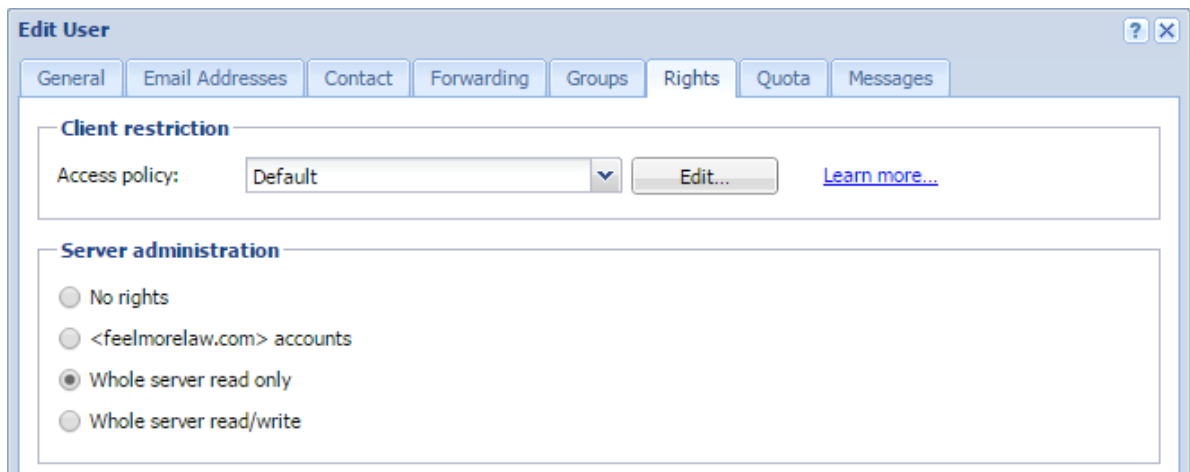
- **Mailing lists** (see [Creating mailing lists in Kerio Connect](#))
- **Resources** (see [Configuring resources in Kerio Connect](#))

The domain admin cannot assign the [archive admin rights](#), and set the [items clean-out](#).



### Assigning admin access rights

1. Go to **Accounts** → **Users** or **Accounts** → **Groups**.
2. Double click a user or a group.
3. On the **Rights** tab, select the level of access rights in the **Server administration** section.
4. Click **OK**.



To manage public and archive folders, see [Public folders in Kerio Connect](#) and [Archiving in Kerio Connect](#).



# Maintaining user accounts in Kerio Connect

---

## Overview

To maintain your user accounts and the mailstore 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](#)

## Deleting old items in users' mailboxes automatically

To save some space on your data store disk, you can set a special rule which deletes all messages older than a specified number of days. You can configure the items clean-out for **individual users** or **per domain**.



If both are configured, settings per user are applied.

Kerio Connect performs the clean-out periodically based on the size of your message store.

You can apply the automatic clean-out to the following folders:

- Trash
- Spam
- Sent
- All folders (except contacts and notes)



If you do not want to lose any messages with the clean-out, [archive](#) or [backup](#) your data store.

## Maintaining user accounts in Kerio Connect

---

### *Per domain settings*

1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Double-click a domain.
3. On the **Messages** tab, select folders for automatic clean-out and set the number of days.
4. Click **OK**.

**Items clean-out**

Permanently delete old items in:

<input checked="" type="checkbox"/> Trash folder, items older than:	<input type="text" value="30"/> days
<input checked="" type="checkbox"/> Spam folder, items older than:	<input type="text" value="30"/> days
<input checked="" type="checkbox"/> Sent folder, items older than:	<input type="text" value="30"/> days
<input type="checkbox"/> All folders except contacts and notes, items older than:	<input type="text" value="3"/> <input type="text" value="years"/>

**i** Old items will be deleted throughout the message store including messages, calendars, tasks, public folders and mailing lists archives.

### *Per user settings*

By default, new users inherit settings from their domain.

To change the settings for individual users:

1. In the administration interface, go to the **Accounts** → **Users** section.
2. Double-click a user.
3. Switch to the **Messages** tab
4. In the **Items clean-out** section, select the **Use custom settings for this user** option.
5. Select folders for automatic clean-out and set the number of days.
6. Click **OK**.

**Items clean-out**

Use the settings defined for this domain:

Use custom settings for this user

Permanently delete old items in:

<input checked="" type="checkbox"/> Trash folder, items older than:	<input type="text" value="55"/> days
<input checked="" type="checkbox"/> Spam folder, items older than:	<input type="text" value="55"/> days
<input checked="" type="checkbox"/> Sent folder, items older than:	<input type="text" value="55"/> days
<input type="checkbox"/> All folders except contacts and notes, items older than:	<input type="text" value="3"/> <input type="text" value="years"/>

## Recovering deleted items

If users accidentally delete a message, you can enable items recovery and recover the deleted items before they are cleared-out.

You can recover:

- Email messages
- Events
- Contacts
- Notes
- Tasks

### Enabling deleted items recovery

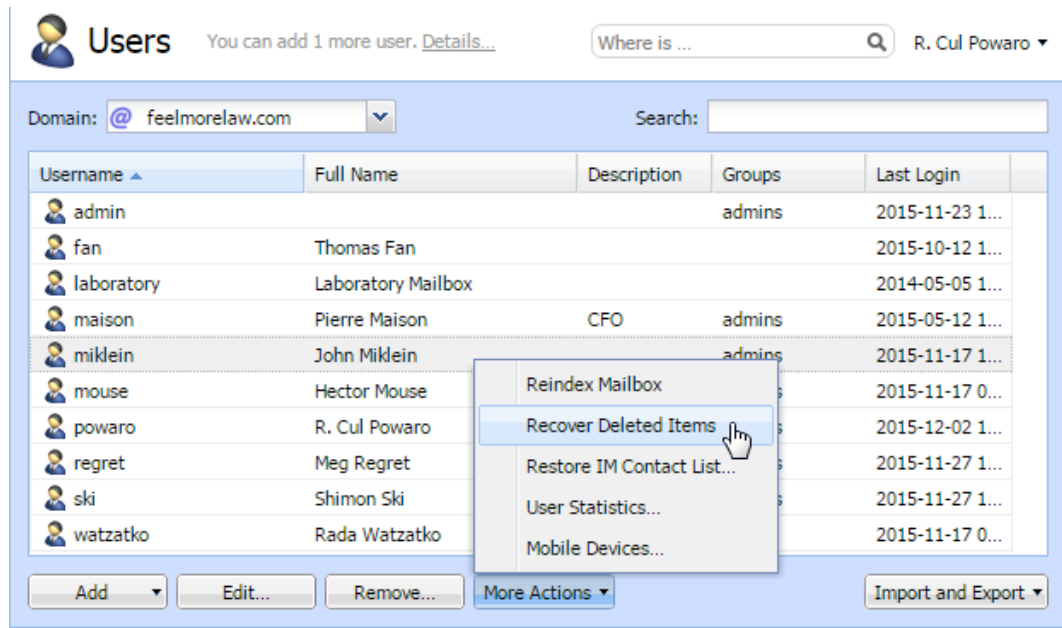
1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Double-click the domain and go to the **Messages** tab.
3. Select the **Keep deleted items for** option.
4. Specify the number of days for which the items will be available after deletion.
5. Click **OK**.

### Recovering deleted items

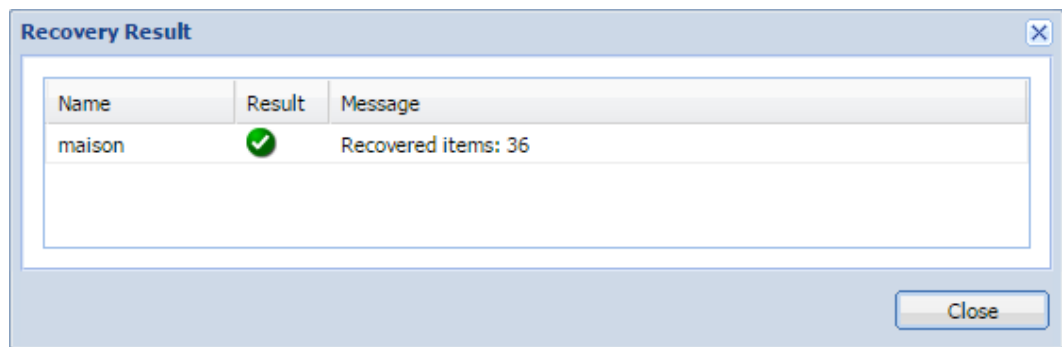
Once recovery is enabled for the user's domain, follow these steps to recover their items:

1. In the administration interface, go to the **Accounts** → **Users** section.
2. Select the user and click on **More Actions** → **Recover Deleted Items**.

## Maintaining user accounts in Kerio Connect



3. Click **Close** to close the result of the process.



4. Users find the recovered items in their **Trash** folder.



If you disable item recovery for a domain, the **Recover Deleted Items** button is not active for users from this domain. If you are using [archiving](#), you can look up the deleted items in an archive.

## Limiting the size of outgoing messages

To avoid overloading your server with large email attachments, you can limit the size of outgoing messages;

- Particular domain

- Individual users
- From Kerio Connect Client (HTTP POST size)



If both are configured, settings per user are applied.  
You can also use server filters — see [Filtering messages on the server](#).

### Per domain

1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Double-click the domain and switch to the **Messages** tab.
3. Select the **Limit outgoing message size to** option.
4. Specify the maximum size of the outgoing messages for this domain.
5. Click **OK**.

### Per user

By default, new users inherit settings from their domain.

To change the settings for individual users:

1. In the administration interface, go to the **Accounts** → **Users** section.
2. Double-click the user for whom you want to limit the message size.
3. On the **Messages** tab in the **Maximum message size** section, select the **Use custom settings for this user** option.
4. Specify the limit for outgoing messages for the user.



Select **Do not limit message size** to disable any limits.

5. Click **OK**.

## Maintaining user accounts in Kerio Connect

---

**Maximum message size**

Use the limit defined for this domain

Limit outgoing message size to (overrides the domain limit):

Do not limit message size

### From Kerio Connect Client

Each new message composed in [Kerio Connect Client](#) is sent to Kerio Connect via HTTP POST requests. Each request contains the message body, all headers and attachments.

You can limit the size of the HTTP POST request (this also limits the message size).

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

See [Installing Kerio Connect](#) for details about restarting.

### Limiting the size of incoming messages delivered via SMTP

1. In the administration interface, go to **Configuration** → **SMT server** → **the Security Options tab**.
2. Select the **Limit maximum incoming SMTP message size to** option.
3. Specify the maximum size of incoming messages.
4. Click **Apply**.

**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)

Max. number of recipients in a message:

Max. number of failed commands in a SMTP session:

Limit maximum incoming SMTP message size to:

Maximum number of accepted Received headers (hops):

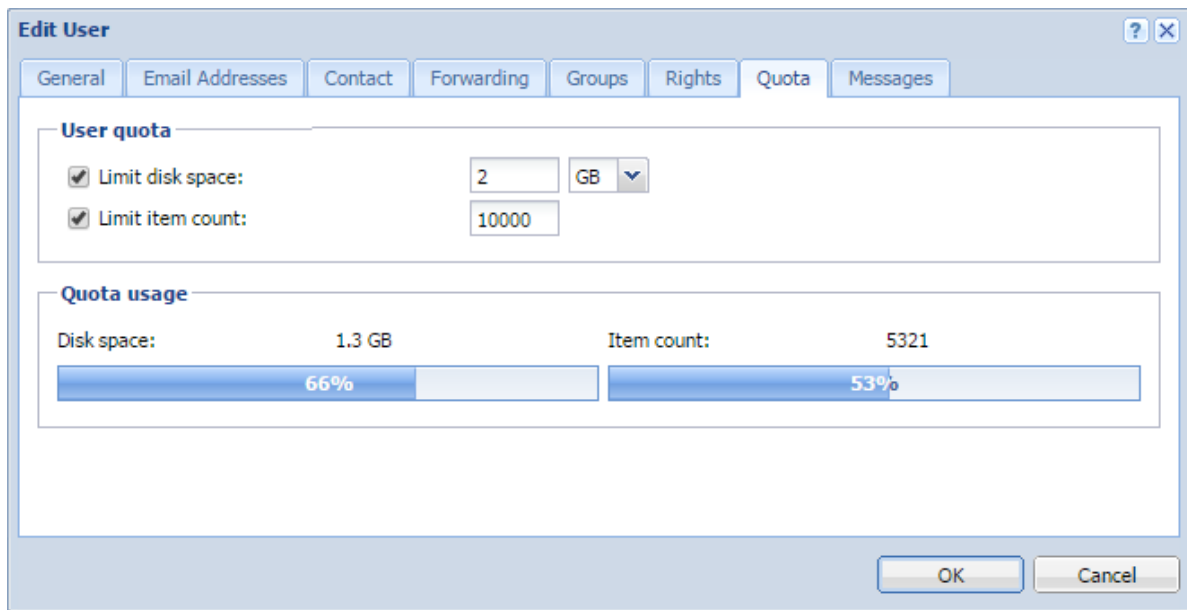


You can also use server filters — see [Filtering messages on the server](#).

## Limit the size of user mailboxes

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

1. In the administration interface, go to the **Accounts** → **Users** section.
2. Double-click the user and switch to the **Quota** tab.
3. To limit the size of the user's mailbox, select **Limit disk space** and specify the size.
4. To limit the number of items in the user's mailbox, select **Limit item count** and specify the number of items.
5. Click **OK**.



## 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 free up some space.

To set the limit for notifying users:

1. In the administration interface, go to **Configuration** → **Advanced Options** → the **Store Directory** tab.
2. In the **User quota** section, specify:

## Maintaining user accounts in Kerio Connect

---

- The **Warning limit**
- The frequency in which Kerio Connect sends notifications to the user
- The email address to which Kerio Connect sends a message if a user reaches the quota

3. Click **OK**.

**User quota**

Warning limit:  %

If the warning limit is reached, send a message to the user:

If quota is reached, send a message to this address:



# Creating mailing lists in Kerio Connect

---

## Overview

Mailing lists are group email addresses. Kerio Connect distributes messages sent to a mailing list 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 by hiding the sender's email address
- Disallowing messages with certain features, for example, messages without a subject

## Special mailing list addresses

Users perform all mailing list actions, such as, moderating, subscribing, by sending empty messages to special addresses.

Special addresses consists of the **mailing list name** and a **special suffix**:

`<mailing_list_name>-<suffix>@<domain>`

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 the **Accounts** → **Mailing Lists** section and select a domain in which you want to create a mailing list.

2. Click **Add**.

3. Type a name for the mailing list.

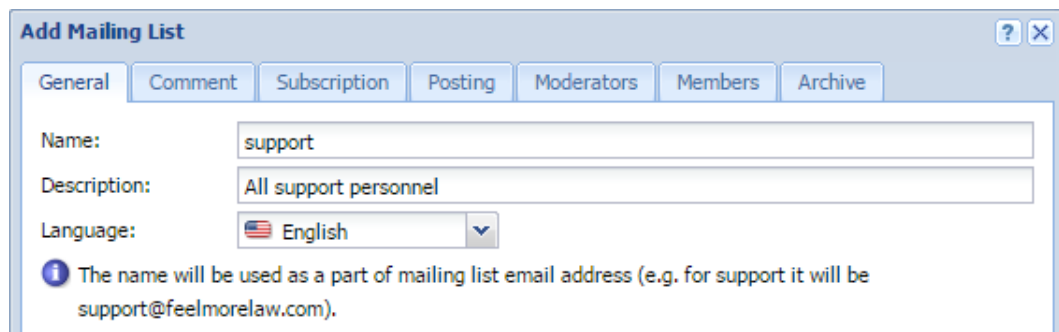
The mailing list name must not:

- Contain [suffixes](#) used for special functions
- Contain the **.** (dot) symbol
- Be identical to other username or [alias](#)

4. Select a 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.



**Add Mailing List**

General | Comment | Subscription | Posting | Moderators | Members | Archive

Name:

Description:

Language:

**i** The name will be used as a part of mailing list email address (e.g. for support it will be support@feelmorrelaw.com).

5. (Optional) On the **Comment** tab, type a text for a welcome message.

Kerio Connect appends this text to a first message sent to new members.

6. (Optional) Type a text that Kerio Connect appends to each message sent to the mailing list.

7. On the **Subscription** tab, select the subscription policy.

You can allow subscriptions via a special email address (see above).

8. On the **Members** tab, click **Add** to add users to the mailing list.

You can select users from Kerio Connect domains, type their email addresses manually, or import them from a CSV file.

Separate the items in the CSV file by commas (,) or semicolons (;). The file may look like this:

```
Email;FullName
miklein@feelmorelaw.com;John Miklein
rcul@powaro.com;R. Cul Powaro
```

9. (Optional) To archive the mailing list, select **Maintain archive of this mailing list** on the **Archive** tab.

See the [Accessing the mailing list archive](#) section below for additional information about accessing the .

10. Save the settings.

Now users can subscribe and send message to mailing lists.

## 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 want the archive to be accessible publicly (to anybody), you must allow anonymous access to the [NNTP service](#):

1. Go to the **Configuration** → **Services** section.
2. Double-click **NNTP** and on the **Access** tab, select the **Allow anonymous access** option.
3. Click **OK**.

## Troubleshooting

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

# Importing users in Kerio Connect

---

## Import options

In Kerio Connect you can import users from:

- CSV files
- Directory service

Importing creates [local user accounts](#).



Read [Creating mailing lists in Kerio Connect](#) for detailed information on importing users to mailing lists.

## Importing from CSV files

### Creating CSV files

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

Individual fields can be separated in either of two ways:

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

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

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

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



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

### Importing from CSV files

To import the file:

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

### Importing from a directory service

#### Windows NT domain



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

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



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

This displays a list of users.

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

#### Microsoft Active Directory

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

## Importing users in Kerio Connect

---

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



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

This displays a list of users.

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

### Novell eDirectory

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



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

This displays a list of users.

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

### Troubleshooting

To log information about the import, enable the **Directory Service Lookup** option in the [Debug log](#) before the import.

# Exporting users in Kerio Connect

---

## What can be exported

In Kerio Connect, administrators with at least [read rights](#) can export lists of

- [Users from a domain](#)
- [Members of a group](#)
- [Members of a mailing list](#)

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

## Exporting users from a domain

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

The file names use this format: users\_<DomainName>\_<date>.csv

## Exporting users from a group

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

The file names use this format: users\_<DomainName>\_<GroupName>\_<date>.csv

### Exporting users from a mailing list

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

The file names use this format: users\_<DomainName>\_<MailingListName>\_<date>.csv



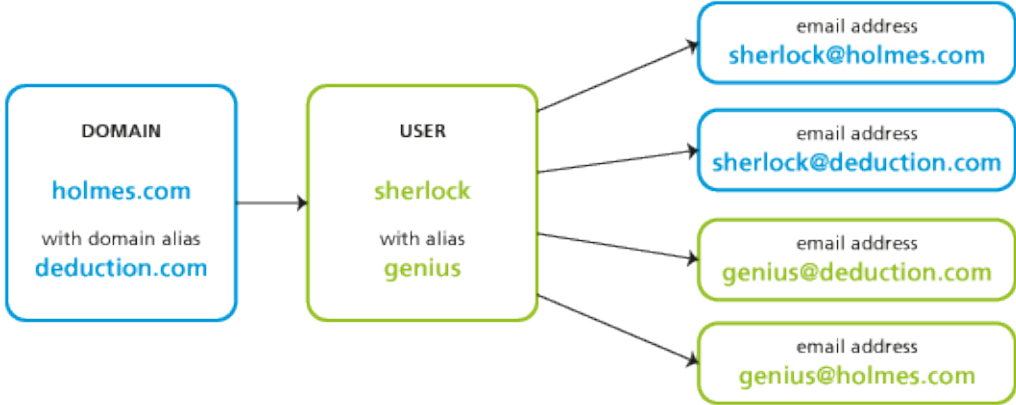
# Creating aliases in Kerio Connect

## Aliases in Kerio Connect

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

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

You can combine both types of aliases:



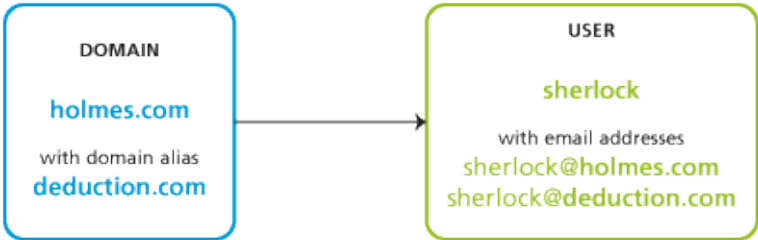
## Domain aliases

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

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

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

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



## Creating aliases in Kerio Connect

---



Once you [rename a domain](#), an alias is automatically created from the original name.

### Creating domain aliases

To create a domain alias in Kerio Connect:

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



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

### Username aliases

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

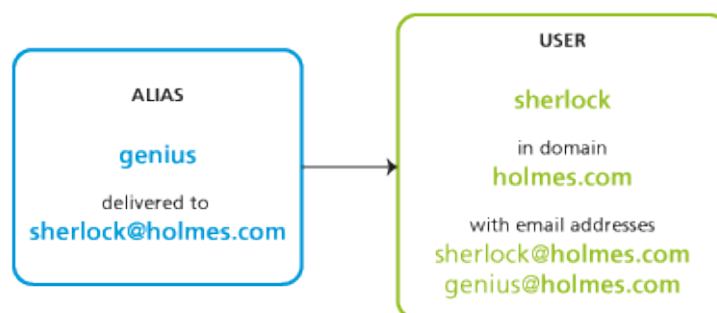
Aliases can be linked to:

- a user
- a group
- an existing alias



If a message is sent to a username, it is marked by a flag so that the aliases not get looped. If such message arrives to the username marked by the flag, it will be stored in the mailbox that belongs to the last unmarked alias.

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



If users have username aliases defined, they can [select from which addresses they want to sent their messages](#).

### *Creating username aliases*

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

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

The alias may contain the following characters:

- a-z — all lower-case letters (no special characters)
- A-Z— all upper-case letters (no special characters)
- 0-9 — all numbers
- . — dot
- - — dash
- \_ — underscore
- ? — question mark
- \* — asterisk

4. The messages can be delivered to:
  - an email address — type the email address or click **Select**
  - public folder — select the public folder form the menu



This item is active only in case at least one email [public folder](#).

5. Confirm and save.

## Creating aliases in Kerio Connect

### **Example:**

Mr Sherlock Holmes has an account with username **sherlock** in domain **holmes.com** (therefore, his email address is **sherlock@holmes.com**).

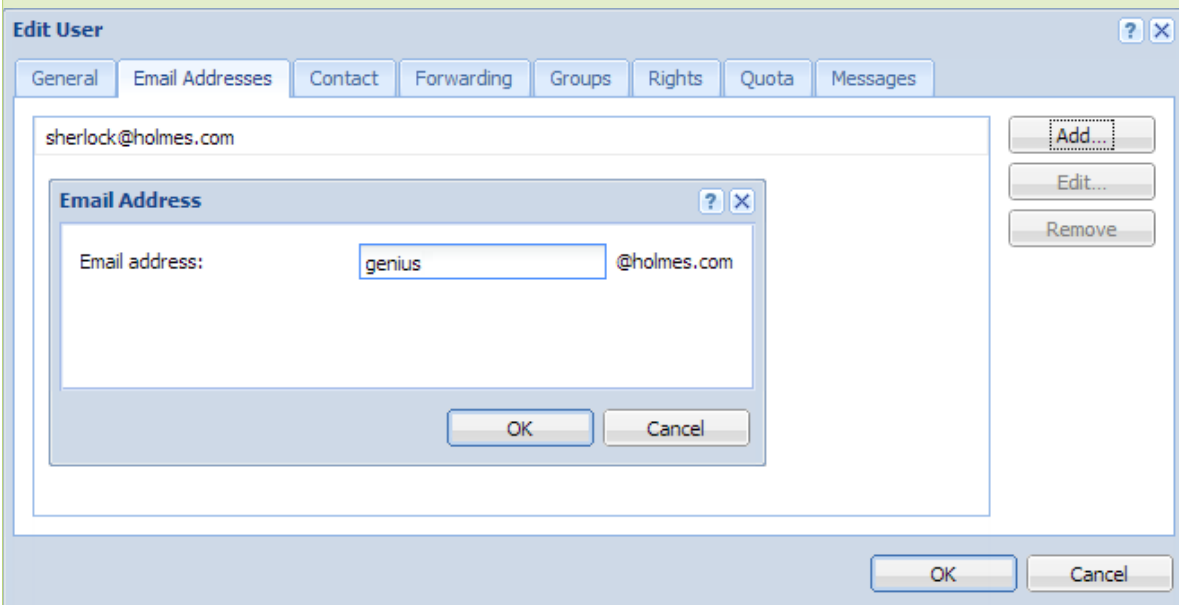
Since he finds himself very smart (what else), he wants another email address — **genius@holmes.com**. The problem is he does not want to manage two accounts.

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:



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:

?i11 → will be sent to sherlock

#### **Alias as a protection against wrong spelling — numerous characters**

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

\*erlock → will be sent to sherlock

### ***Checking aliases***

In Kerio Connect you can verify all the aliases.

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

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

# Configuring resources in Kerio Connect

---

## Overview

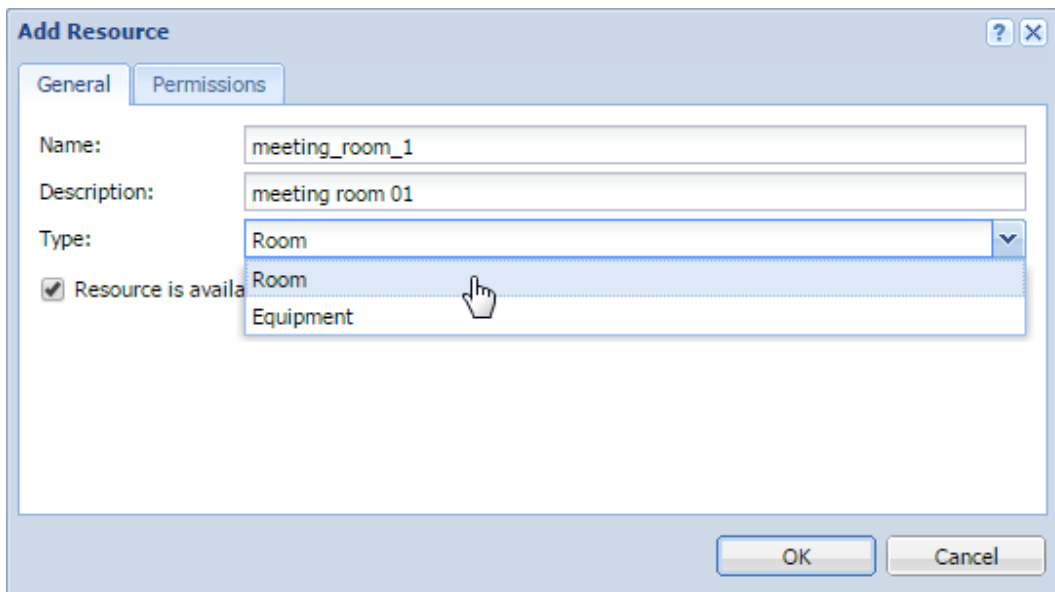
Resources are meeting rooms and other facilities, such as conference rooms, cars, parking lots.

You can [schedule resources](#) in an email client when creating new events in calendars.

Resources do not count against your [license](#).

## Creating new resources

1. In the administration interface, go to **Accounts** → **Resources**.
2. Select a domain and click **Add**.
3. Type a name for the resource and select the resource type.
  - **Room** — The resource is available as a room/location or as an attendee
  - **Equipment** — The resource is available as an attendee



The screenshot shows the 'Add Resource' dialog box with the following details:

- Title:** Add Resource
- Tabs:** General (selected), Permissions
- Name:** meeting\_room\_1
- Description:** meeting room 01
- Type:** Room (selected in dropdown menu)
- Resource is available:**
- Buttons:** OK, Cancel

4. Select the **Resource is available** option.
5. On the **Permissions** tab, add users who can schedule the resource.  
By default, permissions to use resources are set to all users from the domain. You can add single users, groups, a whole domain, or a whole server.
6. On the **Permissions** tab, select a reservation manager.  
By default, the domain administrator is the reservation manager. You can add single users, groups, a whole domain, or a whole server.  
For details, see the **Assigning reservation managers** section below.
7. Click **OK**.

Kerio Connect publishes all resources to a public calendar.

### Assigning reservation managers

Each resource has a reservation manager. Reservation managers are users who manage the resource calendar.

In Kerio Connect Client, resource managers can:

- Add events directly to the resource calendars, and edit them
- Delete any event in the resource calendar

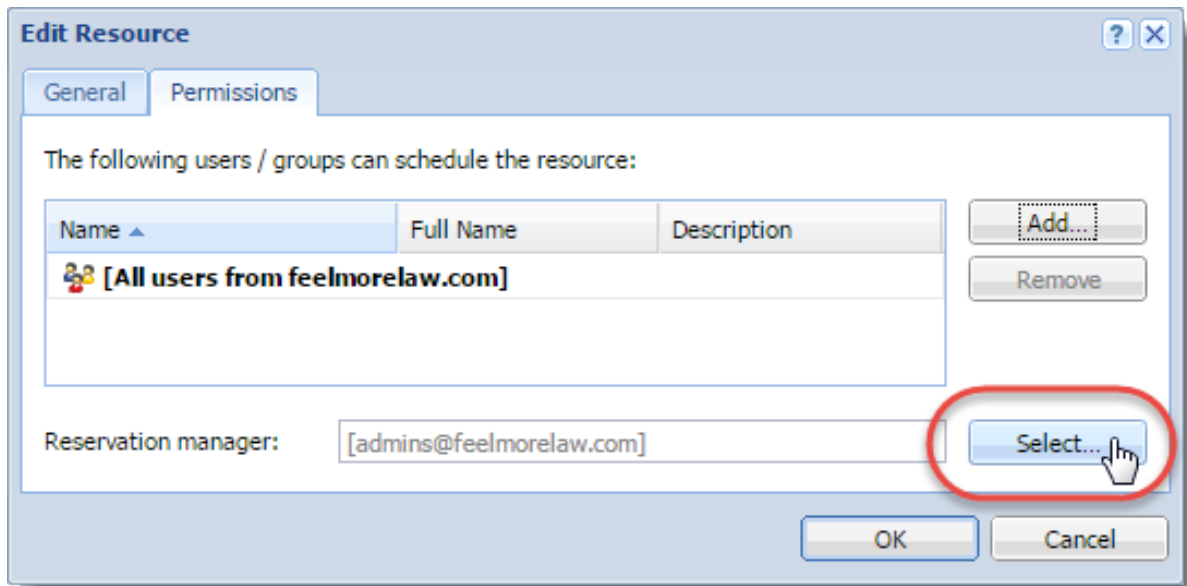


In Kerio Connect 9.0.2 and older, resource managers can only delete other users' reservations for resources.

By default, the domain administrator is the reservation manager. To change the reservation manager:

1. In the administration interface, go to **Accounts** → **Resources**.
2. Double-click a resource and switch to the **Permissions** tab.
3. Click **Select** in the **Reservation manager** section.  
Kerio Connect displays a list of all users and groups.
4. Switch to the desired domain and select a user as the reservation manager.  
You can add single users, groups, a whole domain, or a whole server.
5. Click **OK**.

## Configuring resources in Kerio Connect



### Removing resources

You can remove resources either temporarily or permanently:

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

### Using resources

Read the [Scheduling resources in Kerio Connect Client](#) article for details.

### Troubleshooting

If any problem with resources occurs, consult the [Debug log](#): right-click in the Debug log area and enable **Resource Service**.



# Monitoring Kerio Connect

---

## Overview

In Kerio Connect, you 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

All messages sent or received through Kerio Connect are stored in Kerio Connect installation directory in folder `store/queue`.

Kerio Connect stores the messages as the following files:

- The `*.eml` file is the message itself
- The `*.env` file is the SMTP envelope of the message

## Viewing the message status

You can see the messages in **Status** → **Message Queue** → **Messages in Queue**.

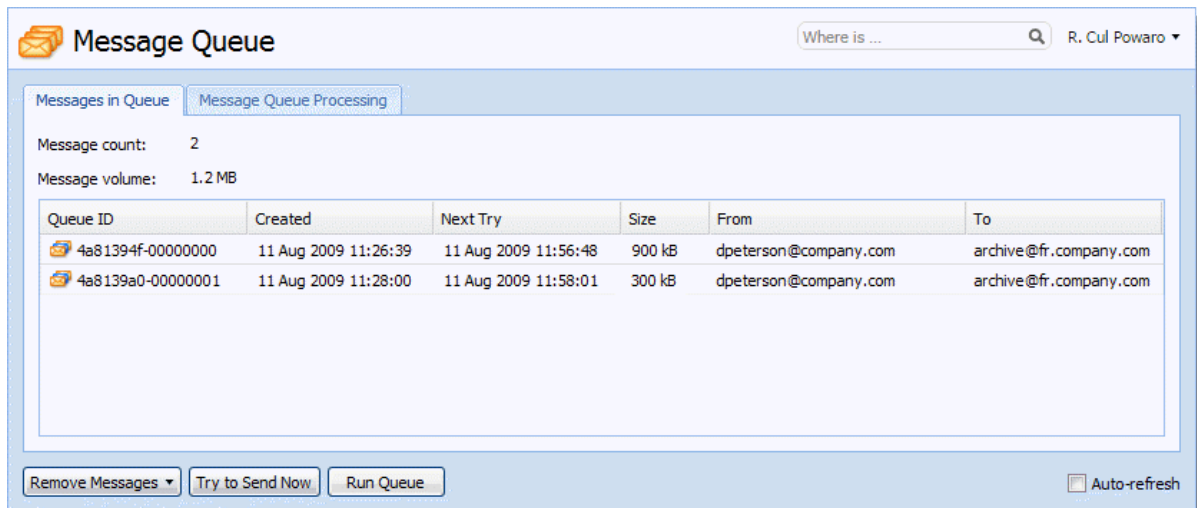
In this section you can:

- Verify whether messages are sent/received properly
- Remove messages from the message 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`.

## Monitoring Kerio Connect



The screenshot shows the 'Message Queue' interface. At the top, there is a search bar with the text 'Where is ...' and a magnifying glass icon, and a user name 'R. Cul Powaro'. Below the search bar, there are two tabs: 'Messages in Queue' (selected) and 'Message Queue Processing'. The main area displays the following information:

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

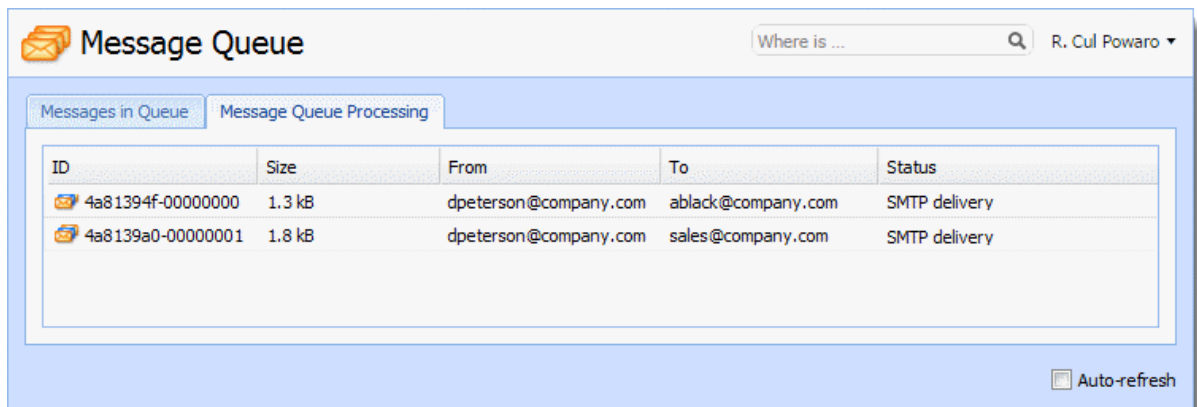
At the bottom, there are three buttons: 'Remove Messages', 'Try to Send Now', and 'Run Queue'. On the far right, there is a checkbox labeled 'Auto-refresh'.

### Processing message queue

When processing the message queue, Kerio Connect creates a new process for each message. This process reports all actions (such as delivery to a local mailbox or a remote SMTP server and antivirus control) and then terminates.

Multiple processes can run simultaneously.

You can display the status of currently processed messages in **Status** → **Message Queue** → **Messages Processing**.



The screenshot shows the 'Message Queue' interface with the 'Message Queue Processing' tab selected. The main area displays the following information:

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

At the bottom right, there is a checkbox labeled 'Auto-refresh'.

### Configuring message queue parameters

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

- The maximum number of messages being delivered at a time
- The interval in which Kerio Connect retries to deliver messages

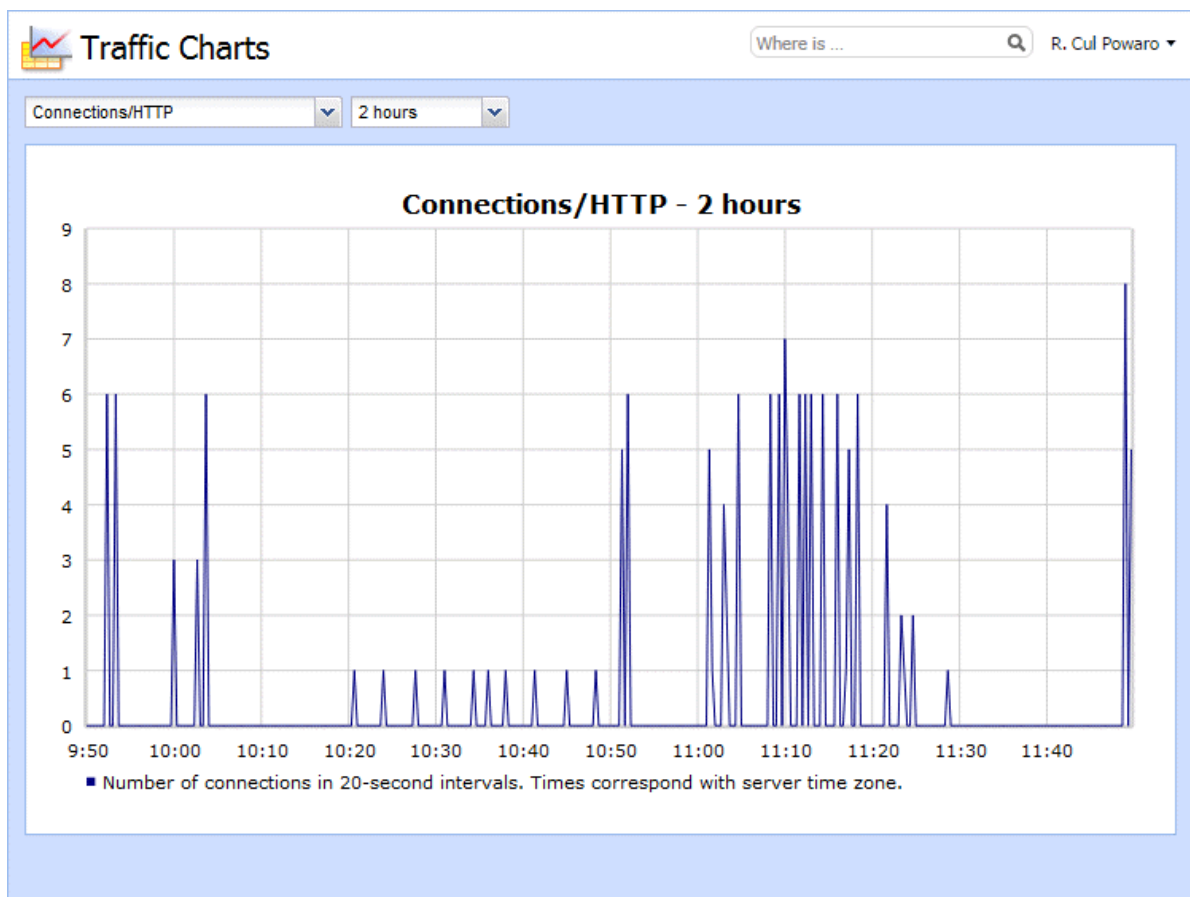
- The interval in which Kerio Connect sends the undelivered messages to senders
- The interval in which senders are notified that their messages have not been delivered



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

## Traffic charts

In the **Status** → **Traffic Charts** section in 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.

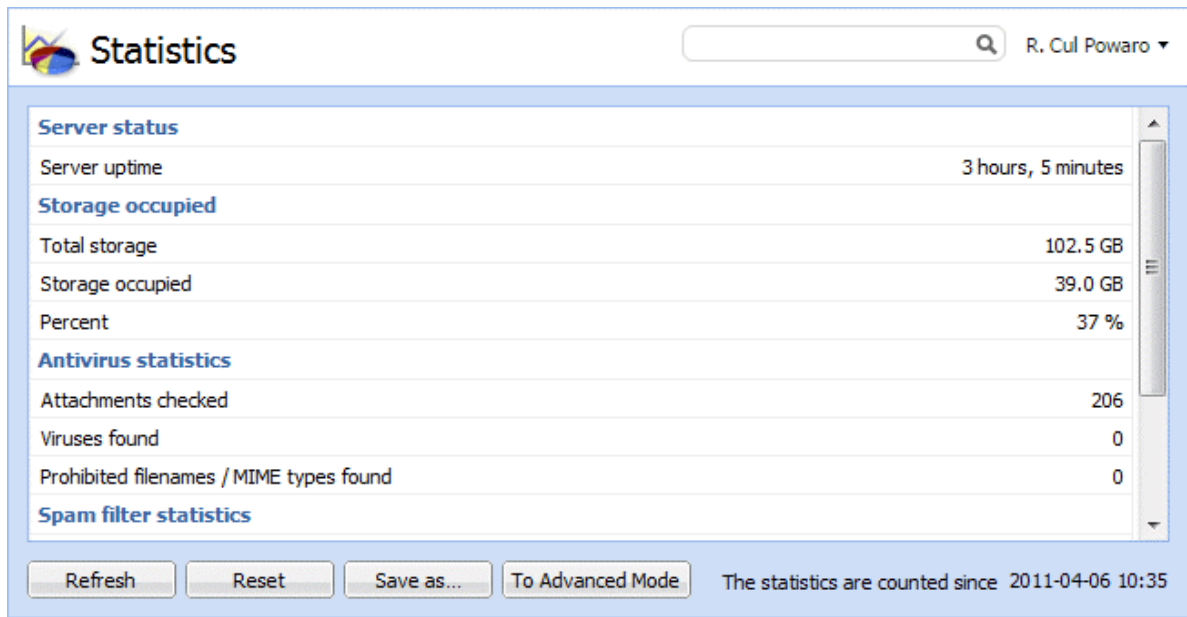


## Viewing statistics

In the **Status** → **Statistics** section, you can view the Kerio Connect statistics.

The statistics are divided into groups, for example, **Storage Occupied**, **Messages sent to parent SMTP server**, **Client POP3 statistics**, and so on.

## Monitoring Kerio Connect



**Statistics** R. Cul Powaro

**Server status**

Server uptime	3 hours, 5 minutes
---------------	--------------------

**Storage occupied**

Total storage	102.5 GB
Storage occupied	39.0 GB
Percent	37 %

**Antivirus statistics**

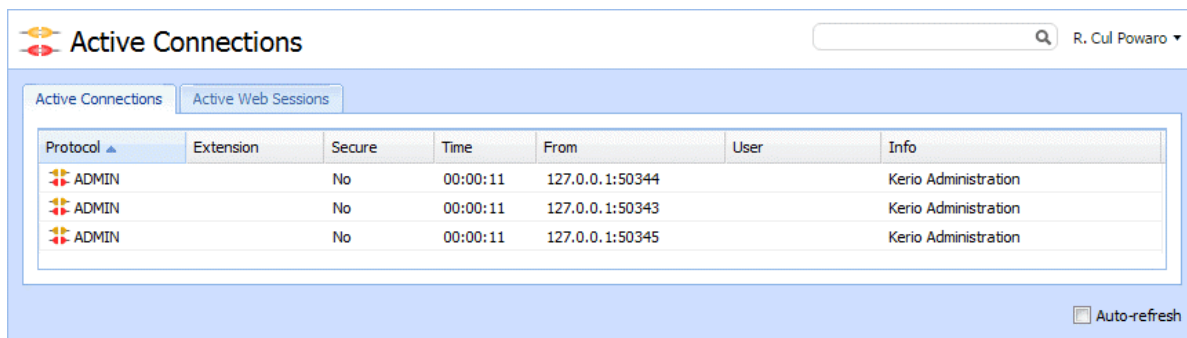
Attachments checked	206
Viruses found	0
Prohibited filenames / MIME types found	0

**Spam filter statistics**

Refresh Reset Save as... To Advanced Mode The statistics are counted since 2011-04-06 10:35

## Displaying users currently connected to Kerio Connect

In the **Status** → **Active Connections**, Kerio Connect displays all network connections established with the server.



**Active Connections** R. Cul Powaro

Active Connections Active Web Sessions

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

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

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

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

In **Status** → **System Health**, Kerio Connect displays the current usage of CPU, RAM and the disk space of the computer where Kerio Connect is running.

### Time interval

Select the time interval in which to display the CPU load and RAM usage.

### CPU

Timeline of the computer's CPU load. Short time peak load rates can be caused, for example, by the network activity.

### RAM

RAM usage timeline.

### Storage usage

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

### Tasks

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

# Services in Kerio Connect

---

## Setting service parameters

You can set parameters for Kerio Connect services in the **Configuration** → **Services** section. By default, all services are running on their standard ports.

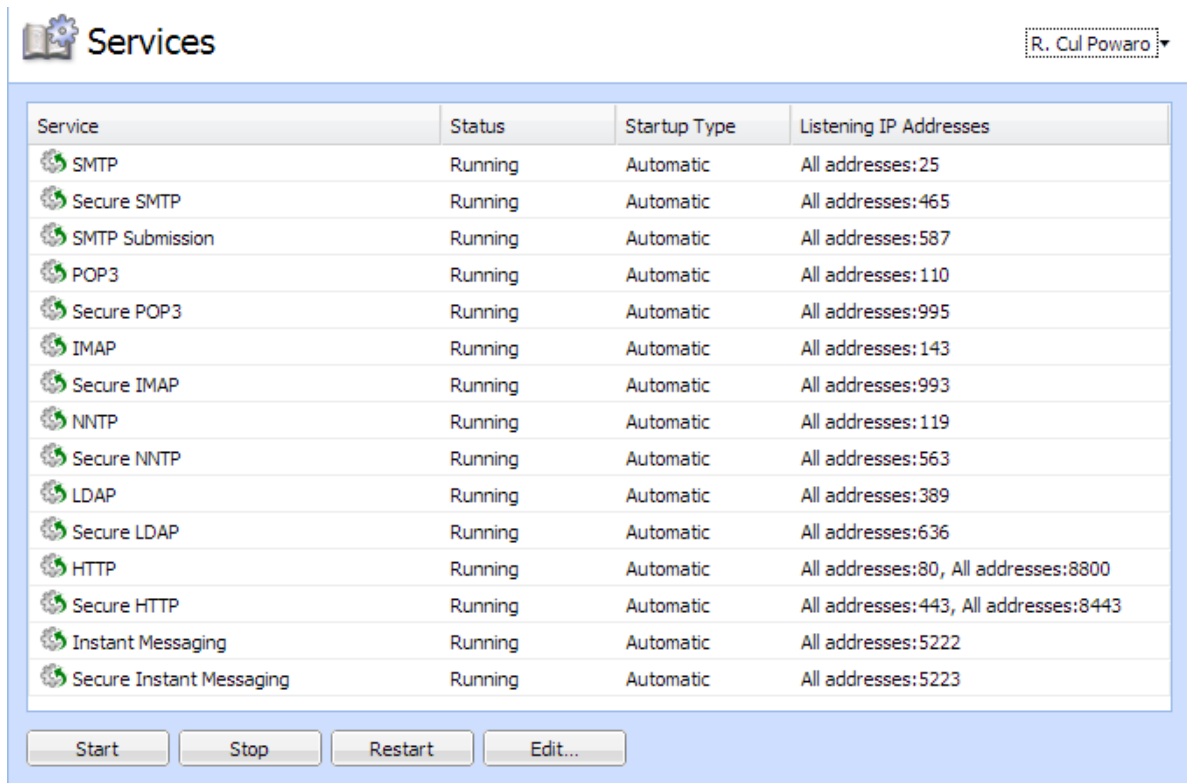


For security reasons, enable only the services you know will be used. See [Configuring your firewall](#) for additional information.

For each service, you can:

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

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



### Port collisions

If any service 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 (not recommended if you reserve IP addresses dynamically, for example, via DHCP)

### Service types

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

#### SMTP

The [SMTP](#) protocol server sends outgoing email messages, receives incoming messages and messages created via mailing lists in Kerio Connect.

You can use two methods for encrypting the SMTP traffic:

- **SMTP on port 25** with STARTTLS if [TLS](#) encryption is supported.

The 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 send email out of the network. SMTPS on port 465 is usually allowed.

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

### POP3

**POP3** protocol server allows users to retrieve messages from their accounts. It can be used as an alternative to IMAP for access messages.

### IMAP

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

### NNTP

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

### LDAP

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

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

### HTTP

HTTP protocol is used to:

- Access user mailboxes in Kerio Connect Client
- Access the Free/Busy server



- Automatically update Kerio Outlook Connector (Offline Edition)
- Synchronize via ActiveSync or NotifyLink
- Publish calendars in iCal format
- (HTTPS) Access [Kerio Connect administration](#)
- (HTTPS) Access user mailboxes in Kerio Connect Client (if secured connection is required)

### Instant Messaging

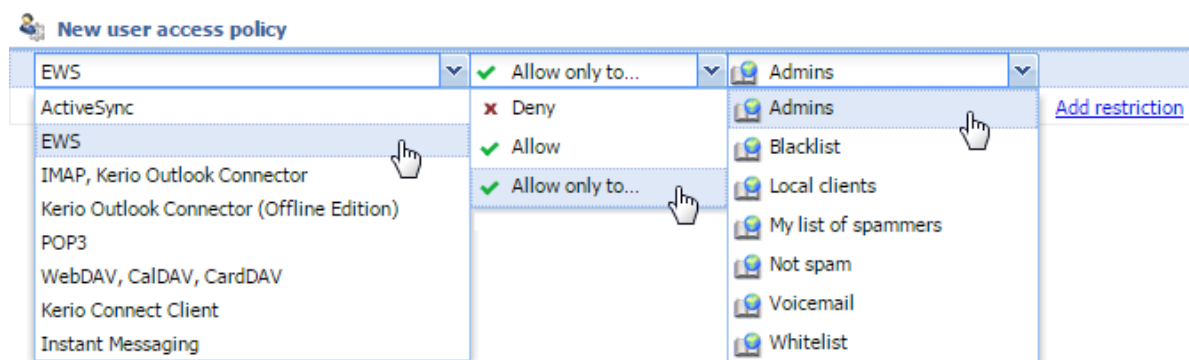
[Instant messaging](#) allows users to chat with other users in or outside of their domain.

### Restricting access to some services

To restrict access to any service for any users, you can define **User Access Policies**. 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 **Configuration** → **Definitions** → **User Access Policies**.
2. Click **Add Policy**.
3. Type a name for the policy.
4. Click the **Add restriction** link and select a protocol.
5. Click **Allow/Deny/Allow only to** to set the access.  
You can add multiple restriction.
6. Set access for the remaining (unselected) protocols.
7. Click **Apply**.



To remove a restriction, select it and click **Remove**.

To remove a policy, select it and click **Remove**.

### Assigning access policies to users

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

1. In the administration interface, go to **Accounts** → **Users**.
2. Double-click a user and go to the **Rights** tab.
3. Select an **Access policy** from the drop-down list.
4. Click **OK**.

## Troubleshooting

If any problem regarding services occurs, consult the [Debug log](#). Right-click the Debug log area, click **Messages**, and select the appropriate message type (service to be logged):

### SMTP

When problems in the communication between the SMTP server and a client arise, use the **SMTP Server** and **SMTP Client** options.

### POP3

When problems with the POP3 server arise, enable the **POP3 Server** option.

### IMAP

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

### NNTP

When problems with the NNTP server arise, enable the **NNTP Server** option.

### LDAP

When problems with the LDAP server arise, enable the **LDAP Server** option.

### HTTP

- The **HTTP Server** option enables logging of HTTP traffic on the server's side.
- The **WebDAV Server Request** option enables logging of queries sent from a WebDAV server. Used it for *Microsoft Entourage* or *Apple Mail* where problems with Exchange accounts arise.
- The **PHP Engine Messages** option helps solving problems with the Kerio Connect Client interface.

**Instant messaging**

When problems with the IM server arise, enable the **Instant Messaging Server** option.

Too many log messages may slow down your server. Once you solve your problem, disable the logging.

# Configuring the SMTP server

---

## Overview

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

If an unprotected SMTP server is accessible from the Internet, anyone can connect and send email messages through Kerio Connect. For example, spammers can use your SMTP server to send out spam messages, and as a result your company could be added to spam blacklists.



Kerio Connect does not check messages from the allowed IP addresses with [SPF](#), [Caller ID](#) and SpamAssassin.

## Configuring the SMTP server

To specify who can send messages from outside your server:

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

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



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

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

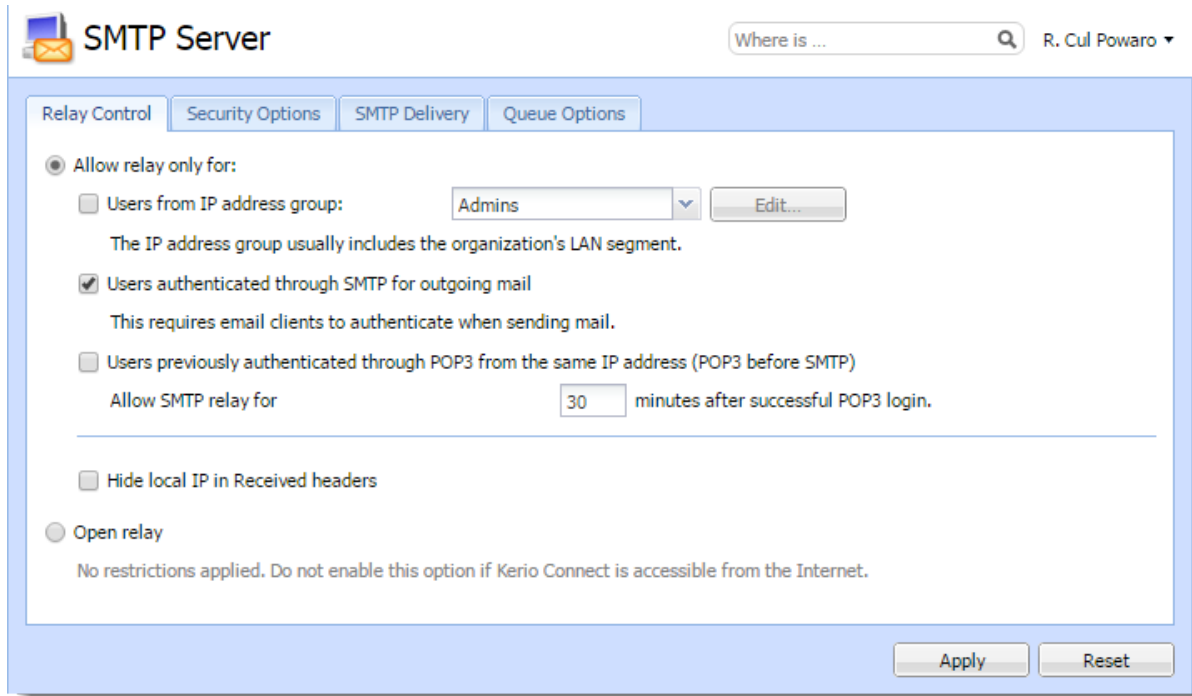


Figure 1 SMTP server

## Sending outgoing messages through multiple servers



New in Kerio Connect 9!

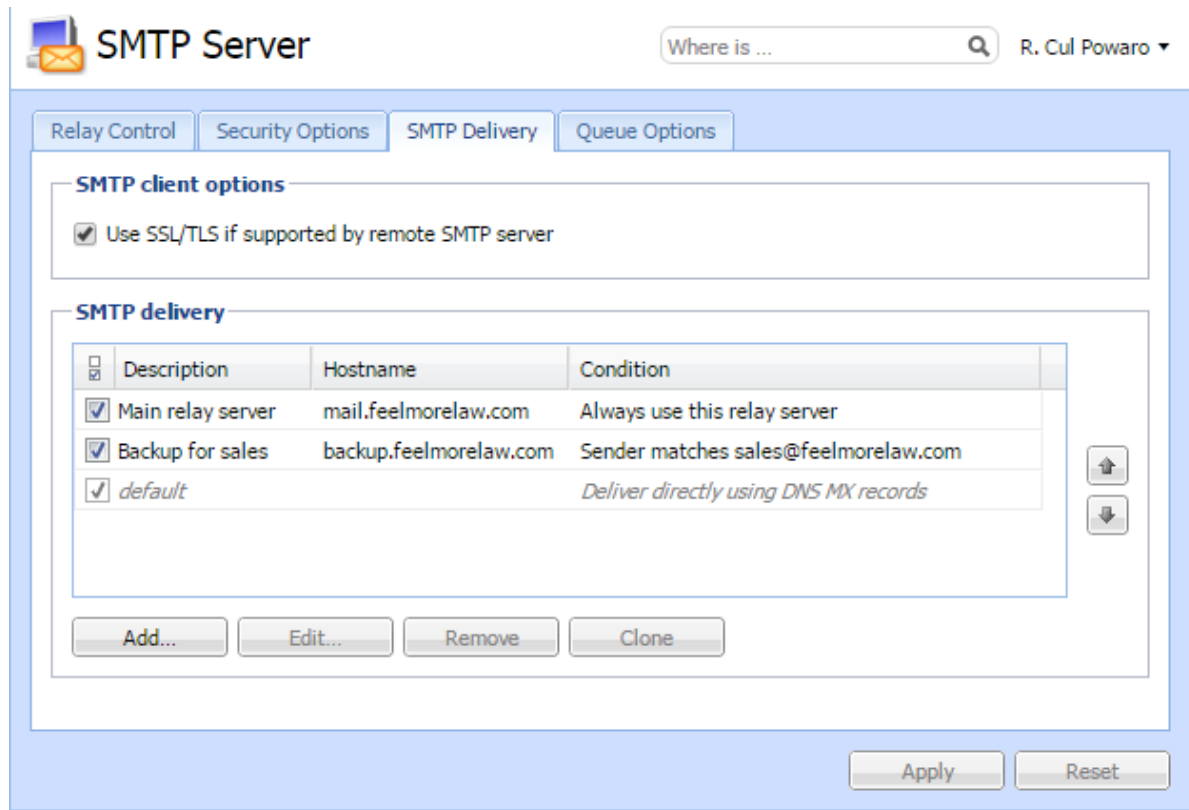
In Kerio Connect 8 and older, you can define only a single SMTP relay server.

Kerio Connect can deliver messages:

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

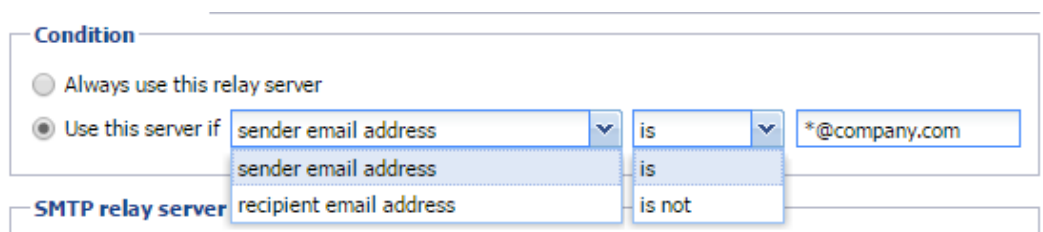
For example, Kerio Connect can use different SMTP relay servers for different domains in Kerio Connect.

## Configuring the SMTP server

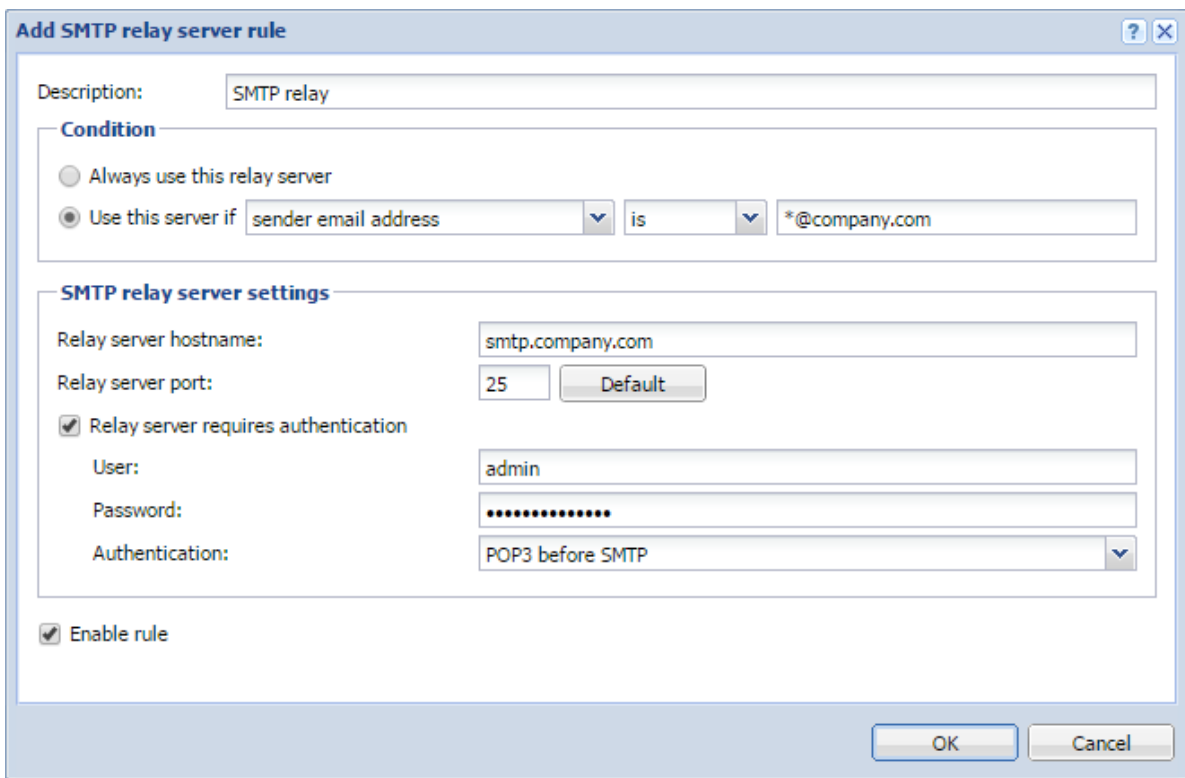


To define a SMTP relay server:

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

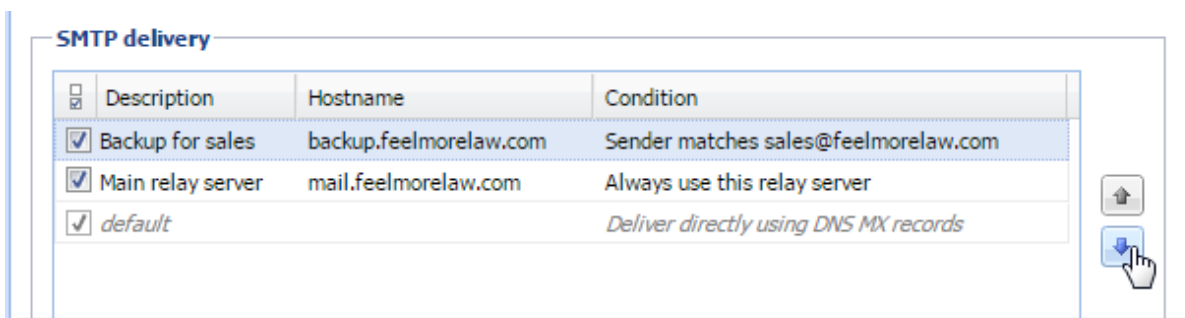


6. Type the relay server hostname and the server port.
7. If the server requires authentication, select **Relay server requires authentication** and type the username and password, and specify the authentication method.
8. Click **OK**.
9. Click **Apply**.



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

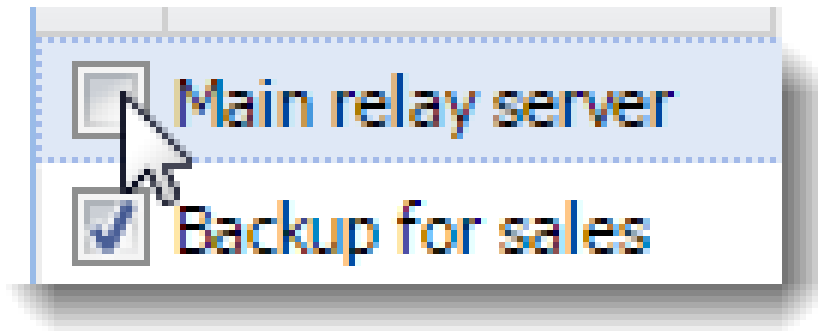
To change the order of the rules, select a rule and use the arrows on the right side to move it up or down.



## Configuring the SMTP server

---

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



## Securing the SMTP server

For information about secure SMTP server, read [Securing the SMTP server](#).

## Troubleshooting

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



# Securing the SMTP server

---

## Overview

In Kerio Connect, you can configure the SMTP server to protect Kerio Connect from misuse. Anyone can connect to an unprotected SMTP server from the Internet and send email messages through Kerio Connect. For example, spammers can use your SMTP server to send out spam messages, and as a result your company could be added to spam blacklists.



For detailed information about configuring the SMTP server, read [Configuring the SMTP server](#).

## Securing the SMTP server

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

1. In the administration interface, go to the **Configuration** → **SMTP Server** → **the Security Options tab** section.
2. For a single IP address you can set the following IP address based limits:
  - **Max. number of messages per hour** discards any new message sent from the same IP address after reaching the set limit.
  - **Max. number of concurrent SMTP connections** gives protection from denial of service, or [DoS](#), attacks which overload the server.
  - **Max. number of unknown recipients** protects Kerio Connect from [directory harvest](#) attacks, in which an application connects to your server and uses the dictionary to generate possible usernames.
3. Enable the **Do not apply these limits to IP address group** option and select a group of trusted IP addresses that are not affected by the above settings.

The screenshot shows the 'SMTP Server' configuration window. At the top, there is a search bar with 'Where is ...' and a magnifying glass icon, and a user name 'R. Cul Powaro'. Below the search bar are four tabs: 'Relay Control', 'Security Options', 'SMTP Delivery', and 'Queue Options'. The 'Security Options' tab is selected. Under the 'IP address based limits' section, there are four checked options with input fields: '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), and 'Do not apply these limits to IP address group:' (Local clients). An 'Edit...' button is next to the dropdown menu.

## Securing the SMTP server

---

4. You can further protect Kerio Connect using several additional:

- To block senders with fictional email addresses, enable **Block if sender's domain was not found in DNS**
- To block incorrectly configured DNS entries, enable **Block messages if client's IP address has no reverse DNS entry (PTR)**
- To block spam messages sent to a large number of recipients, enable **Max. number of recipients in a message**
- Spammers often send messages using applications that connect to SMTP servers and ignore its error reports. The **Max. number of failed commands in a SMTP session** option protects against these applications by closing the SMTP connection automatically after the defined number of failed commands.
- To block messages with large attachments that can overload your server, enable **Limit maximum incoming SMTP message size to**.

**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)
- Max. number of recipients in a message:
- Max. number of failed commands in a SMTP session:
- Limit maximum incoming SMTP message size to:
- Maximum number of accepted Received headers (hops):

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

6. Click **Apply**.

## Troubleshooting

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

# Configuring POP3 connection

---

## About POP3

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

## Defining remote mailboxes

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



For the password, use 119 characters or fewer.

Kerio Connect can:

- deliver the messages to a specific address, or
- use predefined [sorting rules](#)

## Configuring POP3 connection

---

**Add POP3 Account**

General | **Advanced**

**POP3 account**

POP3 server:

POP3 username:

Password:

Description:

**Sorting and delivery**

Deliver to address:  
 

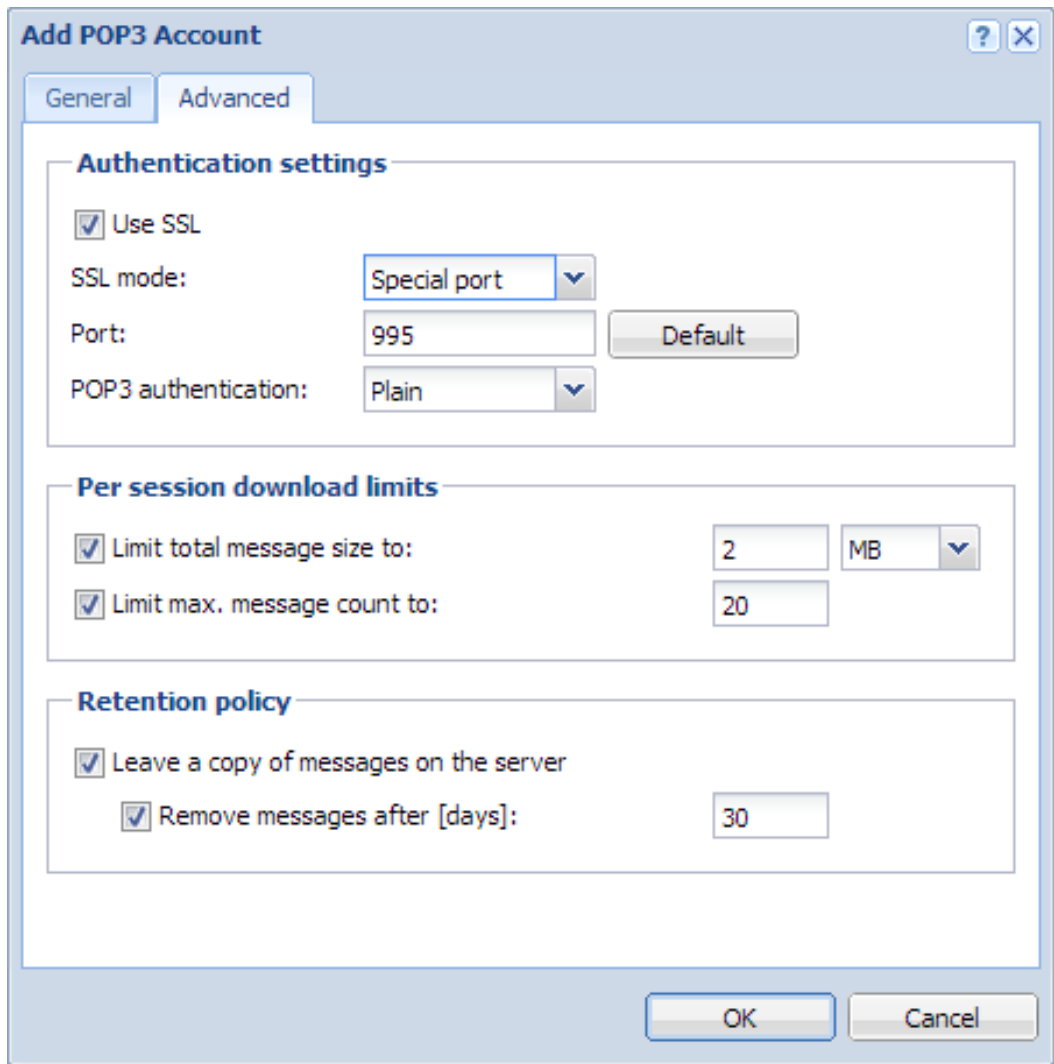
Use sorting rules:  
Preferred header:  ▼

Drop duplicate messages

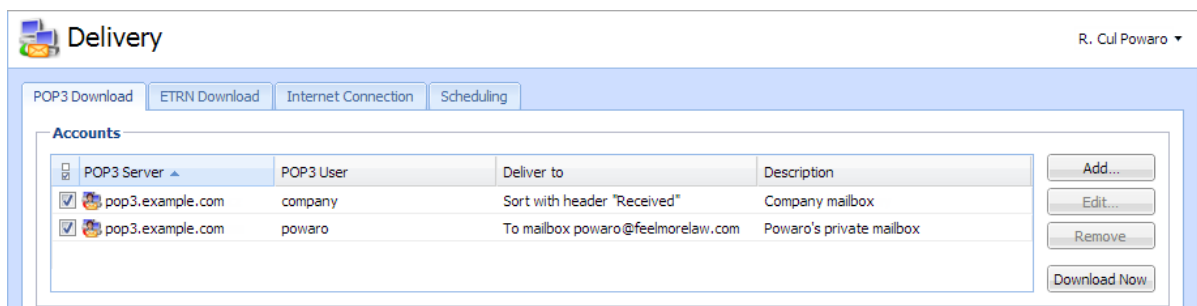
Enable POP3 account

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

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



5. Click **OK**.



## Configuring POP3 connection

---

### Sorting rules

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

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



**Add Sorting Rule**

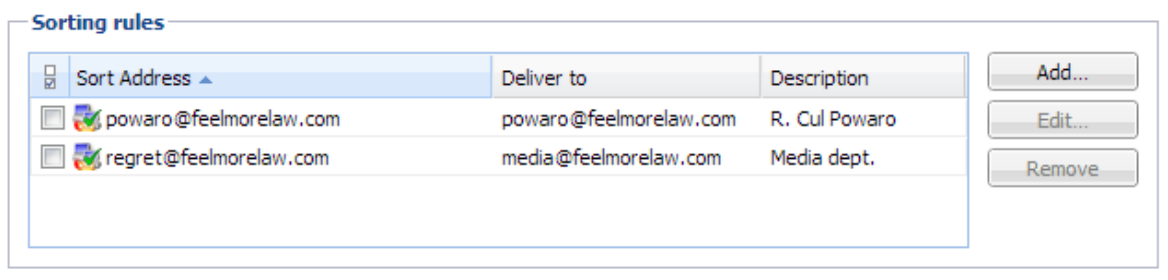
Sort address:

Deliver to:

Description:

Enable rule

5. Click **OK**.



Sort Address	Deliver to	Description
<input type="checkbox"/> powaro@feelmorrelaw.com	powaro@feelmorrelaw.com	R. Cul Powaro
<input type="checkbox"/> regret@feelmorrelaw.com	media@feelmorrelaw.com	Media dept.

### Special sorting rules

\* → **admin@example.com**

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

Without this rule, such messages are discarded.

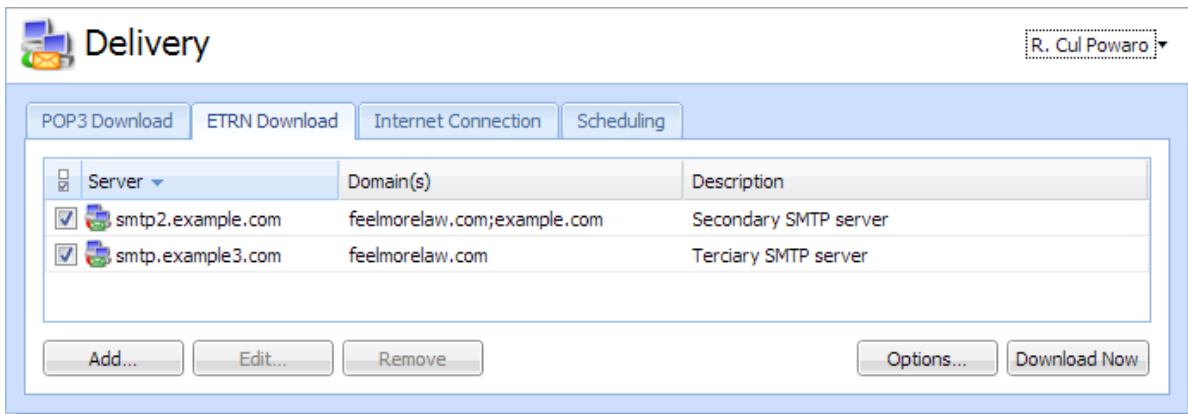
**\*@example.com → \*@example.com**

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

# Receiving email via ETRN

## About ETRN

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



## Configuring the ETRN account

1. In the administration interface, go to section **Configuration** → **Delivery** → **ETRN Download**.
2. Click **Add**.  
The **Add ETRN Account** dialog opens.
3. Type the server name, domain names (can be separated by semi-colon).
4. If authentication is required, type the username and password.
5. Click **OK**.
6. [Schedule an action for the ETRN download.](#)



**Add ETRN Account**

Server:

Domain(s):

Description:

Enable ETRN account

Authentication is required

User:

Password:

**i** You can enter multiple domains separated by semicolons ( ; ).

OK Cancel

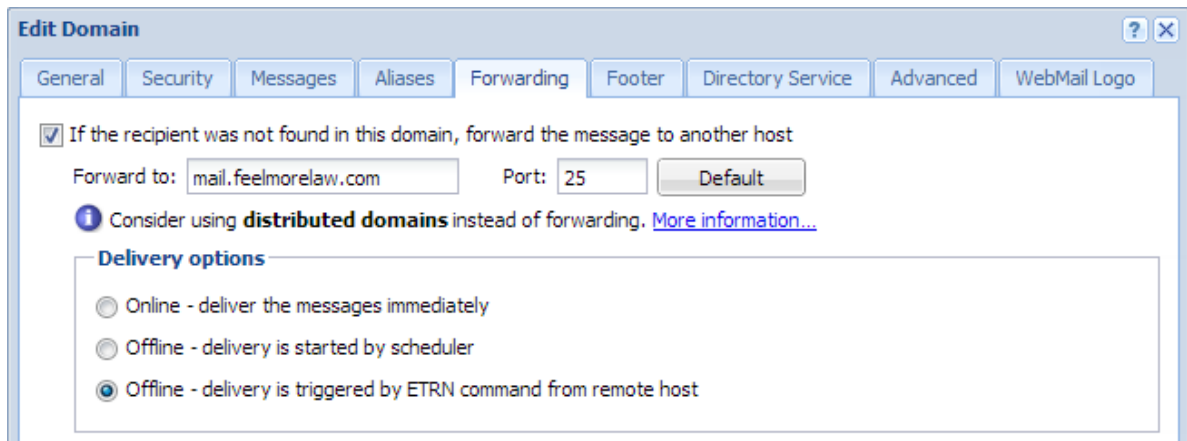
## Forwarding email

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

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

## Receiving email via ETRN

---



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

# Scheduling email delivery

---

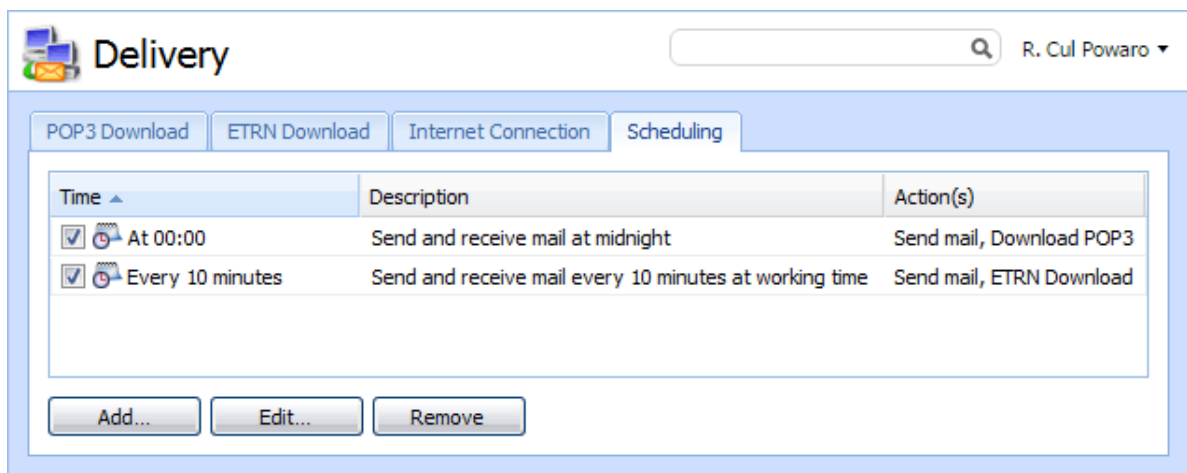
## About scheduling

In Kerio Connect, you can schedule to:

- [Download messages from a remote POP3 server](#)
- [Receive messages using the ETRN command to defined servers](#)
- [Send messages from the message queue](#)

Configure scheduling if you use [POP3](#) or [ETRN](#) and:

- Have a permanent Internet connection,
- Connect to the Internet via a dial-up line.



## Configuring scheduling

To add a new scheduled task:

1. In the administration interface, go to **Configuration** → **Delivery** → **Scheduling**.
2. Click **Add**.
3. Type a **Description** for better reference.

## Scheduling email delivery

---

4. Specify the **Time condition**.

You can schedule tasks to happen:

- Every specific number of minutes or hours
- At a specific time every day

5. To limit the scheduling to a specific **time range**, select **Valid only at time** and select a time range.

6. Specify the **Action**, Kerio Connect performs.

You can schedule any of these:

- Send messages from the message queue
- Download messages through POP3
- Send an ETRN command

7. Click **OK**.

**Add Scheduled Action**

Description: Send and receive email every 10 minutes at working time

**Time condition**

Every 10 minutes

Valid only at time Holiday Edit...

**Action**

Send messages from the outgoing queue

Download messages from POP3 mailboxes

Invoke mail transfer by sending ETRN command to specified SMTP servers

**Optional parameters**

Allow to establish Dial-Up connection if necessary

Enable scheduled action

OK Cancel

# Securing Kerio Connect

---

## Issues to address

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

## Configuring your firewall

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

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

**Table 1** Services to be allowed on the firewall

### Password policy

Read [Password policy in Kerio Connect](#) for detailed information on user passwords.

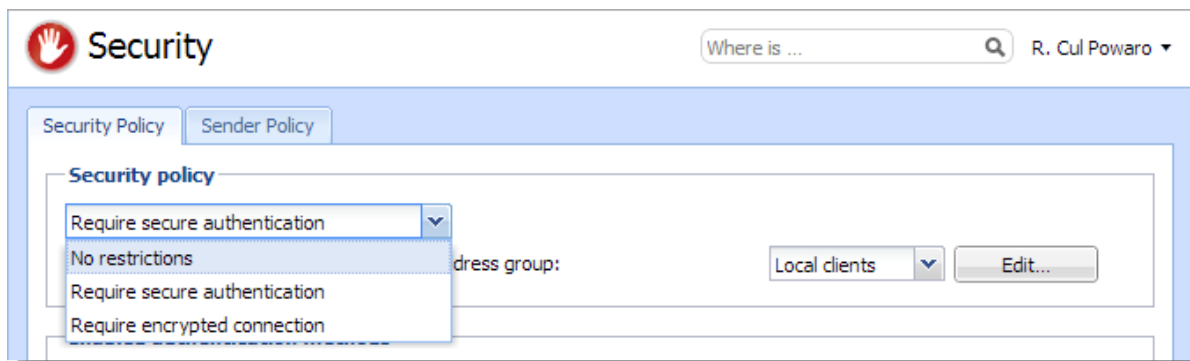
### Configuring a secure connection to Kerio Connect

Kerio Connect can do either of the following:

- [Secure user authentication](#)
- [Encrypt the whole communication](#)

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

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

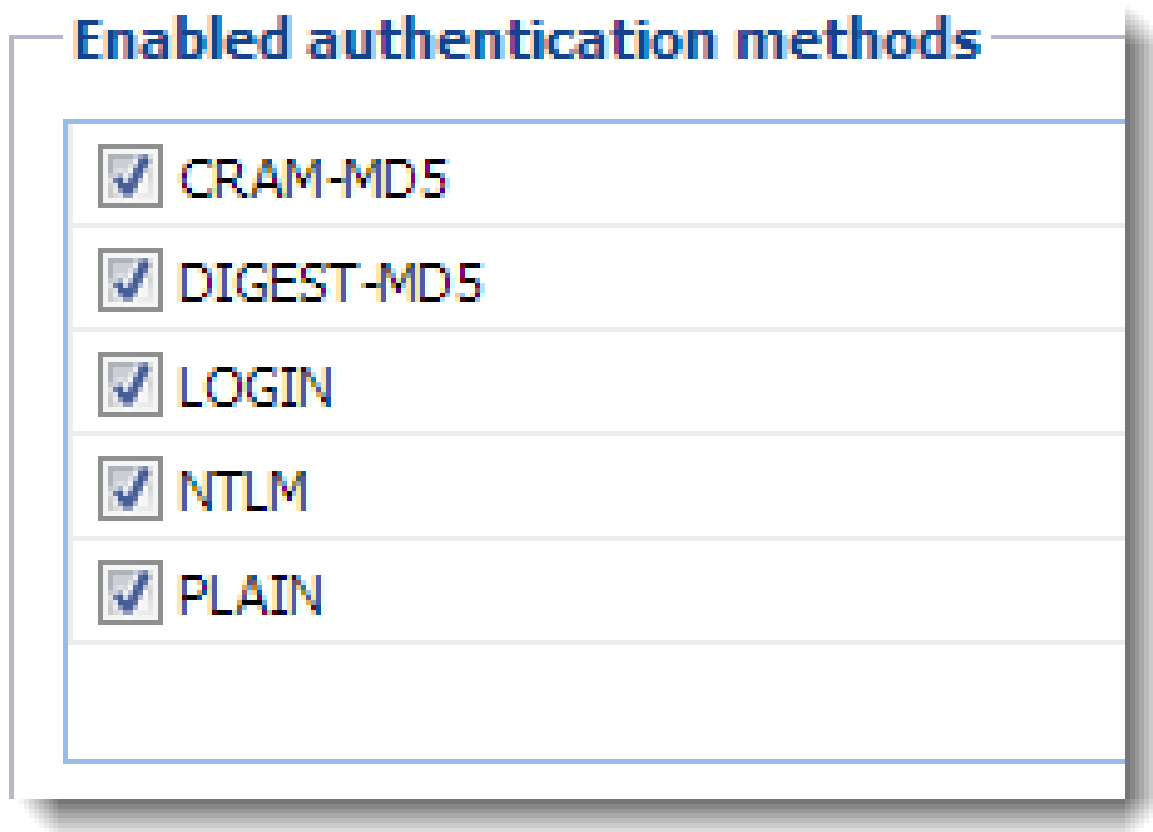


### Securing user authentication

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

You can select any of the following authentication methods:

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



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



If users' passwords are saved in the SHA format:

- Select **PLAIN** and/or **LOGIN**.
- Do not [map users](#) from a directory service.

### Encrypting user communication

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

You must allow the secured version of all service you use [on your firewall](#).



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

# Configuring anti-spoofing in Kerio Connect

---

## About anti-spoofing

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

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

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

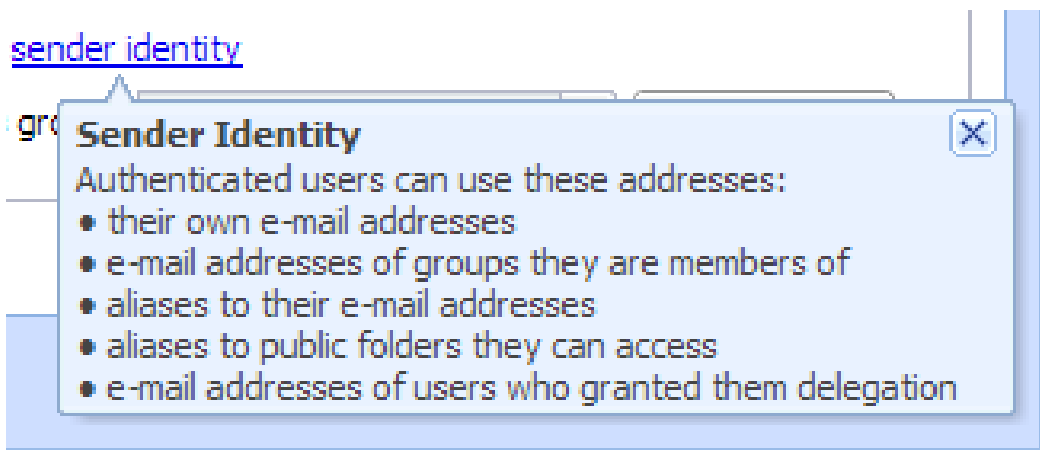
## Configuring anti-spoofing in Kerio Connect

1. Go to the **Configuration** → **Security** → **tab Sender Policy** section.
2. Select the **User must authenticate in order to send messages from a local domain** option.
3. Kerio Connect can automatically **Reject messages with spoofed local domain**.



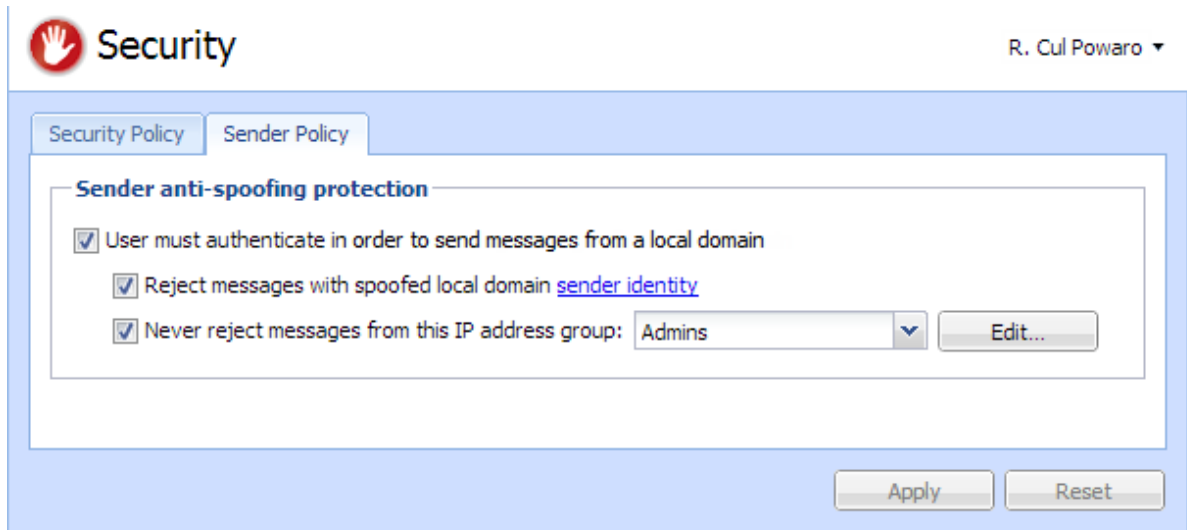
See the [Security log](#) for information about the rejected messages.

4. Click the **sender policy** link to see which types of addresses are available to your users.





5. Define a [group of trusted IP addresses](#).
6. Click **Apply**.

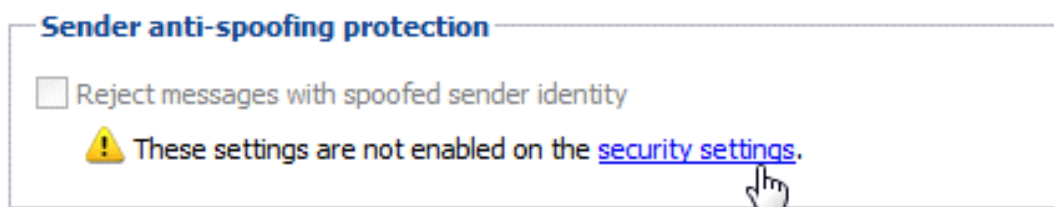


For more information about other security features in Kerio Connect, read [Securing Kerio Connect](#).

## Enabling anti-spoofing per domain

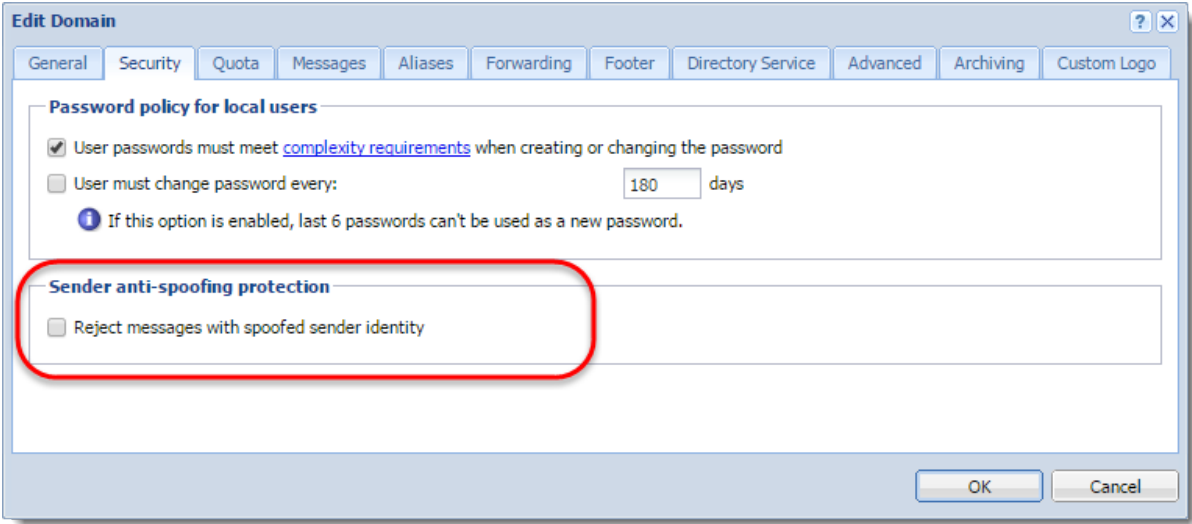
1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Double-click a domain and go to tab **Security**.
3. Select the **Reject messages with spoofed sender identity** option .

If the option is not available, you haven't configured anti-spoofing for the server. Click the **security settings** link, which takes you to the [appropriate section](#).



# Configuring anti-spoofing in Kerio Connect

4. Click OK.



# Password policy in Kerio Connect

---

## About password policy

To [secure](#) users and their passwords in Kerio Connect:

- [Advise users to create strong passwords](#)
- [Require complex passwords](#) (for local users)
- [Enable password expiry](#) (for local users)
- [Protect against login guessing](#)

## Creating strong user passwords

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

### Long

Passwords should be at least 8 characters long.

### Complex

Passwords should contain all of the following:

- Lowercase letters
- Uppercase letters
- Numbers
- Special characters

### Valid

Users should change their password often.

You can also read this [Wikipedia article](#) for more information.

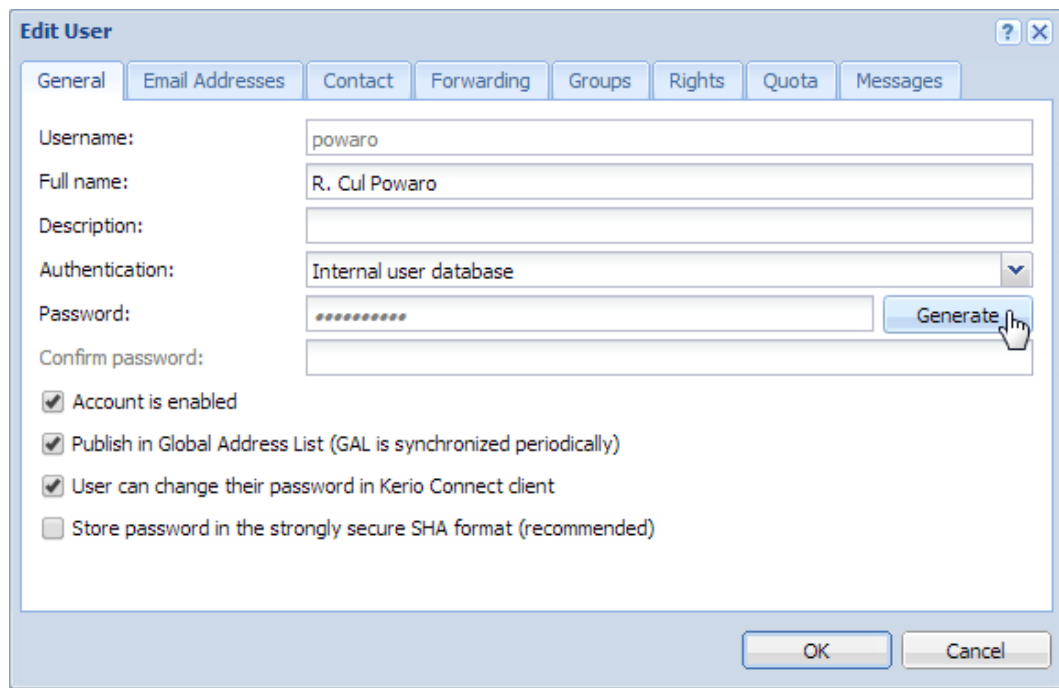
## *Generating strong passwords*

Kerio Connect can generate strong passwords for your users:

1. Go to the **Users** section.
2. Select a user and click **Edit**.
3. On the **General** tab, click **Generate**.

## Password policy in Kerio Connect

---



The screenshot shows the 'Edit User' dialog box with the following details:

- Username:** powaro
- Full name:** R. Cul Powaro
- Description:** (empty)
- Authentication:** Internal user database
- Password:** (masked with asterisks)
- Confirm password:** (empty)
- 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)

4. Copy the generated password and give it to user.
5. Click **OK**.

### Requiring complex passwords (for local users)

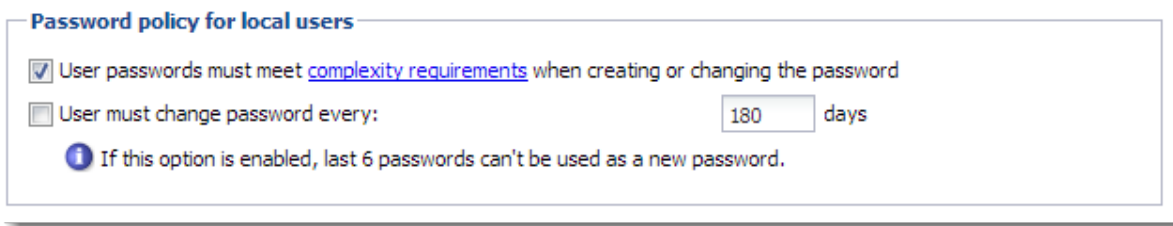
In Kerio Connect, you can force local users to create strong and complex passwords.

Complex password:

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

To configure complex passwords for individual domains:

1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Select a domain and click **Edit**.
3. On the **Security** tab, enable the **User passwords must meet complexity requirements** option.
4. Click **OK**.



From now on, each time local users changes their password in Kerio Connect Client, they must create a password which complies with the Kerio Connect's complexity requirements.



Remember to [enable users to change their passwords](#) in Kerio Connect Client.

This also applies when administrators change passwords via the administration interface.

### Enabling password expiry (for local users)

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

1. In the administration interface, go to the **Configuration** → **Domains** section.
2. Select a domain and click **Edit**.
3. On the **Security** tab, enable the **User must change password every** option.
4. Set the number of days after which users must change their password.
5. Click **OK**.



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

### *Notifying about the expiration*

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

Users must [change their password in Kerio Connect Client](#).

If users fail to change their password, they cannot login to their account and must contact their administrator (who changes the password for them in their user settings).

## Password policy in Kerio Connect

---

If an administrator password expires, the administrator can login to the administration interface to change their password.

### Protecting against password guessing attacks

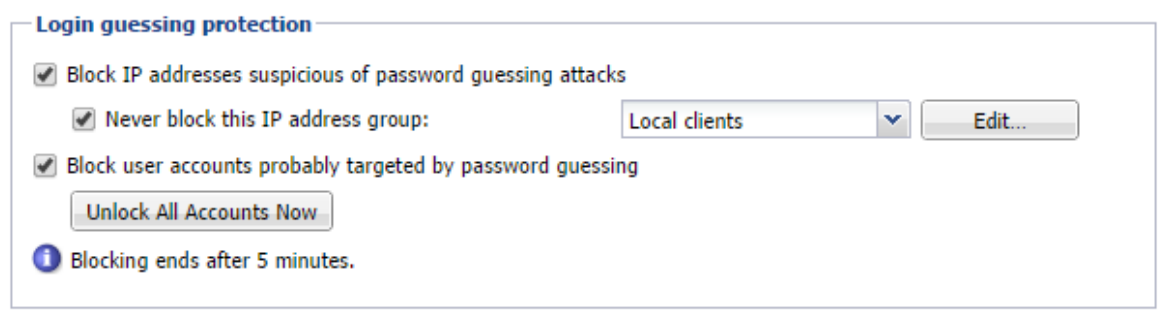
Kerio Connect can block IP addresses suspicious of password guessing attacks (ten unsuccessful attempts in one minute).

1. Go to section **Configuration** → **Security** → **the Security Policy tab**.
2. Select the **Block IP addresses suspicious of password guessing attacks** option.



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. Click **OK**.



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

This action is not identical with temporary [disabling user accounts](#).

# Authenticating messages with DKIM

## About DKIM

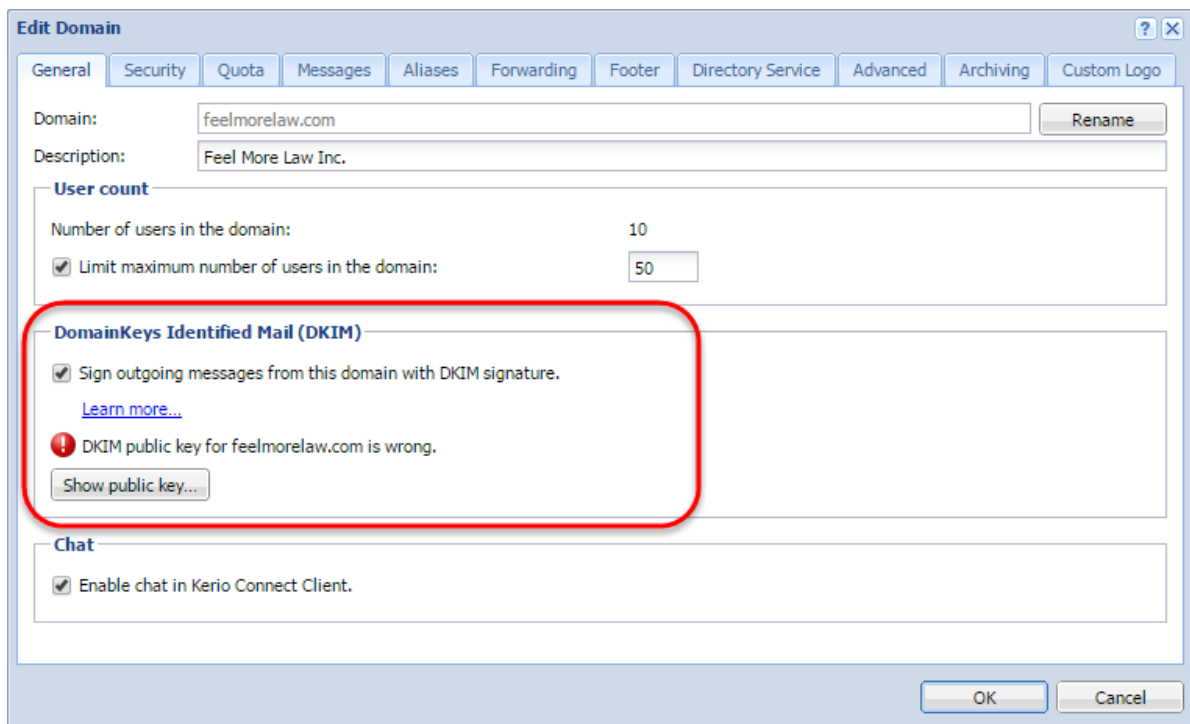
**DomainKeys Identified Mail (DKIM)** signs outgoing messages from Kerio Connect with a special signature to identify the sender. Your users thus take responsibility for the messages they send and the recipients are sure the messages came from a verified user (by retrieving your public key).

To sign messages with a DKIM signature:

1. Enable DKIM authentication in your domain settings.
2. [Add the DKIM public key to your DNS settings.](#)

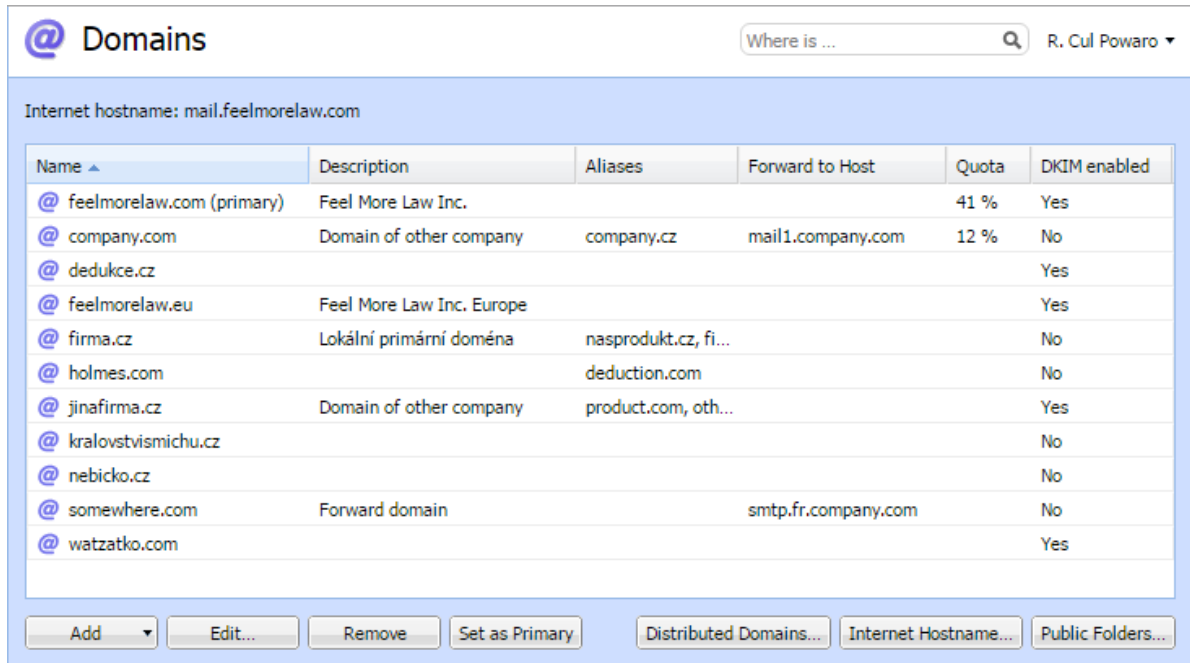
## Enabling DKIM in Kerio Connect

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



## Authenticating messages with DKIM

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



Name ▲	Description	Aliases	Forward to Host	Quota	DKIM enabled
@ feelmorrelaw.com (primary)	Feel More Law Inc.			41 %	Yes
@ company.com	Domain of other company	company.cz	mail1.company.com	12 %	No
@ dedukce.cz					Yes
@ feelmorrelaw.eu	Feel More Law Inc. Europe				Yes
@ firma.cz	Lokální primární doména	nasprodukt.cz, fi...			No
@ holmes.com		deduction.com			No
@ jinafirma.cz	Domain of other company	product.com, oth...			Yes
@ kralovstvismichu.cz					No
@ nebicko.cz					No
@ somewhere.com	Forward domain		smtp.fr.company.com		No
@ watzatko.com					Yes

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

Read article [Configuring DNS for DKIM](#) for more information.

### **Aliases**

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

### **Testing the DKIM signature**

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



# Configuring DNS for DKIM

---

## Adding a DKIM record to your DNS

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

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

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

You can [find the public key in Kerio Connect](#). The key includes two parts:

- **Record name** (or selector)

Example:

```
mail._domainkey.fee1more1aw.com.
```

- **TXT value**

Example:

```
v=DKIM1;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDf10chtL4siFYCrSPxw43fqc4z  
Oo3N+I1220oK2Cp+NZw9Kuv8iu2Ua3zfbUnZWvWK4aEeo1iRd7SXIhKpXkgkwn  
AB3DGAQ6+/7UVXf9x0eupr1DqtNwKt/NngC7ZIZyNRPx1HWK1eP13UXCD8macUEb  
bcBhthrnETKoCg8w0wIDAQAB
```



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

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

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

### **Domain aliases**

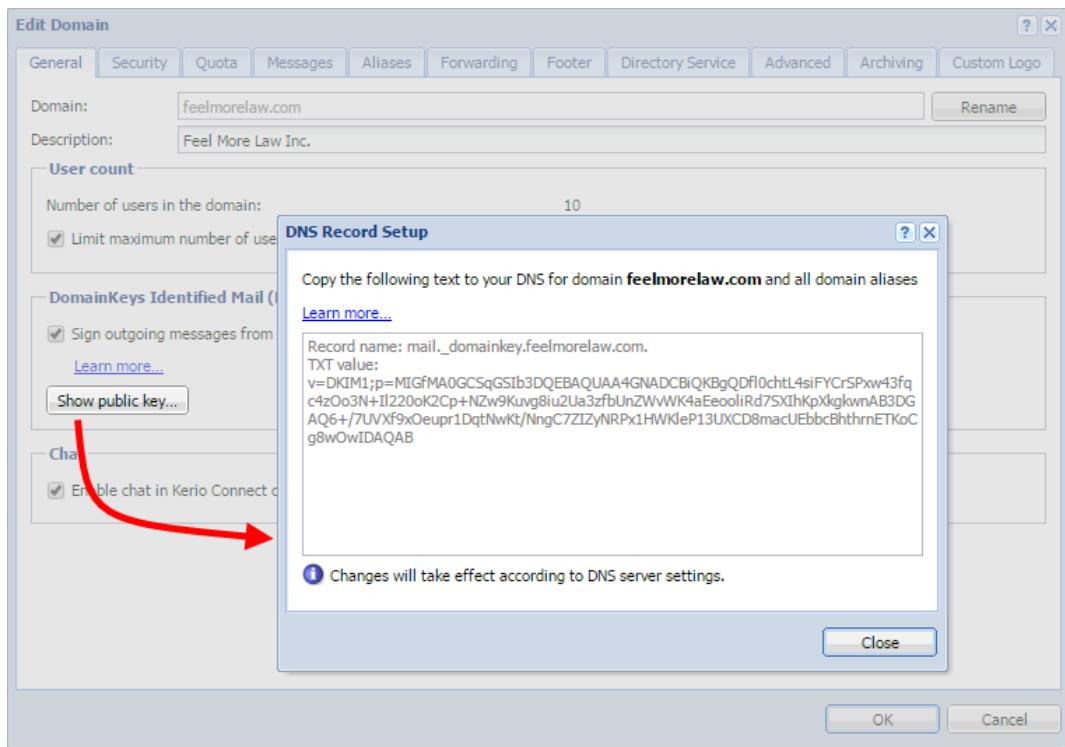
If a domain includes aliases, also add DNS record for DKIM to all aliases.

### Acquiring DKIM public key in Kerio Connect

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

This opens a dialog with you domain public key.

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



### Creating a short DKIM public key

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

#### *Generating a short DKIM key with DKIM wizard*

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

DKIM Wizard

Recommend 33 Follow 177 Recommend 92 Share 5 Tweet 6 Evaluate Now

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.\*\*\*

<input type="text" value="feelmorelaw.com"/>	Domain name of the "From:" header address, not the SMTP "MAIL FROM". (e.g., port25.com)
<input type="text" value="mail"/>	DomainKey Selector (e.g., key1)
<input checked="" type="radio"/> 1024 <input type="radio"/> 2048	Key size in bits.

CREATE KEYS

The page will display your public and private keys. Now, [add the private key to Kerio Connect](#).

## Configuring DNS for DKIM

<input type="text" value="feelmorelaw.com"/>	Domain name of the "From:" header address, not the SMTP "MAIL FROM". (e.g., port25.com)
<input type="text" value="mail"/>	DomainKey Selector (e.g., key1)
<input checked="" type="radio"/> 1024 <input type="radio"/> 2048	Key size in bits.

CREATE KEYS

-----BEGIN PUBLIC KEY-----

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDpnmIWPJXpRmTT2PL4AxYgpOczD0ojoWP8qnlXMLCW/Fdmjnk  
uWwehRqH6ubFh7exI1xn4iXay8Qtv213e3m5yZPnw7LYodRJB5hPoP5PHMVe3Bl  
fcyrUzJmXb3rb99d5UMXANhAJTuOtLM9JILN0s+ikn3QM1IUmAyRCg2XAwIDAQAB
```

-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----

```
MIICWwIBAAKBgQDpnmIWPJXpRmTT2PL4AxYgpOczD0ojoWP8qnlXMLCW/Fdmjnk  
uWwehRqH6ubFh7exI1xn4iXay8Qtv213e3m5yZPnw7LYodRJB5hPoP5PHMVe3Bl  
fcyrUzJmXb3rb99d5UMXANhAJTuOtLM9JILN0s+ikn3QM1IUmAyRCg2XAwIDAQAB  
AoGAU9LTiP0GISRz6xtt2pVo7B+fIU/8HxKF5+d/FGAbNze93AMJgMsTQ0QpB9m+  
IeQXggSZFGEtifsREGUcpwFz5AkcPJG/RlgJuRJVNi+sM9qMxTW3MoOBHhFUNIaZ  
rL9JsJ0gaoNWlp7rpN0iOhanMx3o4uFO0w5ZbpkzP0pM7zkCQD8nFLUV603KmXM  
REUeAdnBDFMSFsnrO4PfMK5i8NDEXb/vsUBXeXqtWou3nqvD0KmatYcm7+RIpzN8  
izbR11jNAkEA7MDTShnhQNYy38f0mUffomkSO6W/Huk/5lpswUNRl/XBz6EbByS2  
DyvGp96RTYV0R0y7mN7cJqA+XdX372jvDwJAM9urrWfqaV7M0yhYwBZFK7q/YcFH  
5oCrS9BknG8vjIBqfLx4pvyLUMxAF8v9Gw/lIzuOg/tjc/7PNQwnTtOxKQJAQBm1  
Gtpk8nkFIxGwWA/trLtmBGBL7sKYWnYBHBjt9QbFAsJL3qRipkboDfsf3qykNt1  
r24njQ211RIpnth6YQJAE5+LE13rwPoFdG8Z9zXIIly8iTclLQglFms8uNT8zldci  
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 backing up the original private key.

4. Start the Kerio Connect server.

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

If you use [distributed domains](#), make sure the new private key is available on all servers.

#### ***BIND DNS server***

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

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

Example:

```
TXT ("v=DKIM1;"  
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDf10chtL4siFYCrSPxw43fqc4z"  
"0o3N+I1220oK2Cp+NZw9Kuv8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn"  
"AB3DGAQ6+/7UVXf9x0eupr1DqtNwKt/NngC7ZIZyNRPx1HWK1eP13UXCD8macUEb"  
"bcBhthrnETKoCg8wOwIDAQAB")
```

# Configuring spam control in Kerio Connect

---

## Antispam methods and tests in Kerio Connect

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

- **Kerio Anti-spam** — Advanced filtering of spam messages using Bitdefender's online scanning services.

For more information, see [Kerio Anti-spam filter](#).



In Kerio Connect 9.2 and newer, you can use Kerio Anti-spam together with SpamAssassin.

- **Black/white lists** — You can create lists of servers and automatically block or allow all messages they send.

For detailed information, see [Blocking messages from certain servers](#)

- **SpamAssassin** — [Apache SpamAssassin](#) is an antispam filter that employs several testing methods.

- **Caller ID and SPF** — You can filter out messages with fake sender addresses.

For detailed information, see [Configuring Caller ID and SPF in Kerio Connect](#)

- **Greylisting** — The greylisting method delivers only messages from known senders.

For detailed information, see [Configuring greylisting](#)

- **Delayed response to SMTP greeting (Spam Repellent)** — You can set a delayed SMTP greeting that prevents delivery of messages sent from spam servers.



Spam Repellent decreases the load on your server because messages rejected by Spam Repellent are not processed by other antispam and antivirus tests.

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

For detailed information, see [Creating custom rules for spam control in Kerio Connect](#)



Combine as many antispam features as possible. The more tests you use, the tighter the antispam filter is and the less spam is delivered to users' mailboxes. Also, spam detection is more granular, which reduces the number of messages marked as spam by mistake ("false positives").

For each method, except for Spam repellent, you can specify two actions for handling the spam messages:

- Deny message — This helps to reduce the load on the server
- Increase the message's spam score — This helps eliminating possible "false positives"

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

### Setting the spam score

Kerio Connect tests each message with all the enabled tests and filters. Based on the resulting spam score, Kerio Connect marks the message as spam or delivers it as a legitimate message.

To set the limits for marking messages as spam or not spam, set the following on the **Spam Rating** tab:

- **Tag score** — If the message reaches the tag score, Kerio Connect marks it as spam.
- **Block score** — If the messages reaches the block score, Kerio Connect discards the message.



If you set the block value too low, legitimate messages may be discarded. Use the **Forward the message to quarantine address** option when testing and optimizing the spam filter, and specify an account where Kerio Connect sends and stores the copies of all blocked messages.

## Configuring spam control in Kerio Connect

**Spam Filter** Where is ... R. Cul Powaro

Spam Rating | Kerio Anti-spam | Blacklists | Custom Rules | Caller ID | SPF | Greylisting | Spam Repellent

Enable spam rating

**Spam filter configuration**

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

**Spam rating limits**

Not Spam Spam

Tag score: 5

Block score: 9.5

**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

Apply Reset

### Monitoring the spam filter's functionality and efficiency

Kerio Connect includes several options for monitoring the spam filter's functionality.

#### Spam filter statistics

Kerio Connect generates statistics of its SpamAssassin filter. You can find the statistics in **Status** → **Statistics**.



Spam filter statistics	
Messages checked	21233
Spams detected (tagged)	1863
Spams detected (rejected)	284
Messages marked by users as spam	154
Messages marked by users as non-spam	89



This statistics does not include [Kerio Anti-spam advanced filter](#).

### Graphical overviews

Kerio Connect also uses traffic charts to trace certain values about spam messages.

In **Status** → **Traffic Charts**, you can find the following spam-related traffic charts:

- **Connections/Rejected SMTP** displays the number of SMTP connection attempts that were rejected by the Spam Repellent tool in the set time period.
- **Messages/Spam** displays how much spam was delivered and when in the set time period.

### Logs

You can solve problems related to the antispam filter in the following [Kerio Connect logs](#):

- **Spam** — All messages marked as spam are recorded in this log.
- **Debug** — Right-click in the **Debug** log area, click **Messages**, and select the following
  - **Spam Filter** — Logs the spam rating of each message that passes through the Kerio Connect antispam filter.
  - **SPF Record Lookup** — Gathers information about SPF queries sent to SMTP servers.
  - **SpamAssassin Processing** — Traces the processes that occurred during the SpamAssassin antispam tests.
  - **Kerio Anti-spam Processing** — Traces the processes regarding the Kerio Anti-spam scanning.

### Optimizing spam protection

For additional information about protection against spam in Kerio Connect, read:

- [Optimizing spam protection in Kerio Connect](#)
- [Recommended anti-spam settings](#)

# Kerio Anti-spam filter

---

## Overview



Changed in Kerio Connect 9.2.0!

The **Kerio Anti-spam** extension uses the Bitdefender online scanning service and provides an advanced level of spam filtering on incoming messages.

In Kerio Connect 9.0.3-9.1.1, Kerio Anti-spam replaces the SpamAssassin's SURBL and Bayes filters. Users don't need to use the **Spam** and **Not spam** buttons in Kerio Connect Client and Microsoft Outlook with Kerio Outlook Connector, so Kerio Connect hides those buttons.

In Kerio Connect 9.2 and newer, you can use Kerio Anti-spam together with SpamAssassin.

Kerio Anti-spam is available as an add-on. Without Kerio Anti-spam, you can still use the standard [antispam features](#) in Kerio Connect.

## How Kerio Anti-spam works

When Kerio Anti-spam is enabled, the following happens when Kerio Connect receives a message:

1. Kerio Connect sends encrypted data to the Bitdefender online scanning service.

See the [What data is sent to Bitdefender](#) section below for information about the data Kerio Connect sends.



If the computer with Kerio Connect is behind a firewall, you must allow unrestricted access to:

- \*.nimbus.bitdefender.net, port 443 (HTTPS)
- http://bda-update.kerio.com, port 80 (HTTP)

If Kerio Connect uses a proxy server, Kerio Anti-spam communicates with Bitdefender via the proxy server.

2. Bitdefender scans the data and sends the result to Kerio Connect.

The score can be:

- 0 (zero) for non-spam
- 1-9 for different levels of spam

## Kerio Anti-spam filter

---

3. Kerio Connect calculates the spam score using a special algorithm, and adds the score to the overall spam rating (see [Calculating the Kerio Anti-spam score](#) below).
4. If Bitdefender recognizes malware or a phishing message, Kerio Connect automatically blocks the message regardless of other Kerio Connect settings, such as whitelists or custom rules.

Kerio Connect discards the message or forwards it to a quarantine address depending on your settings. See [Setting the spam score](#) section in the “Configuring spam control in Kerio Connect” article.



You can disable this function in the [configuration file](#) (mailserver.cfg). Look for `<variable name="BlockMalware">` and `<variable name="BlockPhishing">` in the **Kerio Anti-spam** table and set the values to 0 (zero).

## What data is sent to Bitdefender

Kerio Connect doesn't send any information that could be used to identify a specific person, such as content of the original e-mail body, attached images, or attached files.

Bitdefender online scanning service receives the following information via HTTPS:

- The sender and the sender's IP address of the original message from the email SMTP envelope.
- The e-mail message fingerprint, a set of cryptographic hashes on different parts of the e-mail headers and body.

The hashes are irreversible. Kerio Connect doesn't send the original email body.

- URLs, e-mail addresses and telephone numbers contained in the body of the scanned e-mail message
- MD5 hashes of:
  - The FROM address, FROM domain and REPLY-TO address
  - Certain types of attachments, for example, Microsoft Office documents, PDFs, executable files
- The hashes of images embedded in the messages

The actual images are not transmitted.

## Calculating the Kerio Anti-spam score



Changed in Kerio Connect 9.2!

Kerio Connect calculates the Kerio Anti-spam score using a special algorithm and adds the score to the overall [spam rating](#).

The algorithm works as follows:

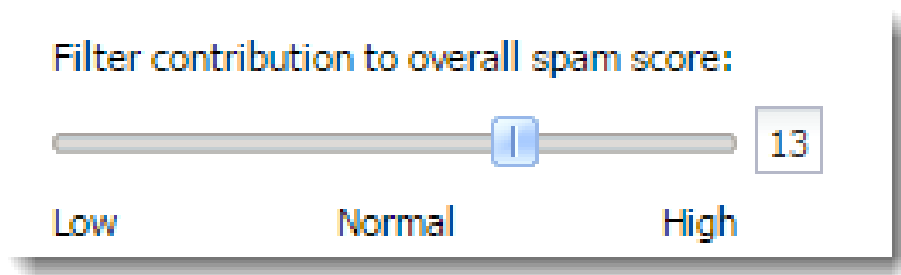
### *Bitdefender score is 1-9 (spam)*

Kerio Anti-spam score =  $X*Y/9$

- X is the score Kerio Connect receives from Bitdefender.
- Y is the Kerio Anti-spam setting.

If SpamAssassin is disabled, you can set the Kerio Anti-spam settings to 2-18.

If SpamAssassin is enabled, you can set the Kerio Anti-spam settings to 1-9.



In Kerio Connect 9.0.3-9.1.1, you can set Kerio Anti-spam setting to **moderate** (6), **normal** (10), and **high** (14).

### *Bitdefender score is 0 (non-spam)*

Kerio Anti-spam score = 0



In Kerio Connect 9.0.3 and 9.0.4, the algorithm is:  
 Kerio Anti-spam score =  $-1*Y$ , where Y is the Kerio Anti-spam setting (moderate = 1, normal = 2, and high = 3).

### Configuring Kerio Anti-spam

1. In the administration interface, go to **Configuration** → **Content Filter** → **Spam Filter**.
2. Switch to the **Kerio Anti-spam** tab.
3. Select **Enable Kerio Anti-spam advanced filter**.
4. Set the **Contribution to spam rating**.

The value of the setting affects only spam messages:

- If SpamAssassin is **disabled**, you can set the Kerio Anti-spam settings to 2-18.
- If SpamAssassin is **enabled**, you can set the Kerio Anti-spam settings to 1-9.



In Kerio Connect 9.1.0 and 9.1.1, you can set this value to moderate = 6, normal = 10, high = 14.

In Kerio Connect 9.0.3 and 9.0.4, this value also affects non-spam messages: moderate = 1, normal = 2, high = 3.

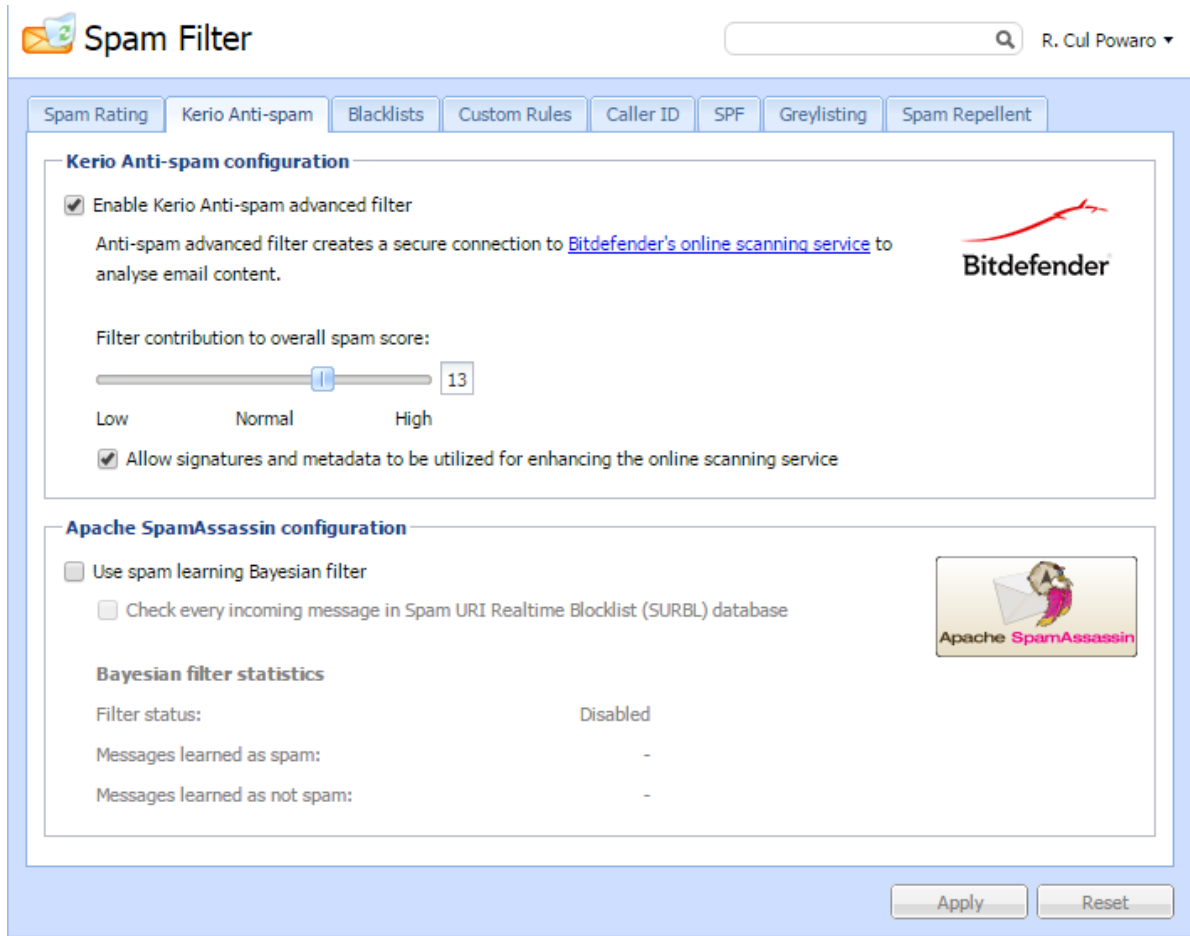
Also see the [Calculating the Kerio Anti-spam score](#) section above for information about the score.

5. (Optional) To allow Bitdefender to save the encrypted data from Kerio Connect, select the **Allow signatures and metadata to be utilized for enhancing the online scanning service**.



In Kerio Connect 9.0.3-9.1.1, select **Allow use of spam** and **Allow use of non-spam** options.

Bitdefender saves only the encrypted data, not the entire messages. See the [What data is sent to Bitdefender](#) section above.



If you're using [Kerio Connect Multi-Server](#), enable Kerio Anti-spam on the **Front-end** server.

### ***Kerio Connect on Debian 6***

If you install Kerio Connect on the Debian 6 operating system, you must perform the following before initializing Kerio Anti-spam:

```
wget --no-check-certificate https://www.thawte.com/roots/thawte_Primary_Root_CA-G3_SHA256.pem
cp thawte_Primary_Root_CA-G3_SHA256.pem /etc/ssl/certs
cd /etc/ssl/certs/
ln -s thawte_Primary_Root_CA-G3_SHA256.pem ba89ed3b.0
```

### Troubleshooting

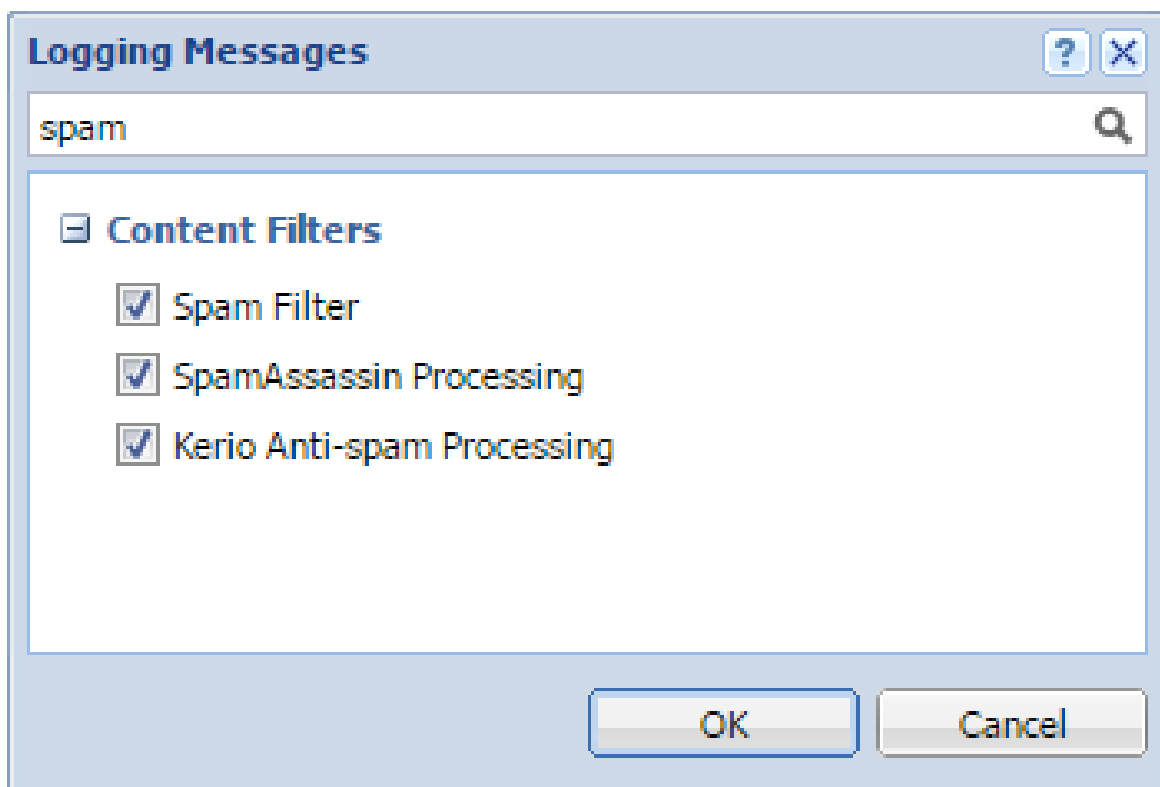
If you are upgrading from a previous version, restart Kerio Connect after you enable Kerio Anti-spam.

If any problem with Kerio Anti-spam occurs, consult the [Debug log](#):

1. Right-click in the Debug log area, and click **Messages**.
2. Select the **Kerio Anti-spam Processing**, **SpamAssassin Processing**, and **Spam filter** options.



After debugging, clear those options. Otherwise, the logging may slow down server performance.





# Configuring greylisting

---

## Overview

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

Greylisting is an antispam method that complements other [antispam methods](#) and mechanisms in Kerio Connect.

## How greylisting works

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

1. Kerio Connect contacts the greylisting server and provides information about the message. The greylisting server includes a list of trustworthy IP addresses.
2. If **the list contains** the message sender's IP address, the message passes the greylisting check immediately.
3. If **the list does not contain** the sender's IP address, the greylisting server delays the delivery. Trustworthy mailservers try to redeliver messages later. Spam senders usually do not.
4. Once the message is received again, the Kerio Greylisting Service adds the sender's IP address to the whitelist. All future messages from this sender will pass the greylisting check immediately (see step 2).



To learn more about greylisting, consult [greylisting.org](http://greylisting.org) or [Wikipedia](#).

## What data is sent to Kerio Technologies

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

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

The data is periodically deleted from the greylisting server.

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

## Configuring greylisting

---



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

To see the data sent by Kerio Greylisting Service, enable **Greylisting** in the [Debug log](#).

## Configuring greylisting

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

It is available to:

- Registered trial users
- Licensed users with valid Software Maintenance

Greylisting is disabled by default. To enable it:

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



Make sure your firewall allows outgoing connection on port 8045.

3. (Optional) Create a [list of IP addresses](#) to skip in the greylisting check.
4. Click **Test Connection** to check the connection with Kerio Greylisting Service.



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

5. Click **Apply**.

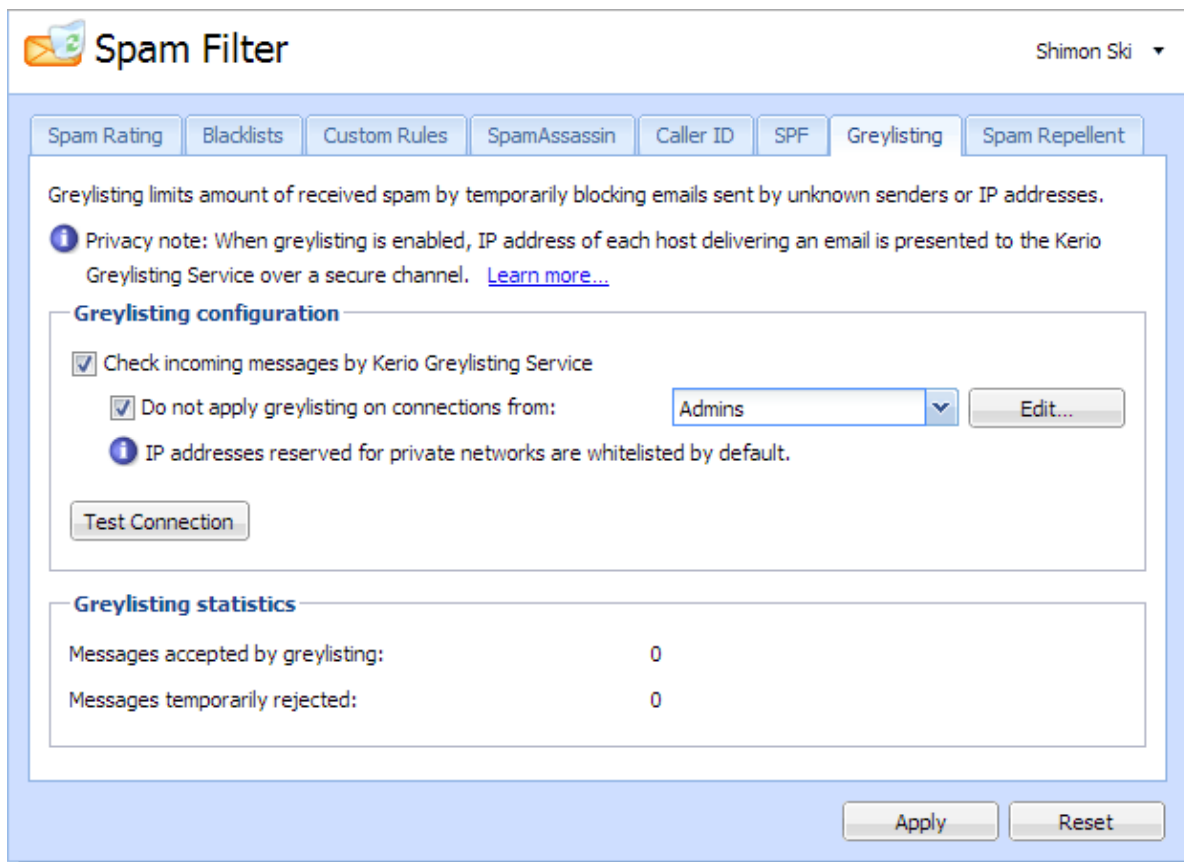


Figure 1 Greylisting

## Troubleshooting

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

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

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

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

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

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

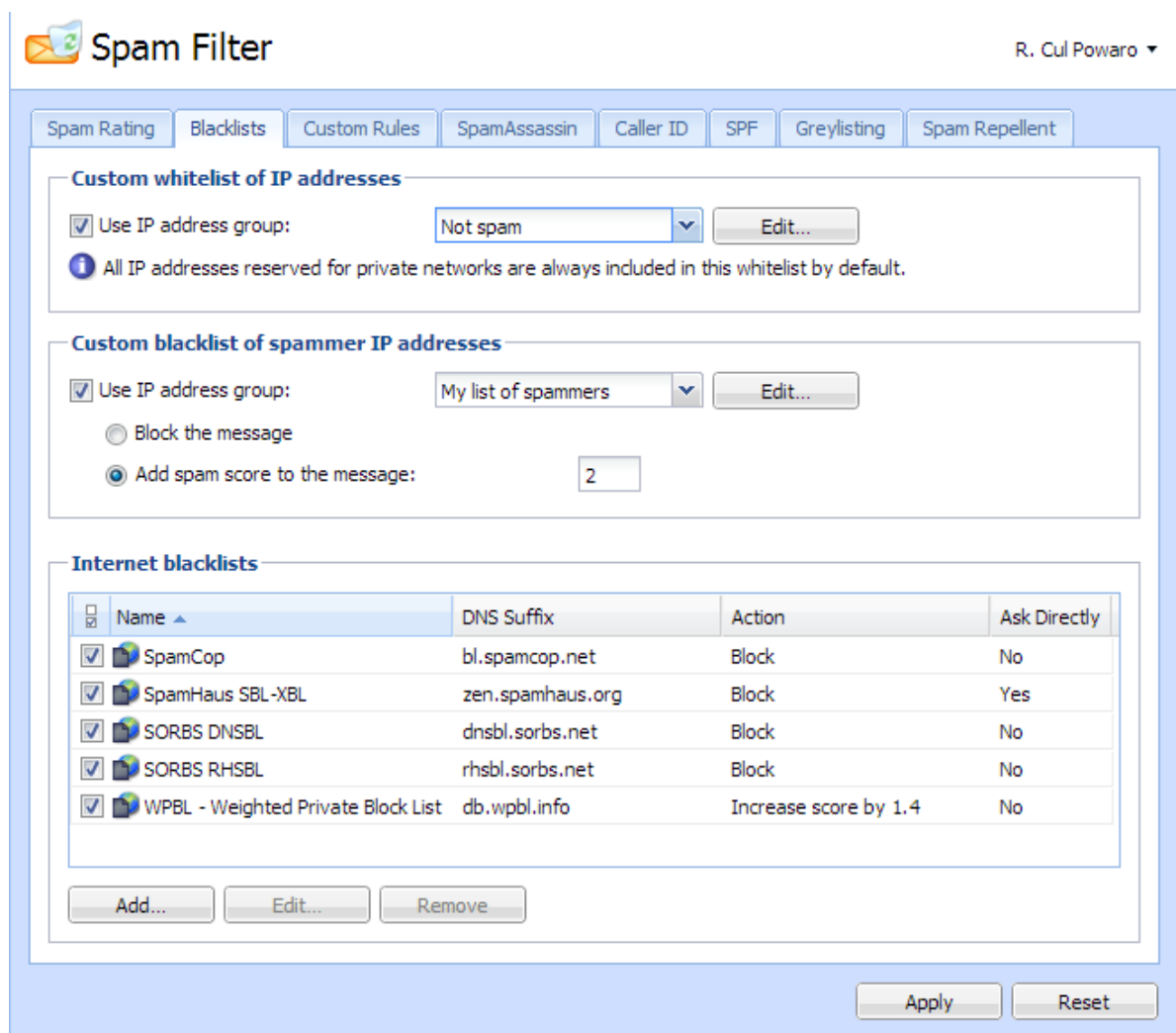
# Blocking messages from certain servers

## Automatically blocking or allowing messages from certain servers

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

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

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



### Blocking messages from spam servers — Custom blacklists

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

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

### Blocking messages from spam servers — Public databases

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

To use blacklists from **public databases**:

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

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

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

## Blocking messages from certain servers

---

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

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



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

## Allowing messages from trusted servers — Custom whitelists

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

To create your own whitelist:

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

# Configuring Caller ID and SPF in Kerio Connect

---

## Overview

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

The check verifies whether IP addresses of the remote SMTP server are authorized to send emails to the domain specified. Spammers thus have to use their real addresses and the unsolicited emails can be recognized quickly using different blacklists.



You can use Caller ID and SPF only if messages are delivered by the [SMTP protocol](#).

## Configuring Caller ID

To configure Caller ID in Kerio Connect:

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



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

## Configuring Caller ID and SPF in Kerio Connect

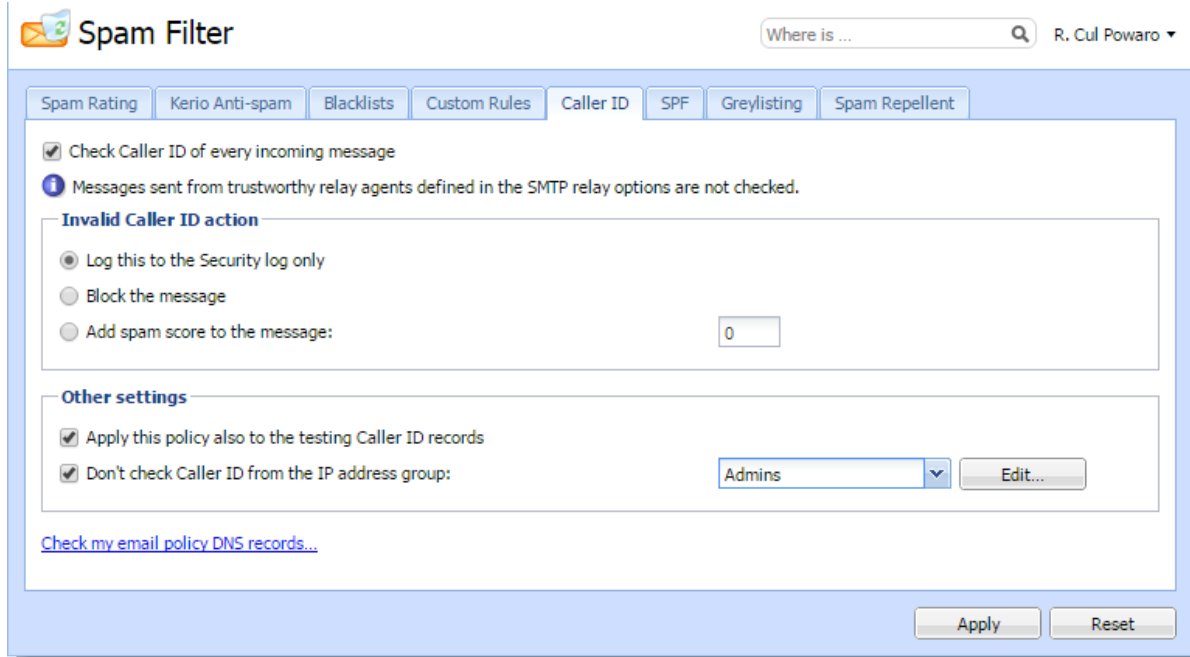


Figure 1 Caller ID

## Configuring SPF

To configure SPF in Kerio Connect:

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



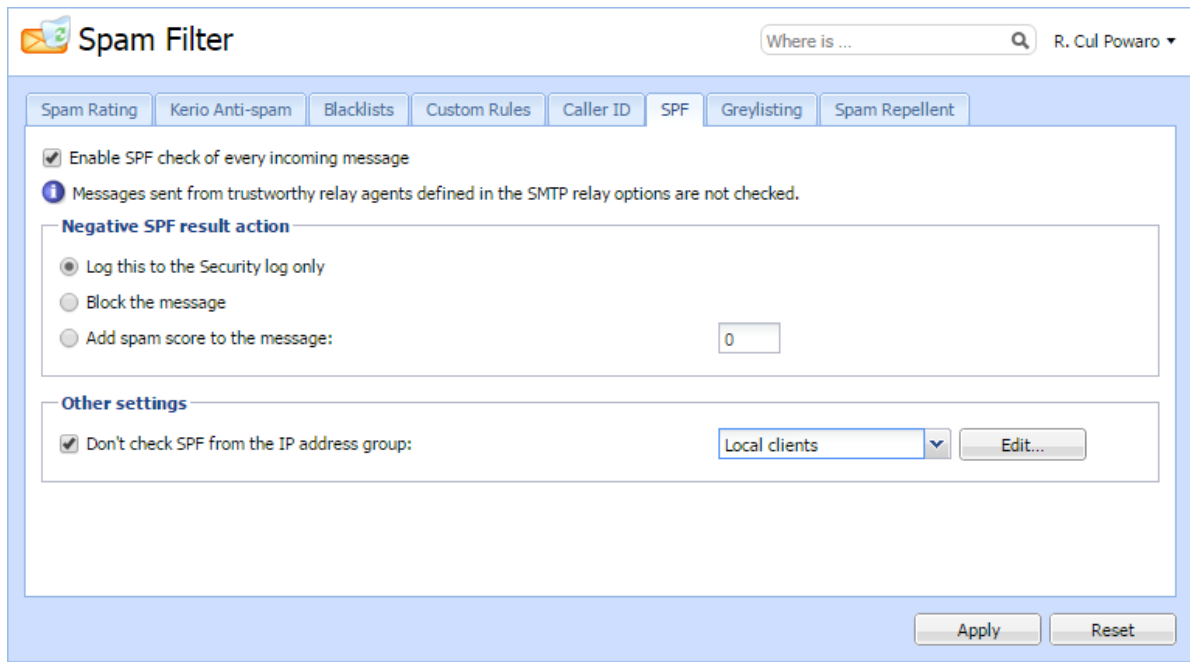


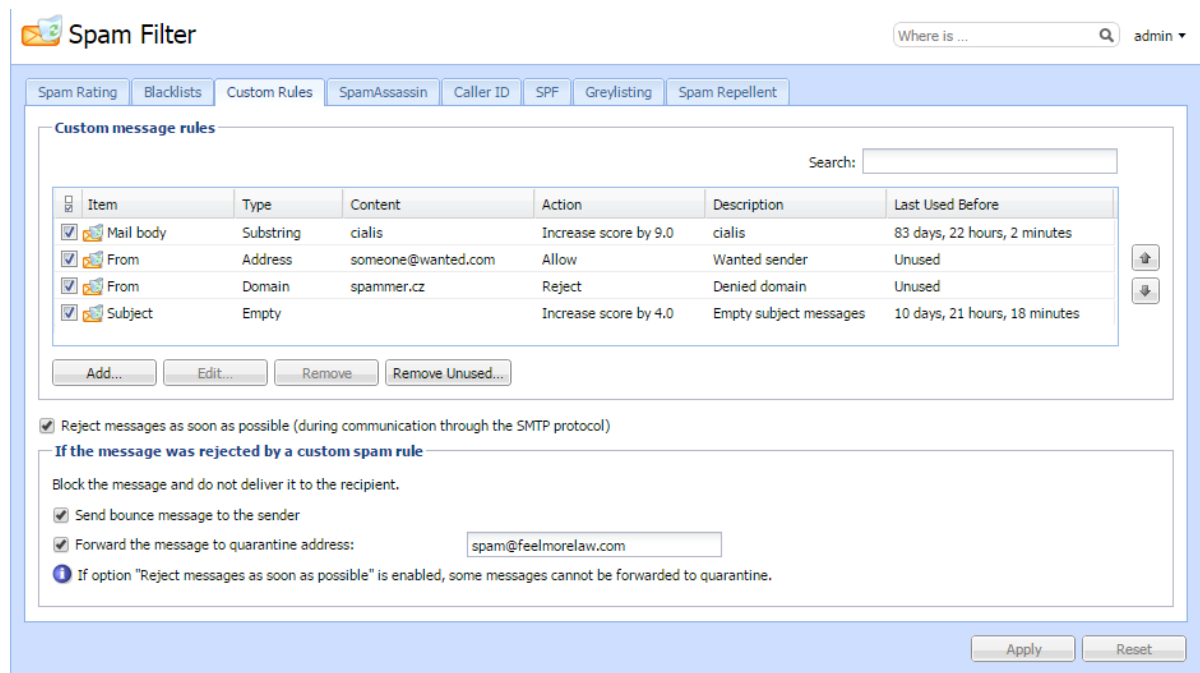
Figure 2 SPF

# Creating custom rules for spam control in Kerio Connect

## Overview

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

To create custom rules for spam control, go to **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules**.



## Creating custom rules

You can create as many rules as you like.

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

1. In the administration interface, go to **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules**.
2. Click **Add**.

3. In the **Add Rule** dialog, type a name for the rule.
4. Select **Mail header** or **Mail body** filter.
5. Type the string you want to filter.

You can use:

- Any text
  - \* to represent any number of characters
  - ? to represent a single character
  - Regular expressions (mail body only)
6. For any message that matches the rule, you can:
    - Treat the message as non-spam
    - Treat the message as spam and reject it
    - Add **spam score** to the message
  7. Click **OK**.



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

### Example for regular expressions

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

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

1. In **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules**, click **Add**.
2. Select **Mail body** and type the following regular expression:  
`/\bcialis\b/i`
3. Select **Treat the message as spam and reject it**.
4. Click **OK**.

**Add Rule**

Description:

**Condition**

Mail header

Mail body

Contains:

**Action**

Treat the message as non-spam (overrides the SpamAssassin score)

Treat the message as spam and reject it

Add spam score to the message:

Enable rule

From now on, Kerio Connect rejects all messages that include `cialis` as a single word.

For detailed information on regular expressions, see the [SpamAssassin wiki page](#).

### Defining actions for custom rules

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

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


You can select these option in **Configuration** → **Content Filter** → **Spam Filter** → **Custom rules** under the list of your custom rules.

**If the message was rejected by a custom spam rule**

Block the message and do not deliver it to the recipient.

Send bounce message to the sender

Forward the message to quarantine address:

 If option "Reject messages as soon as possible" is enabled, some messages cannot be forwarded to quarantine.



To decrease the load on the server, Kerio Connect can reject messages during the SMTP session.

To enable rejection during the SMTP session, select **Reject messages as soon as possible...** However, Kerio Connect cannot now perform the two actions described above.

# Bayesian self-learning in Kerio Connect

---

## Overview

There are many problems associated with detecting spam for the final recipient of an email. It is important to understand these problems in order to understand what Bayesian self-learning is and how it fits into Kerio's solution for spam protection.

## Terminology

- **Spam** is a message the recipient considers an unsolicited junk email.
- **Ham** is a message the recipient considers to be not spam.
- **False Positive** is a message that is incorrectly marked as spam.
- **False Negative** is a message that is incorrectly marked as ham.

## SpamAssassin

SpamAssassin uses static rule sets to determine if a message is spam.

Fixed set of rules cannot accurately define spam for everybody. It may result in SpamAssassin capturing most spam, however, it will always have some false positives and false negatives.

Also, the content in spam changes over time and the spam mutates. Unless the rules in SpamAssassin change, too, more and more spam gets in. Therefore, constant upgrades are necessary to maximize the spam blocking capabilities.

## Bayesian filtering

Recipients can train the Bayes database to recognize messages as **spam** or **ham**. The filter breaks messages into small pieces called tokens and determines which tokens occur mostly in spam messages, and which tokens occur mostly in ham messages.

The Bayes database must learn a lot of emails before it can function effectively. In general, the Bayes database begins to work after it has learned at least 200 spams and 200 hams. End-users must train the Bayes database enough to effectively fight mutating spam.

## Bayesian self-learning

SpamAssassin and additional Kerio Connect antispam features can help the Bayesian self-learning:

- The higher the SpamAssassin score, the more probable the message is a spam
- The lower the SpamAssassin score, the more probable the message is a ham.

SpamAssassin trains the Bayes database as follows:

- If the total SpamAssassin score is more than 12, and both the header score and body score are more than 3, consider the message as a **spam**.
- If the total SpamAssassin score is less than 0.1, consider the message as **not a spam**.

Additional antispam tests in Kerio Connect, such as blacklists, SPF, header tests, train the Bayes database as follows:

- If the total score from tests other than SpamAssassin is more than the required tag score, and SpamAssassin score is less than 0.1, consider the message as **spam**.
- If the total score including SpamAssassin is more than  $(\text{block score} - \text{tag score} / 1.8) + \text{tag score}$ , and SpamAssassin score is less than 12, consider the message as **spam**.
- If the total score from tests other than SpamAssassin is less than 0, and SpamAssassin trains the Bayes database with spam, consider the message as **ham**.

# Antivirus protection in Kerio Connect

---

## Overview



For Kerio Connect 9.2.1 and earlier, see [Antivirus protection in Kerio Connect 9.2.1 and earlier](#).

Kerio Connect includes Kerio Antivirus, an integrated protection against malicious emails with viruses. Viruses may infect your computer and cause harm to your files or to your computer system.



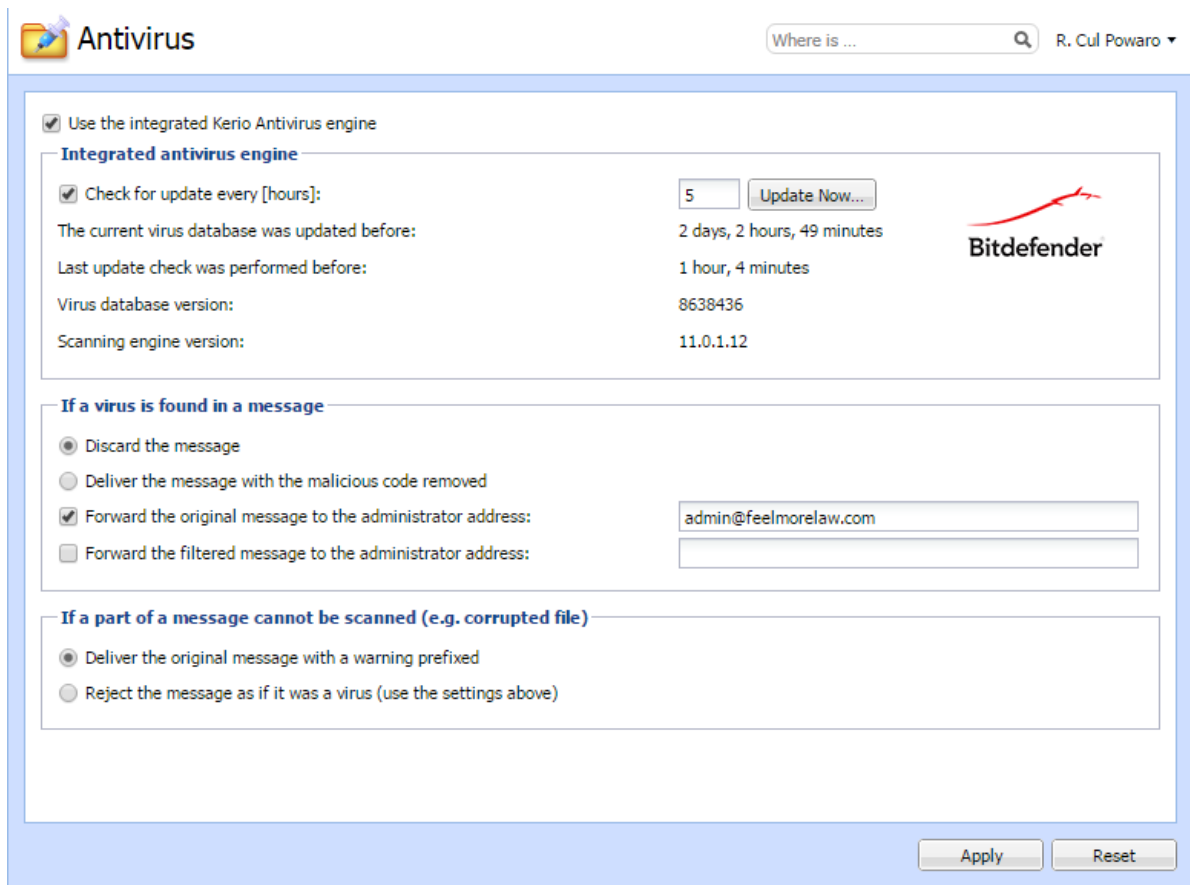
Kerio Antivirus is an optional component and is not available for [unregistered trial versions](#). See [Licenses in Kerio Connect](#).

## Configuring Kerio Antivirus

1. In the administration interface, go to **Configuration** → **Content Filter** → **Antivirus**.
2. Select the option **Use the integrated Kerio Antivirus engine**.
3. To update the virus database automatically, select **Check for update every [hours]**.  
If any new update is available, it is downloaded automatically.  
Kerio Connect downloads the database files via the HTTP protocol. Provide a persistent connection and allow the communication on your firewall or [proxy server](#).
4. Select the action for messages that contain a virus. Kerio Connect can:
  - **Discard the message**
  - **Deliver the message with the malicious code removed**
5. In addition, you can select from two options for forwarding messages:
  - **Forward the original message to an administrator address**
  - **Forward the filtered message to an administrator address**



6. For any message that Kerio Antivirus cannot scan, Kerio Connect can do one of the following:
- **Deliver the original message with a warning prefixed**
  - **Reject the message as if it was a virus**
7. Click **Apply**.



### Updating the antivirus database

After you install Kerio Connect, you must download the initial Kerio Antivirus definitions. Without it, your mail queue will be stopped.

The update starts automatically shortly after you install/update the server.

If your Kerio Connect server is behind firewall, allow HTTPS connection to:

- `bdupdate.kerio.com`
- `bdupdate-cdn.kerio.com`

## Antivirus protection in Kerio Connect

---

### Configuring the HTTP proxy server

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

To configure the proxy server:

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

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

### External antivirus

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

Read [Using external antivirus with Kerio products](#) and this [Kerio Blog post](#) for detailed information.

### Filtering message attachments

For information on scanning message attachments, read [Filtering message attachments in Kerio Connect](#).

### Troubleshooting

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

Antivirus statistics	
Attachments checked	1256
Viruses found	14
Prohibited filenames / MIME types found	123

You can also consult the following [logs](#):

- [Security](#) — For information about virus database updates.
- [Debug](#) — Right-click the Debug log area and enable **Messages** → **Antivirus Checking**



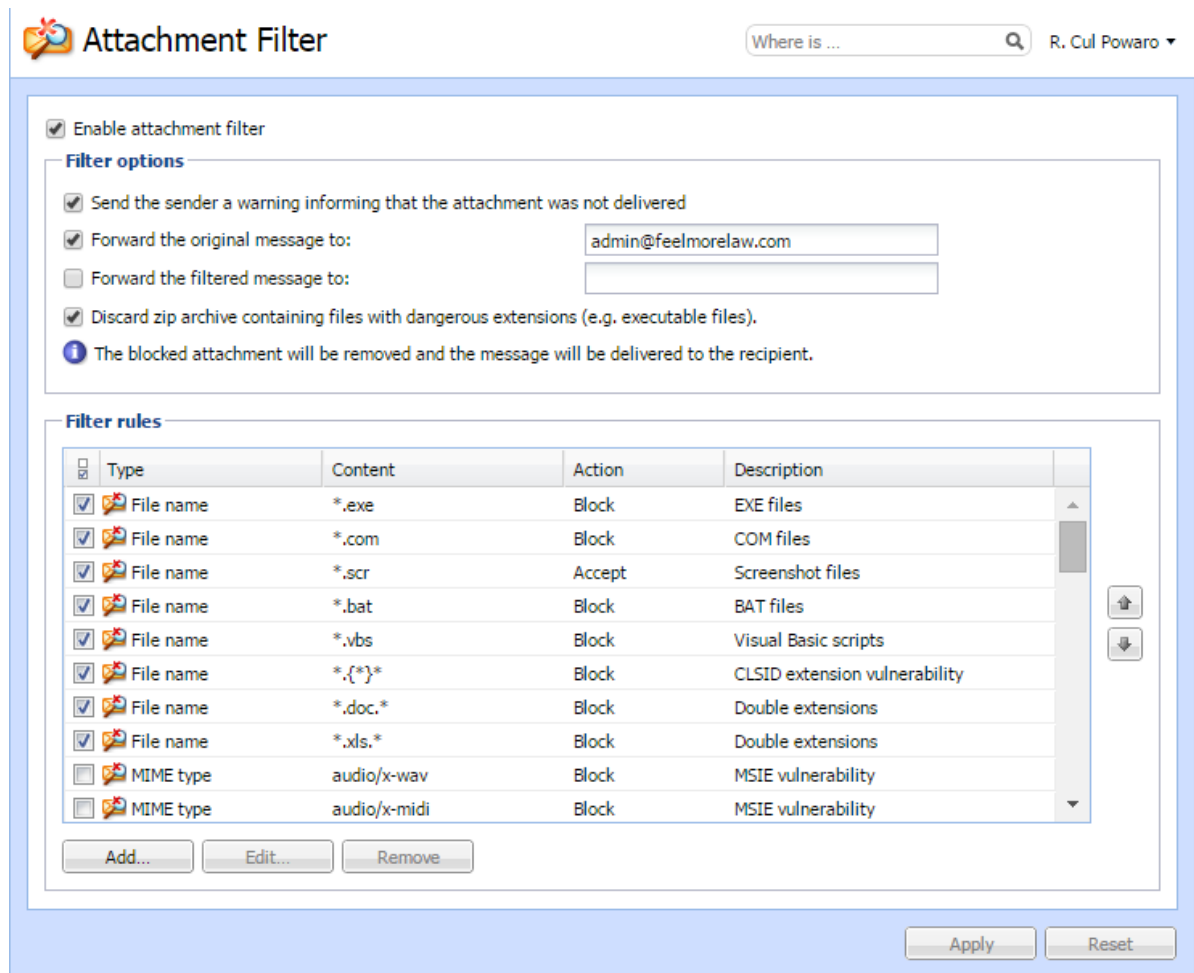
If the time from the last update is several times greater than the interval set, update the database manually and check the [Error](#) and [Security](#) logs.

# Filtering message attachments in Kerio Connect

## Overview

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

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



## Configuring the attachment filter

To configure attachment filtering:

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



New in Kerio Connect 8.5!

To discard the ZIP attachments with dangerous files, select the **Discard zip archive containing files with dangerous extensions...** option.

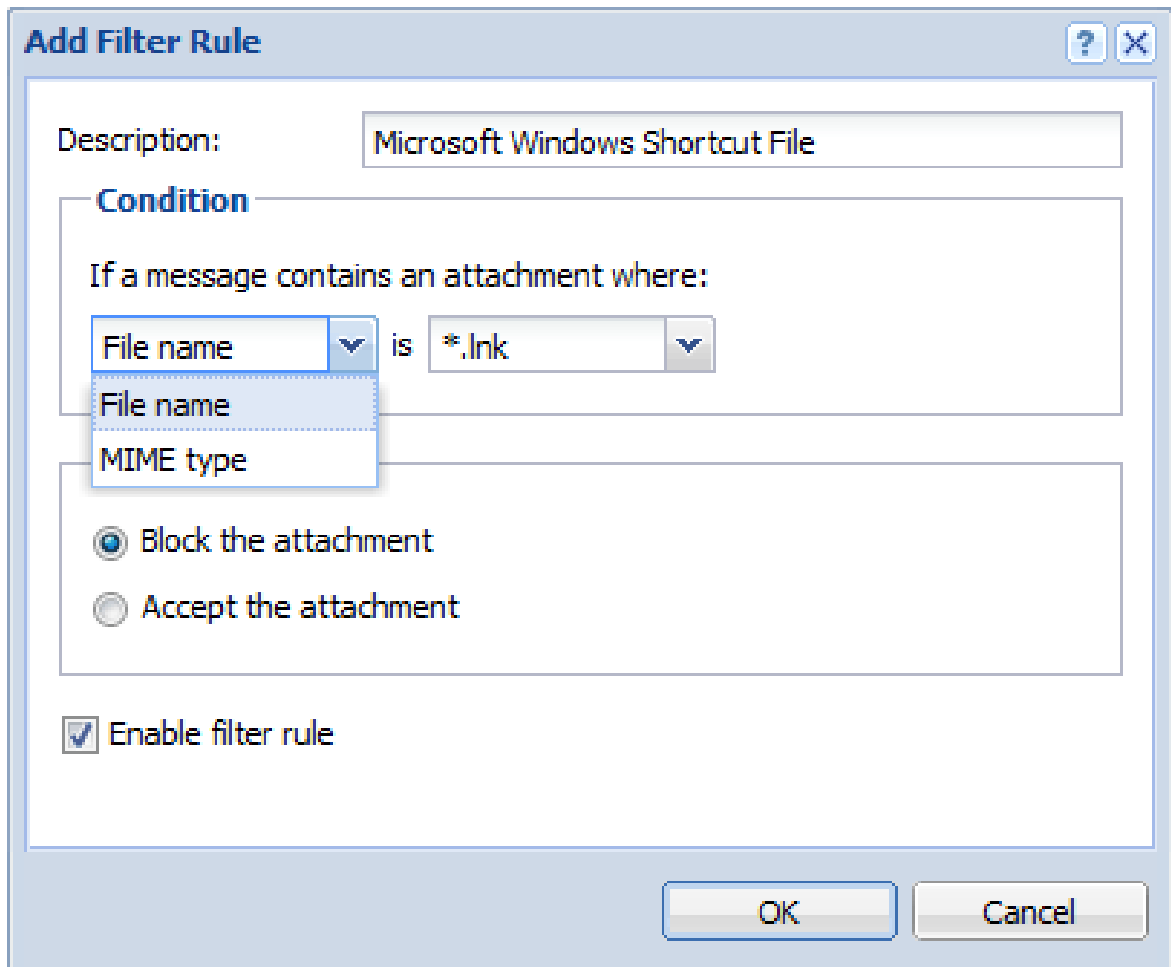
7. Select any of the predefined filter rules.  
Each rule can allow or block one specific type of attachment.
8. Click **Apply**.

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

## Creating custom attachment filter rules

To customize your filter rules:

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



### Troubleshooting

For details on attachment filtering in your Kerio Connect, consult the [Security log](#).

# Using an external antivirus with Kerio products

---

## Antivirus SDK for Kerio products

Kerio Connect and Kerio Control include Kerio Antivirus.

You can use alternative antivirus solutions by using the Kerio **Antivirus SDK for Kerio Connect and Kerio Control**. The Antivirus SDK includes a public API that can be used to write plugins for alternative antivirus solutions.

[Get the SDK](#) and read our [blog](#) to get detailed information.

# Configuring IP address groups

---

## Overview



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

IP address groups help easily define who has access to, for example, remote administration, services, and are used in additional settings in Kerio Connect.

You can define IP address groups:

- In the **Configuration** → **Definitions** → **IP Address Groups** section
- From any section in the administration interface where IP address groups are used



Item	Description
<b>Admins</b>	
<input checked="" type="checkbox"/> 192.168.25.25	
<b>Blacklist</b>	
<input checked="" type="checkbox"/> 125.45.5.5	
<b>Local clients</b>	
<input checked="" type="checkbox"/> 10.0.0.0 / 255.0.0.0	Private address space for local networks
<input checked="" type="checkbox"/> 127.0.0.1	Private address space for local networks
<input checked="" type="checkbox"/> 172.16.0.0 / 255.240.0.0	Private address space for local networks
<input checked="" type="checkbox"/> 192.168.0.0 / 255.255.0.0	Private address space for local networks
<input checked="" type="checkbox"/> ::1	Private address space for local networks
<input checked="" type="checkbox"/> fc00:: / 7	Private address space for local networks
<input checked="" type="checkbox"/> fe80:: / 10	Private address space for local networks
<b>My list of spammers</b>	
<input checked="" type="checkbox"/> Blacklist	
<b>Not spam</b>	
<input checked="" type="checkbox"/> Whitelist	
<b>Voicemail</b>	
<input checked="" type="checkbox"/> 129.12.158.2	
<b>Whitelist</b>	
<input checked="" type="checkbox"/> 124.45.4.5	

## Configuring IP address group



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

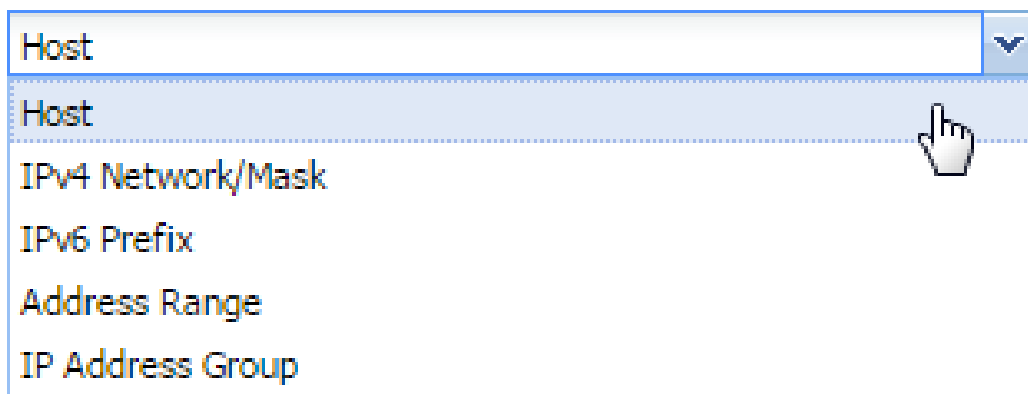
1. In the administration interface, go to the **Configuration** → **Definitions** → **IP Address**

## Configuring IP address groups

---

**Groups** section.

2. Click **Add**
3. To create a new IP address group, select **Create new**.  
To add IP addresses to an existing group, select the IP address group in **Select existing**.
4. Select the type and specify the IP address.



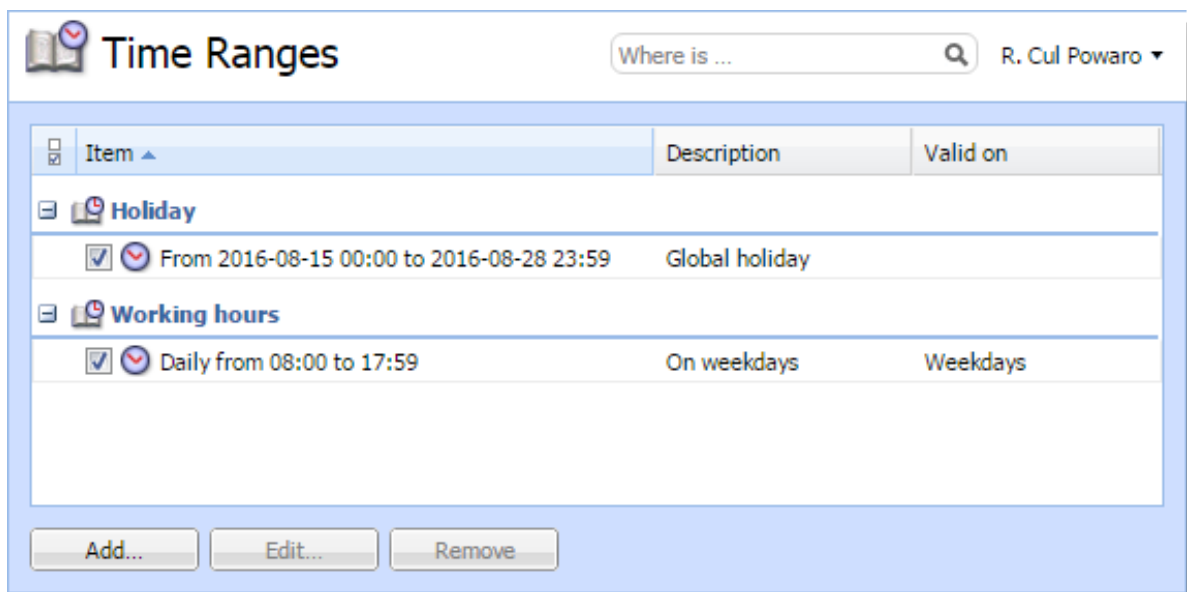
5. Add a description for better reference.
6. Click **OK**.

# Creating time ranges in Kerio Connect

## Overview

You can restrict all scheduled tasks in Kerio Connect to certain time intervals — **time ranges**.

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



## Creating time ranges

1. In the administration interface, go to **Configuration** → **Definitions** → **Time Ranges**.
2. Click **Add** and
3. To create a new time range, select **Create new**.  
To add a time range to an existing interval, select **Selecting existing** and select the parent time interval in the drop-down list.
4. Type a **Description** for better reference.
5. Configure the **Time settings** — frequency, time interval, and days.
6. Click **OK**.

## Creating time ranges in Kerio Connect

**Add Time Range**

**Add to a group**

Select existing: No groups available

Create new: Working hours

**Description**

On weekdays

**Time settings**

Type: Daily

From: 08:00

To: 17:59

Valid on: Weekdays

Mon  Tue  Wed  Thu  Fri  Sat  Sun

**i** Times set in the dialog correspond with server time zone.

OK Cancel

# Filtering messages on the server

---

## Overview



New in Kerio Connect 9!

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

For example, you can:

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

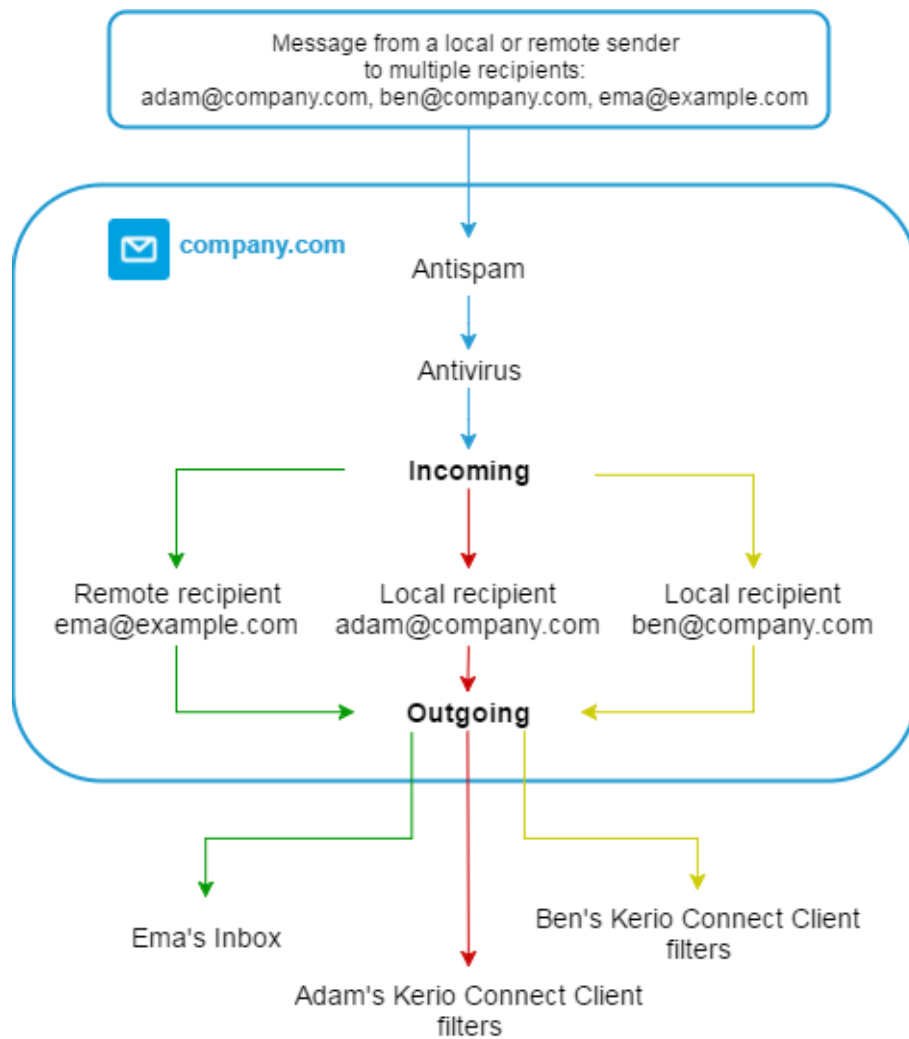
### *How message filters work*

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

Here is an example of a message sent to multiple recipients. You can see the order how Kerio Connect processes the rules:

## Filtering messages on the server

---



You can find the following specific examples below:

- [Forwarding messages to public folders](#)
- [Prohibiting sending messages to remote recipients for individual users](#)
- [Sending a copy of a message to another email address](#)
- [Rejecting messages with large attachments](#)
- [Sending an auto-reply message](#)

## Creating incoming rules

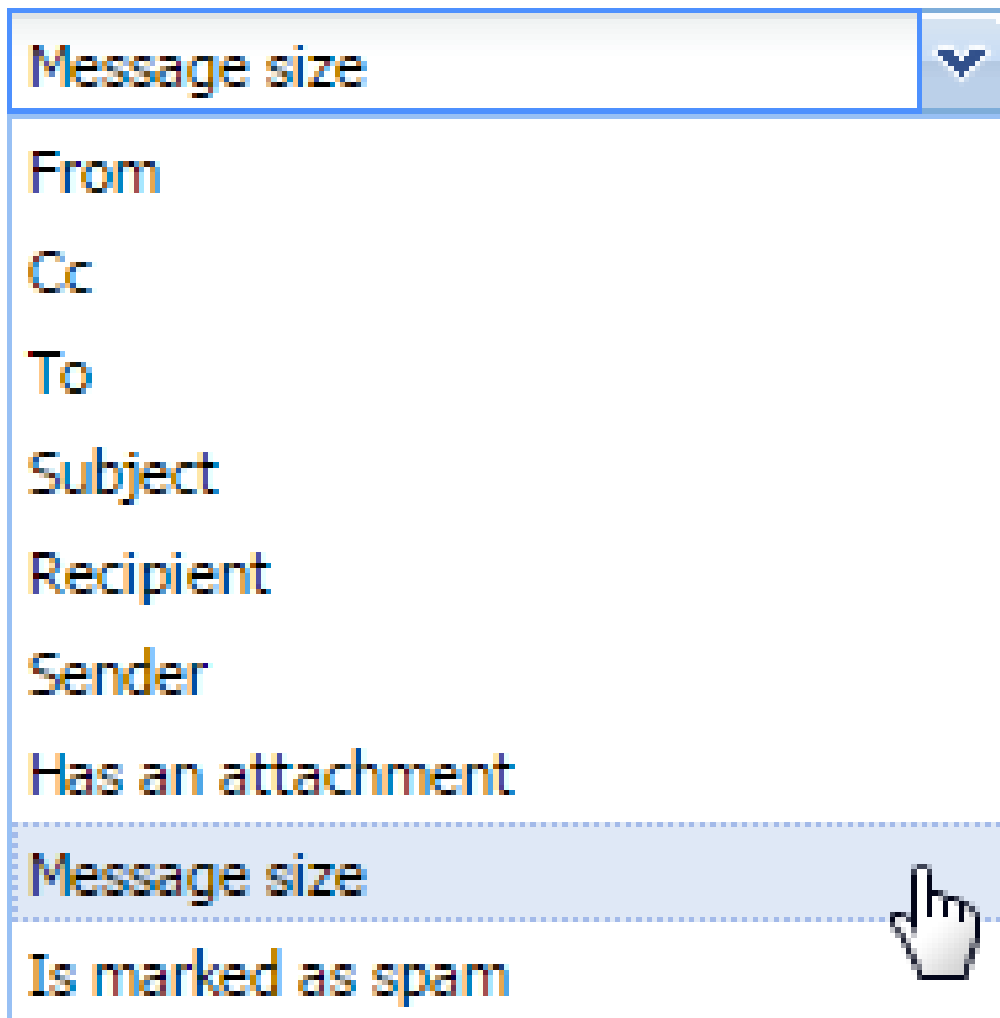
Kerio Connect applies incoming rules to all messages that come to the server from local or remote senders.

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

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

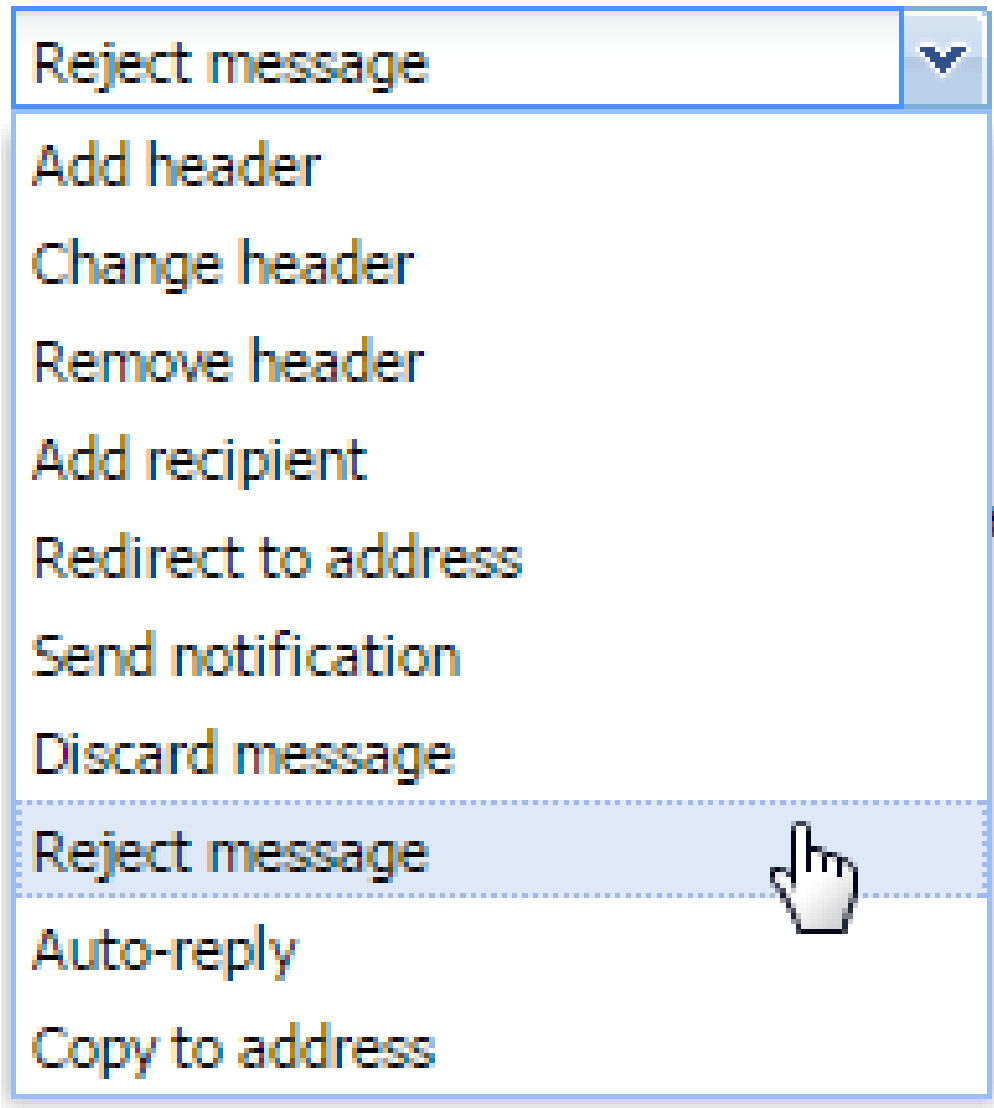
To specify multiple email addresses, use a comma (,), or a semi-colon (;).

Regular expressions and the ? / \* placeholders are not supported.



5. Specify the actions.

Perform the following actions:



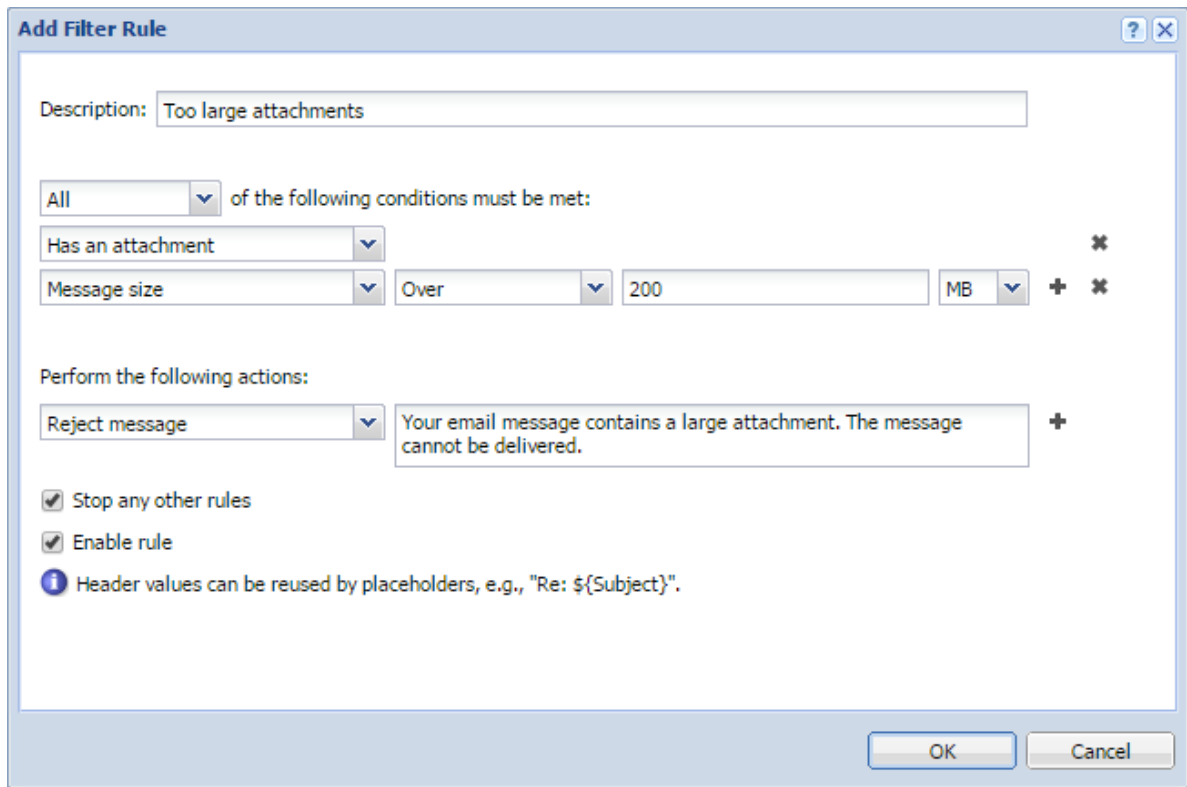
You can use placeholders for headers values — `#{size}` for message size, `#{subject}` for message subject, and so on (for more headers see, for example, [Wikipedia](#)).

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



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

7. Click **OK**.
8. Click **Apply**.



## Creating outgoing rules

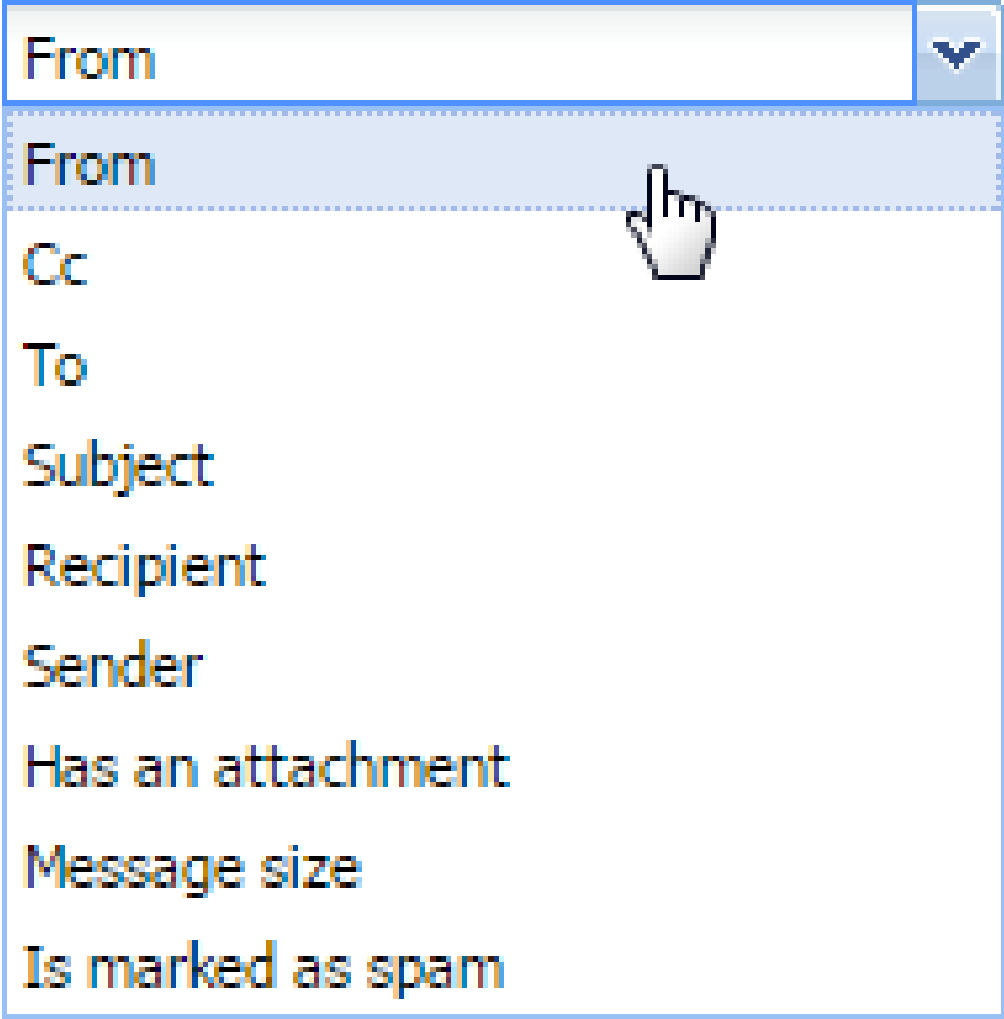
Kerio Connect applies outgoing rules to all messages that Kerio Connect sends to local or remote recipients.

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

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

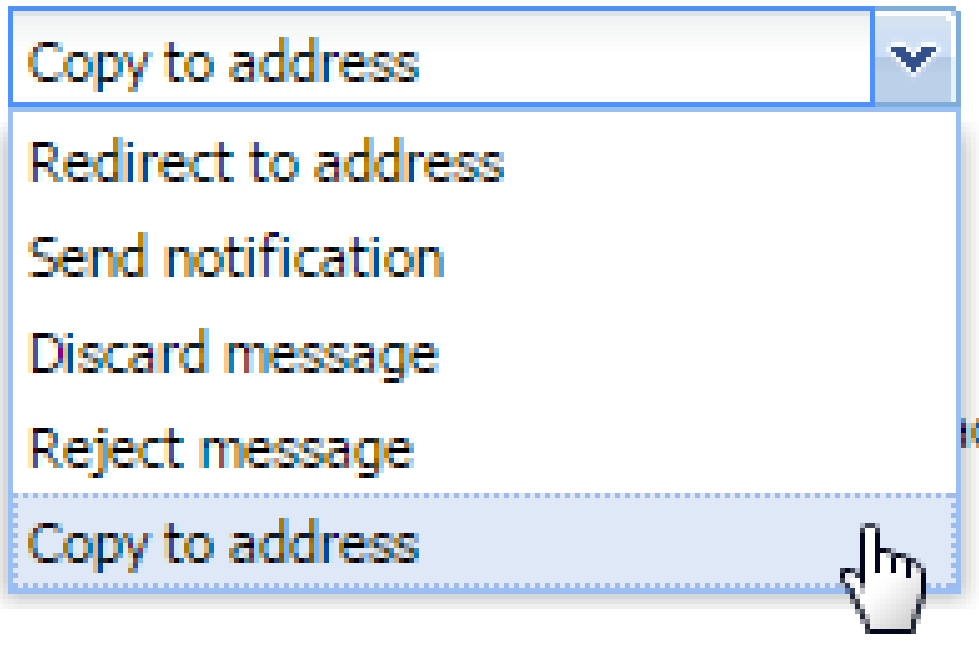
To specify multiple email addresses, use a comma (,), or a semi-colon (;).

Regular expressions and the ? / \* placeholders are not supported.



5. Specify the actions.

Perform the following actions:



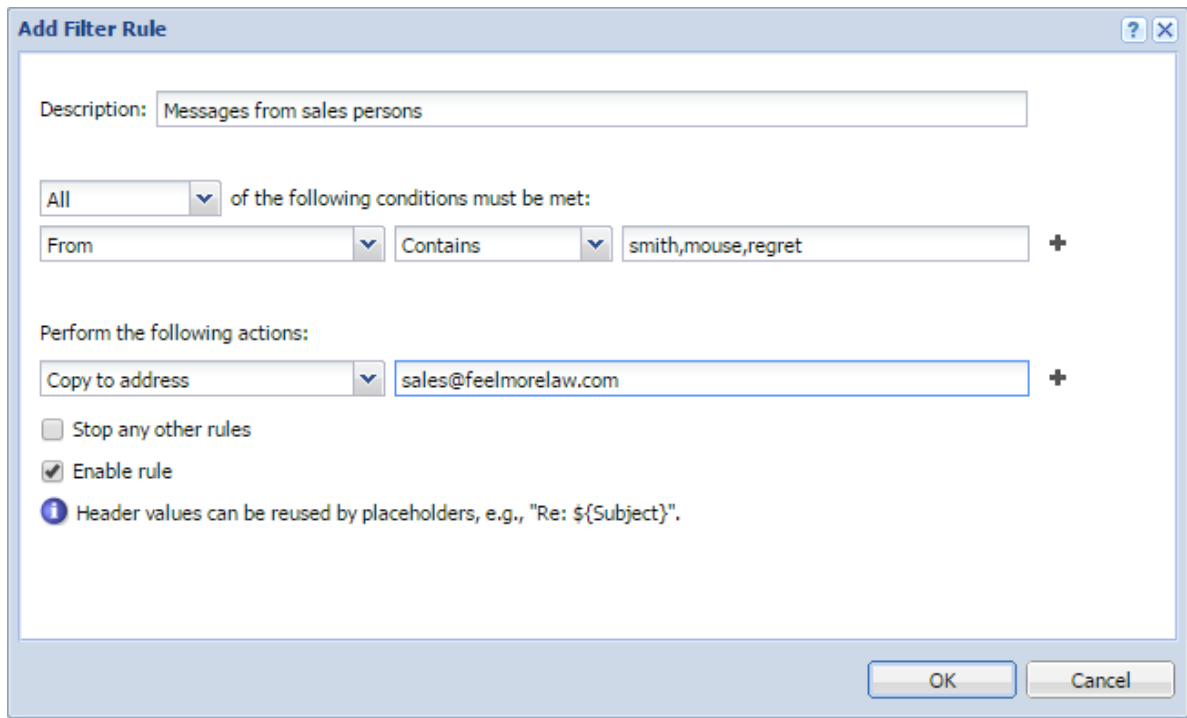
You can use placeholders for headers values — `#{size}` for message size, `#{subject}` for message subject, and so on (for more headers see, for example, [Wikipedia](#)).

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

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

7. Click **OK**.
8. Click **Apply**.

## Filtering messages on the server



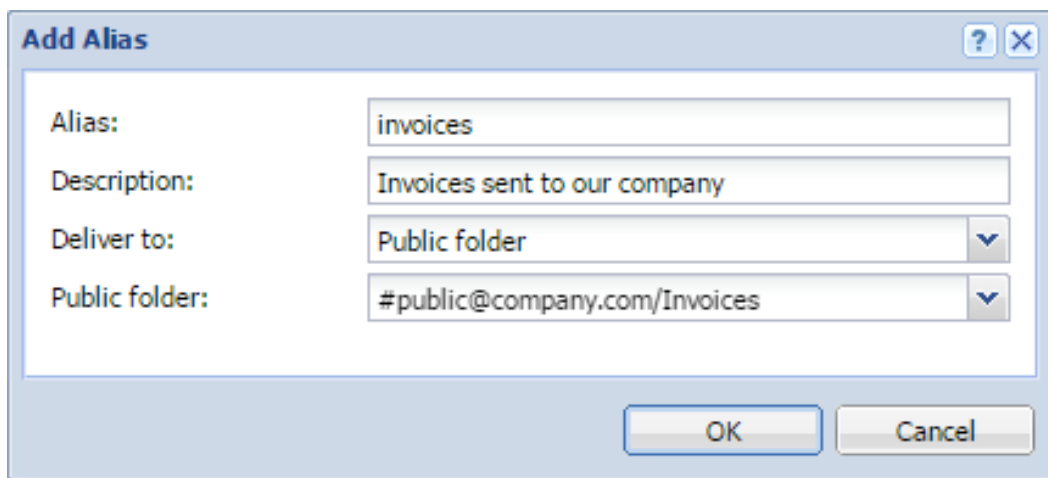
### Example 1 - Forwarding messages to public folders

To forward messages to public folders, you must create:

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

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

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



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



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

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

**Add Filter Rule**

Description: Forward messages with incoming invoices to public folder

All of the following conditions must be met:

Recipient	Equals	accounting@company.com	✕
Subject	Contains	invoice	✕
Has an attachment			+ ✕

Perform the following actions:

Redirect to address	invoices@company.com	+
---------------------	----------------------	---

Stop any other rules

Enable rule

**i** Header values can be reused by placeholders, e.g., "Re: \${Subject}".

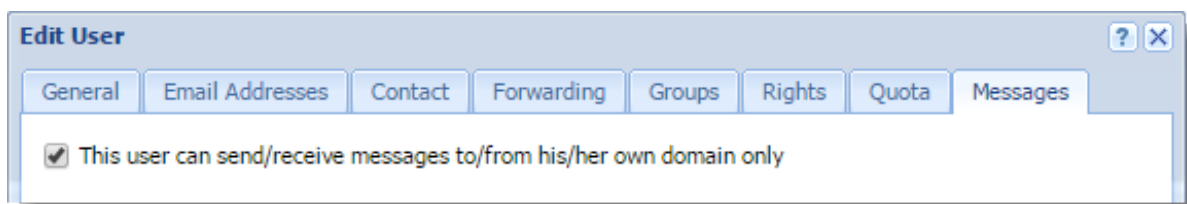
OK Cancel



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

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

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



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

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

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



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

- Delivers the message to the recipients from the user's domain
- Rejects to deliver to message to recipients outside the user's domain

If you create the same rule in the **Incoming rules** section, neither remote nor local recipients get the message.

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

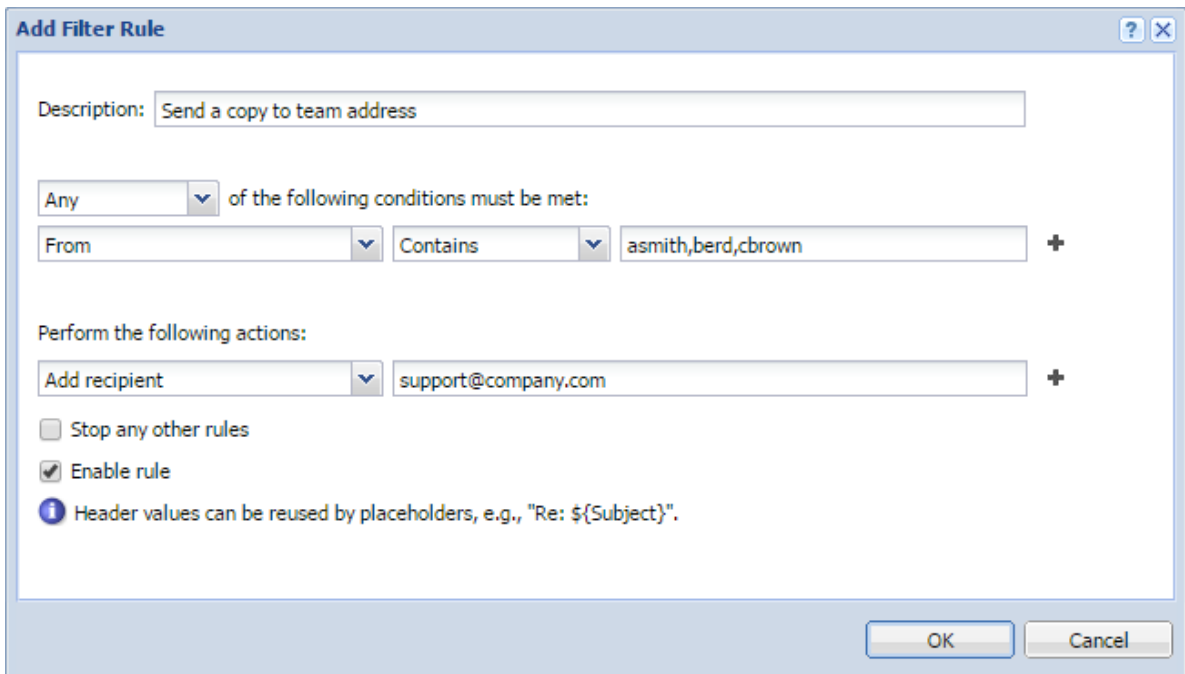
A team of support technicians help customers solve their problems. They communicate via their email addresses:

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

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

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

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





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

### Example 4 - Rejecting messages with large attachments

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

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

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



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

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



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

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



**Add Filter Rule**

Description: Messages with large attachments

All of the following conditions must be met:

- Has an attachment
- Message size Over 100 MB

Perform the following actions:

- Reject message: Your email message contains a large attachment. The message cannot be delivered.

Stop any other rules  
 Enable rule  
*Header values can be reused by placeholders, e.g., "Re: \${Subject}".*

OK Cancel



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

All of the following conditions must be met:

- Has an attachment
- Message size Over 100 MB
- Recipient Equals jsmith@company.com

Perform the following actions:

- Discard message

## Examples 5 - Sending an auto-reply message

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

1. In the **Incoming rules** section, click **Add**.
2. Set the condition to **Recipient** → **Equals** → **support@company.com**.

## Filtering messages on the server

---

3. Set the action to **Auto-reply** and type the text.
4. Click **OK** and **Apply**.

**Add Filter Rule** [?] [X]

Description:

Any [v] of the following conditions must be met:

Recipient [v] Equals [v]  +

Perform the following actions:

Auto-reply [v]  +

Stop any other rules

Enable rule

Header values can be reused by placeholders, e.g., "Re: \${Subject}".

OK Cancel

# Public folders in Kerio Connect

---

## Overview

Public folders are folders available to all users in a domain or the whole server. You can create public folders of these types:

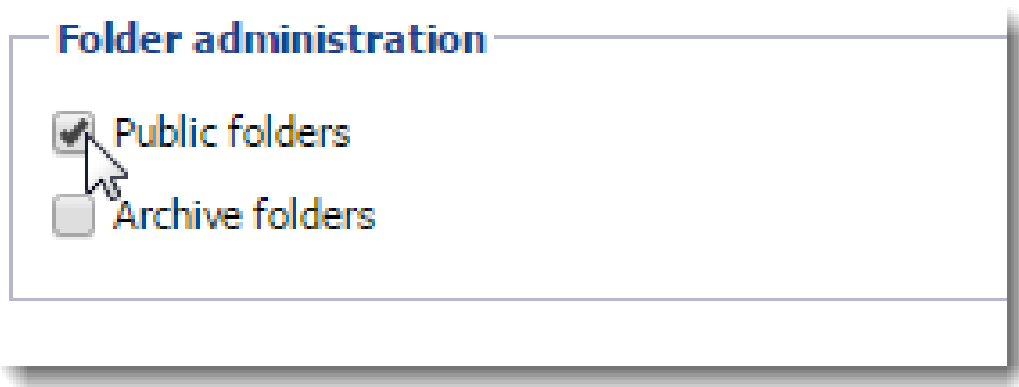
- Mail
- Calendar
- Contacts
- Tasks
- Notes

You can create public folders in Kerio Connect Client or Microsoft Outlook.

To create or edit public folders, users must have [appropriate admin rights for public folders](#) assigned (see below).

## Assigning administrator rights to manage public folders

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



4. Click **OK**.

### Global vs. domain public folders

In Kerio Connect, public folders can be:

- **Unique for each domain**
- **Global for all domains**

### *Sharing in Kerio Connect Client*

Users can share folders across all domains in Kerio Connect:

- **Unique** public folders — Users must write the whole email address when they want to share folders with users from other domains on the server.
- **Global** public folders — Kerio Connect Client automatically offers users from the other domains on the server in the [sharing dialog](#).

### *Chat in Kerio Connect Client*

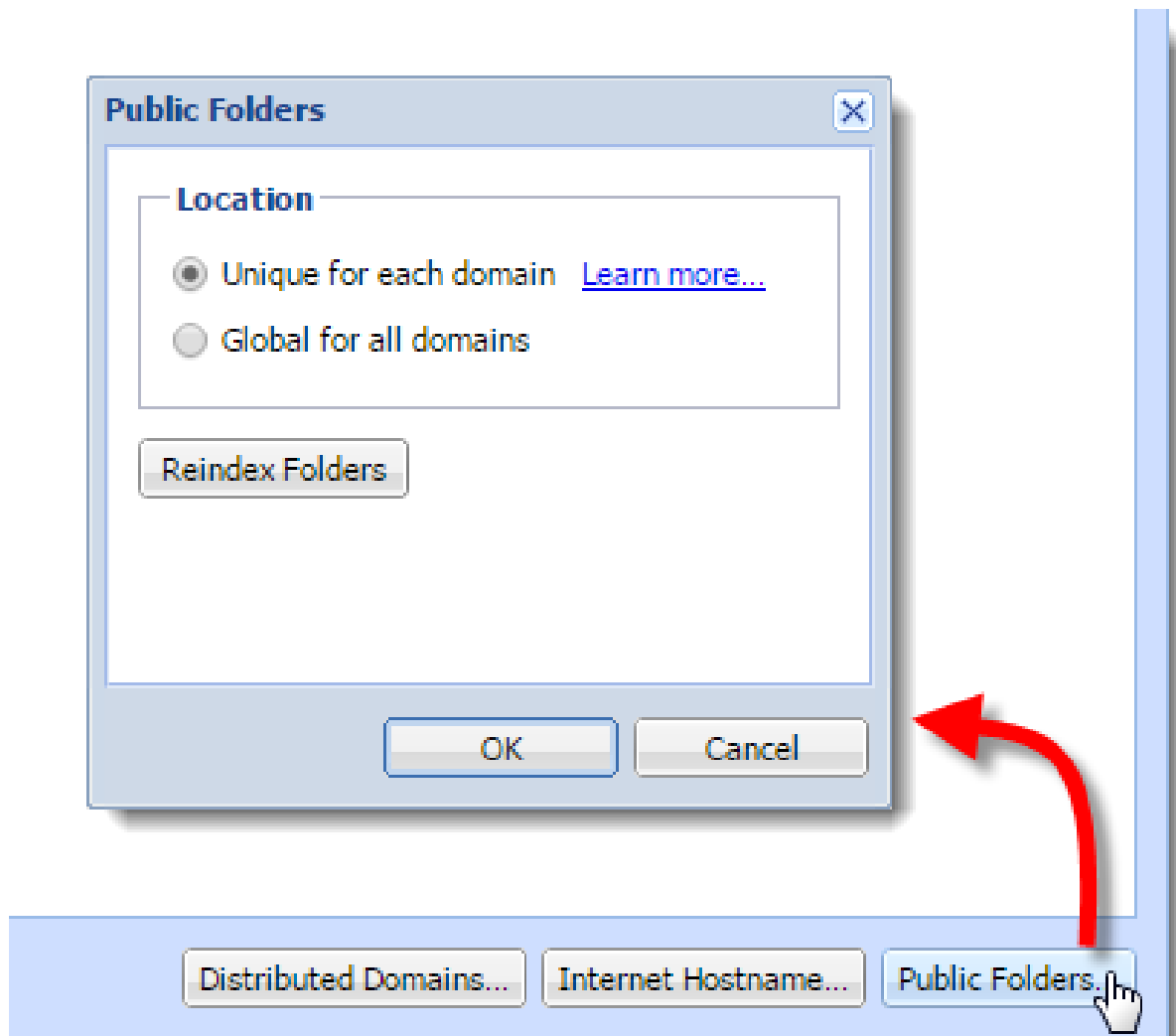
The contacts that users can chat with depend on the public folder settings:

- **Unique** public folders — You can chat only with users from your own domain
- **Global** public folders — You can chat with all users from all domains on the server

### Configuring public folders

To select the type of public folders:

1. Go to the administration interface to the **Configuration** → **Domains** section.
2. Click the **Public Folders** button in the right bottom corner.
3. Select the public folder type.
4. Click **OK**.

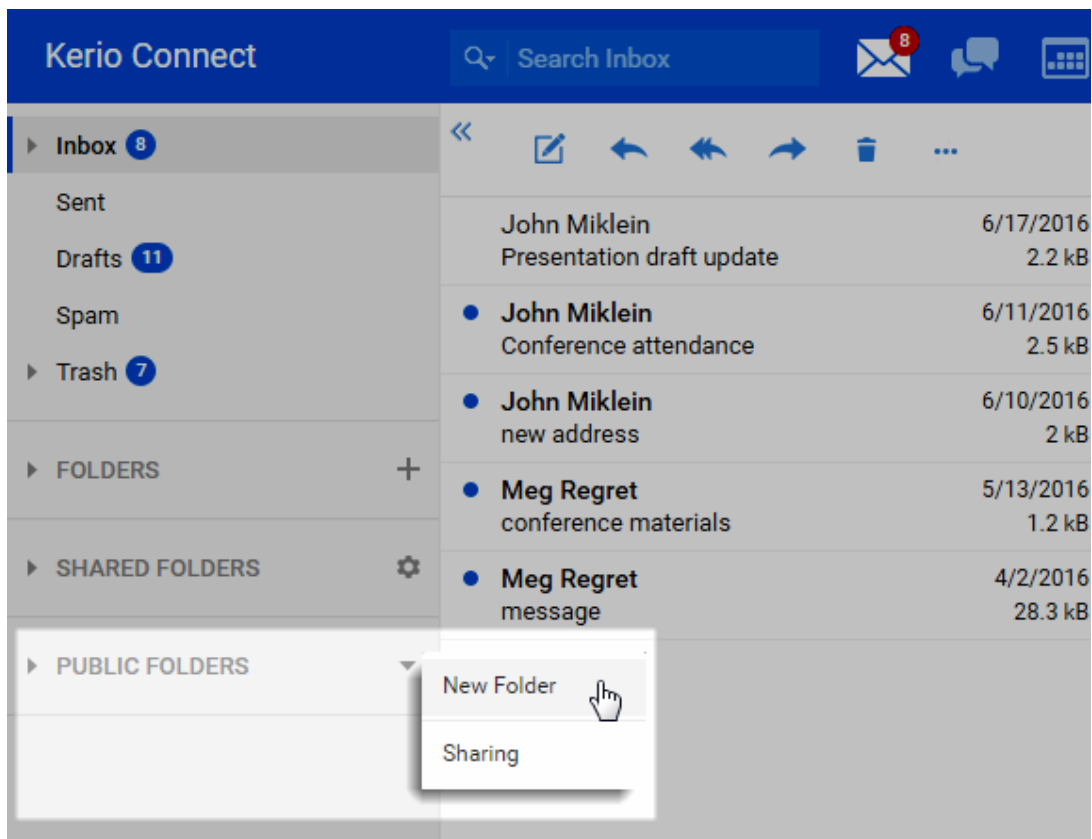


If you switch the public folder type after public folders has already been created, you must create new public folders — users will not be able to see the old ones.

Read [How to change from individual public folders to global public folders and keep your existing public folder data](#) for additional information.

## Creating public folders in Kerio Connect Client

1. Go to your Kerio Connect Client.
2. In the left folder tree, right-click **Public folders** and select **New Folder**.



3. Type a name for the public folder.

By default, all users from the domain can view public folders. To change the sharing rights, read article [Sharing in Kerio Connect Client](#).



Microsoft Outlook has a similar procedure.

### Viewing public folders

All public folders are automatically displayed in Kerio Connect Client and other clients.

See the following table for detailed information:

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

**Table 1** Viewing public folders in individual account types

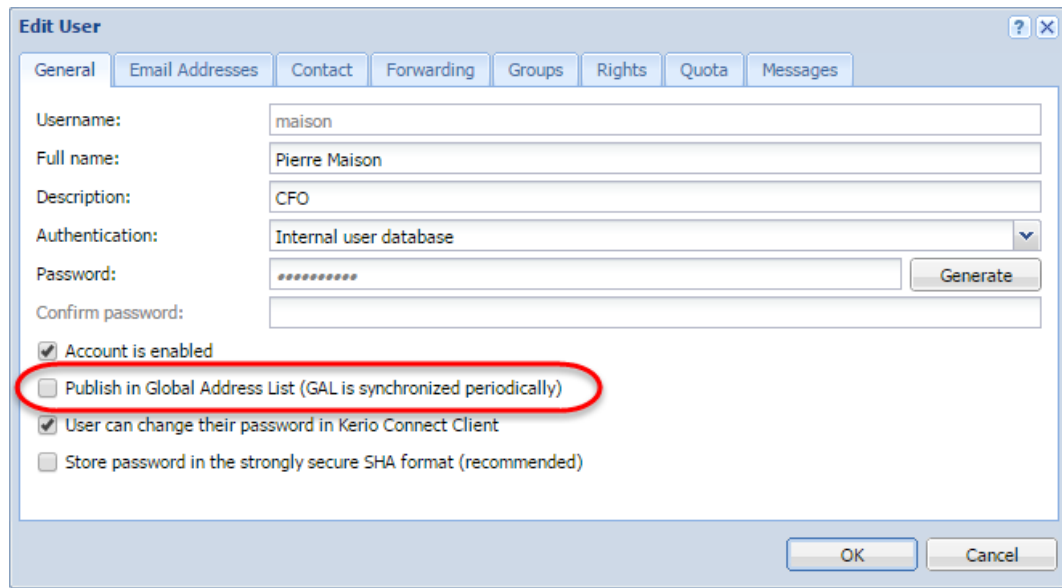
## Global Address List

Kerio Connect can automatically add users to a public contacts folder which is used as an internal source of company contacts.

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

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

## Public folders in Kerio Connect



The screenshot shows the 'Edit User' dialog box with the following fields and options:

- Username: maison
- Full name: Pierre Maison
- Description: CFO
- Authentication: Internal user database
- Password: [masked]
- Confirm password: [empty]
- 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)

Buttons: OK, Cancel, Generate



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



# How to change from individual public folders to global public folders and keep your existing public folder data

---

## Changing to global folders

When you change the type of public folders, users cannot access the previously created public folders.

To change to global public folder and keep the content of your old domain public folders:

1. [Change the public folders to global folders.](#)
2. Stop Kerio Connect.
3. Go to your Kerio Connect installation directory to the **Mail** folder. The default locations are:
  - **Mac OS X:** /usr/local/kerio/mailserver/store/mail
  - **Red Hat/SuSE:** /opt/kerio/mailserver/store/mail
  - **Windows:** C:\Program Files\Kerio\MailServer\Store\Mail
4. For each domain, go to a domain folder and copy the contents of the **#public** folder to the **#public** folder in the **Mail** folder.



All folders must have unique names. If any folders have the same name, you must rename them to prevent the data to be overwritten.

5. Start Kerio Connect.



Users with Kerio Outlook Connector (Offline Edition) must either clear the KOFF cache (in control **Panel** → **Mail** → **Email Accounts**) or re-create their profiles.

# Enabling chat in Kerio Connect Client

---

## Overview



New in Kerio Connect 9.1!

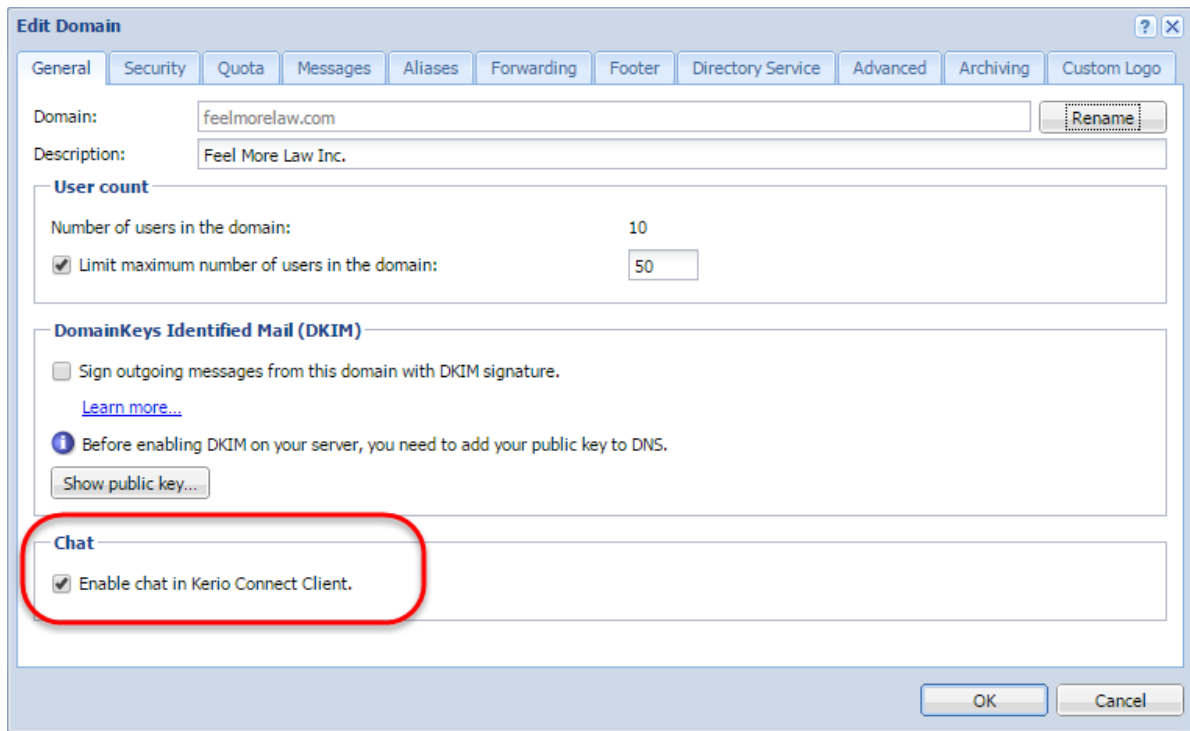
Kerio Connect Client includes a **Chat** feature for exchanging instant messages. Chat enables users to view their colleagues' online status, and to chat with them in real time. This is useful when they cannot wait for an email response or prefer a quick back-and-forth conversation without the use of a phone.

Administrators must enable chat for individual domains. Users can then enable/disable chat in their Kerio Connect Client settings.

Chat in Kerio Connect Client is an additional option to using a [XMPP/Jabber application](#).

## Enabling chat for individual domains

1. In the administration interface, go to **Configuration** → **Domains**.
2. Double-click a domain.
3. On the **General** tab, select **Enable chat in Kerio Connect Client**.  
To disable chat, deselect the option.
4. Click **OK**.



### ***Enabling chat among all domains on the server***

The contacts users can chat with depend on the [public folder](#) settings on your server:

- **Unique** public folders enable them to chat only with users from within their own domain.
- **Global** public folders enable all users from all domains on the server to chat with one another.

### **Archiving Kerio Connect Client chat messages**

Chat messages can be archived for future reference. See [Archiving chat in Kerio Connect Client](#) for more information.

### **Using Kerio Connect Client chat**

For additional information about chat, see [Sending chat messages in Kerio Connect Client](#).

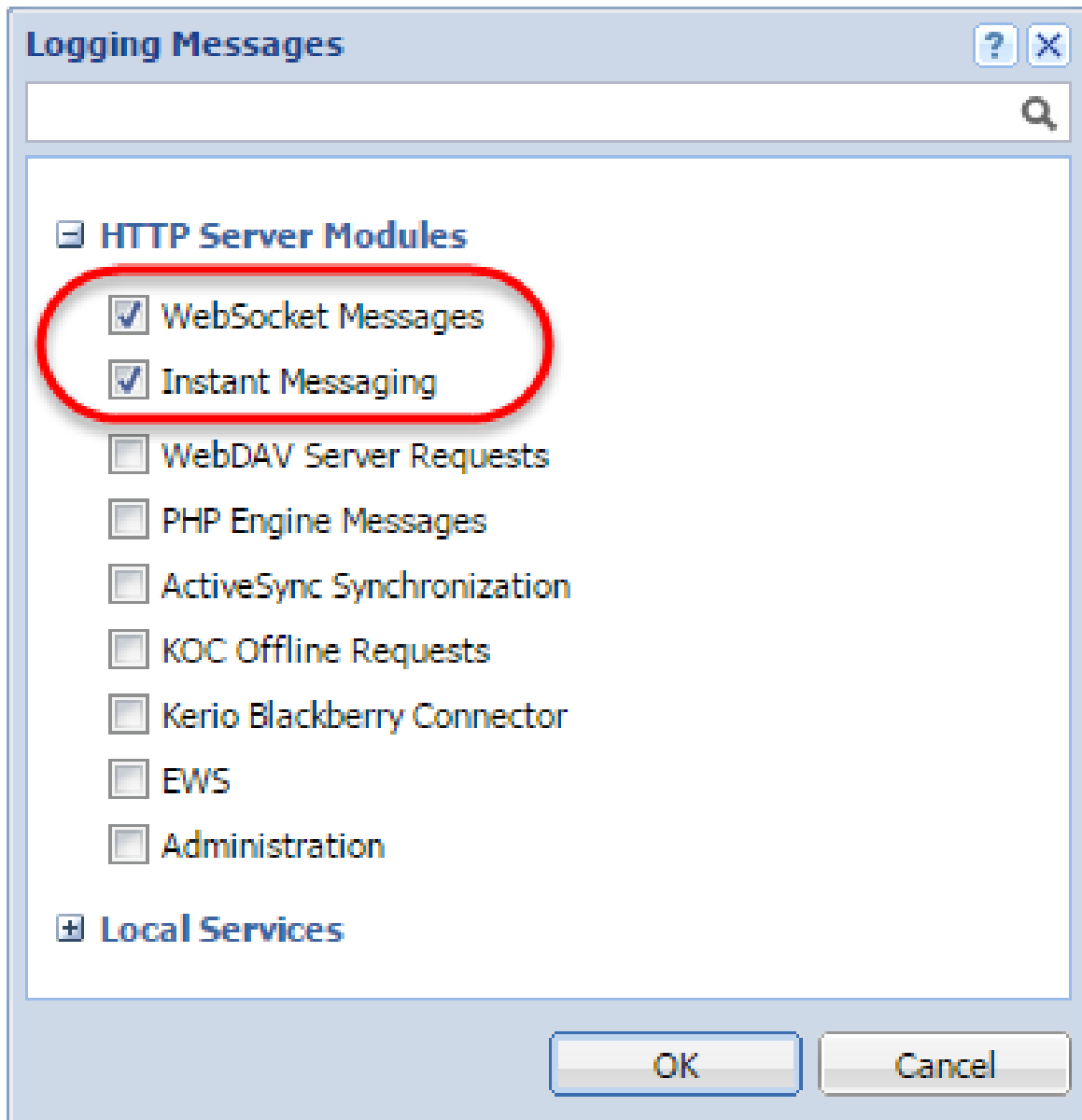
### Troubleshooting

If any problem with Kerio Connect Client chat occurs, consult the following [logs](#):

- **Warning**
- **Error**
- **Debug**
  1. Right-click in the Debug log area, and click **Messages**.
  2. Select the **Instant Messaging** and **WebSocket Messages** options.
  3. Click **OK**.



After debugging, clear those options. Otherwise, the logging may slow down server performance.



# Configuring instant messaging in Kerio Connect

## Overview



For information about enabling chat messages through Kerio Connect Client, read [Enabling chat in Kerio Connect Client](#).

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**.

Domain	DNS A	DNS SRV client	DNS SRV server	XMPP ping
feelmorrelaw.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**).

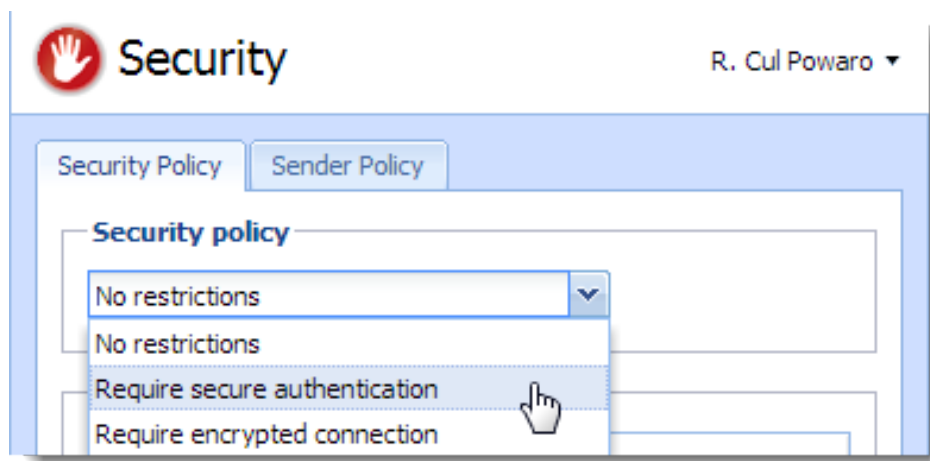


Remember to [configure DNS for instant messaging](#).

## 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)



## Configuring instant messaging in Kerio Connect

---

- 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	<a href="#">Add restriction</a>

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](#)).



## Archiving instant messages

For information about archiving instant messages, read article [Archiving instant messaging](#).

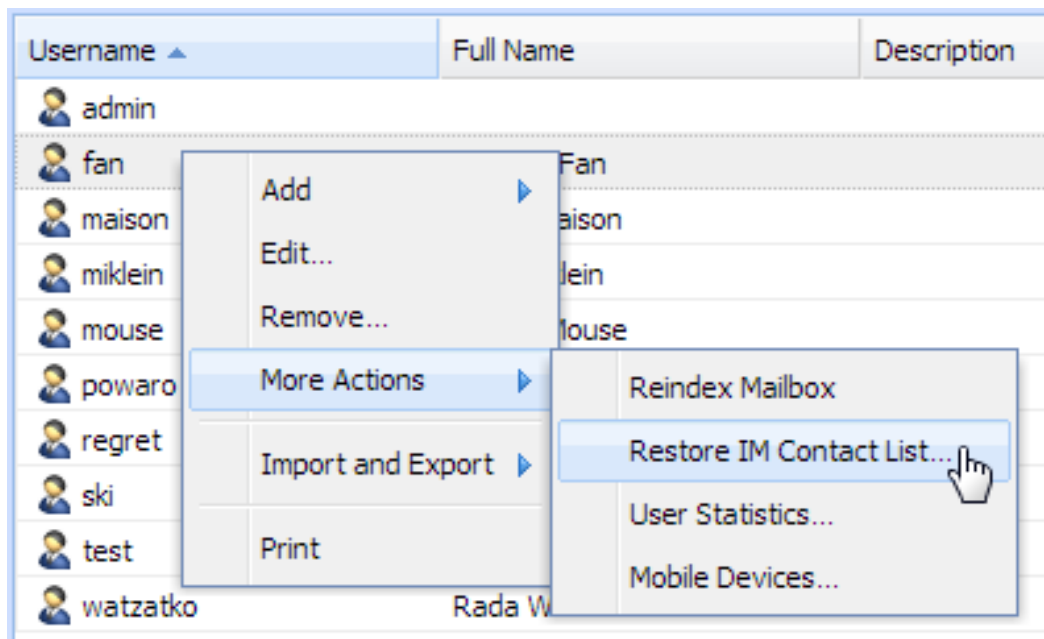
### Automatic contact list

Kerio Connect automatically creates contact lists of all domain users who are published in the [global address list](#).

Once users login to an [IM client](#), their account will display list of contacts of users from their domain (**Colleagues**).

If a user is having problems with their contact list (e.g. if they delete any users), you can restore their contact list:

1. In the administration interface, go to section **Accounts** → **Users**.
2. Right-click the user and select **More Actions** → **Restore IM Contact List**.
3. Confirm.



Restoring contact lists discards any changes the user has made to their **Colleagues** list. Added contacts will remain preserved.

## Configuring instant messaging in Kerio Connect

---

### *Maximum size of the automatic contact list*

Maximum number of users in the automatic contact list is set to 300. The users who exceed this number are not included in the **Colleagues** contact list and also their contact list is empty.

To change the maximum size of the contact list:

1. Stop the Kerio Connect engine.
2. Open the `mailserver.cfg` file.
3. Edit the following line:

```
<variable name="RosterMaximum">300</variable>
```

To disable the automatic contact list completely, set the `MaximumRoster` value to 0 (zero).

4. Save the file.
5. Start the Kerio Connect engine.

Kerio Connect saves the information about exceeding the maximum number of users in the [Warning log](#).



The size of the contact list affects the performance of the server. We recommend the following RAM size for the different contact list sizes:

- 0-100 users — 256 MB
- 100-200 users — 384 MB
- 200-500 users — 768 MB
- 500+ users — 2048 MB

## Configuring IM clients

For recommended clients and their configuration, read article [Configuring clients for instant messaging](#).

## Troubleshooting

If any problem regarding instant messaging occurs, consult the [Debug log](#) (right-click the Debug log area and enable **Messages** → **Instant Messaging Server**).

If you [rename a domain](#), users must re-configure their IM clients. All previous changes to their contact list will be lost.

# Configuring DNS for instant messaging

---

## About SRV records

SRV (service) records are entries in your DNS which specify the location of service servers. You must configure SRV records to make instant messaging in Kerio Connect accessible from other servers.

There are two types of SRV records:

- xmpp-server — necessary if you enable sending messages [outside of your domain](#)
- xmpp-client

Go to the Kerio Connect administration (**Configuration** → **Instant Messaging**) to check if the SRV records for your domain are configured (for detailed information, read article [Configuring instant messaging in Kerio Connect](#)).

You must add SRV records on your DNS server or use the management interface of your DNS registrar to add the records.



Visit [XMPP wiki](#) or [Wikipedia](#) for more information on SRV records.

## Configuring DNS records for server to server communication

Follow this example to add a server SRV record to your DNS:

```
_xmpp-server._tcp.feelmorelaw.com. 18000 IN SRV 0 5 5269 mail.feelmorelaw.com.
```

<b>Service</b>	_xmpp-server
<b>Protocol</b>	_tcp
<b>Hostname/Name</b>	Your domain name
<b>Priority</b>	Priority of the target
<b>Weight</b>	Weight for records of the same priority
<b>Port</b>	5269
<b>Target/Value</b>	Your server hostname
<b>TTL</b>	Time to live value

## Configuring DNS for instant messaging

---

The following items can be changed:

- Domain name (feelmorelaw.com)
- Server hostname (mail.feelmorelaw.com)
- TTL (18000)
- Record priority (0)
- Record weight (5)



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 allows 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 mail.feelmorelaw.com.
```

<b>Service</b>	_xmpp-client
<b>Protocol</b>	_tcp
<b>Hostname/Name</b>	Your domain name
<b>Priority</b>	Priority of the target
<b>Weight</b>	Weight for records of the same priority
<b>Port</b>	Port for communication from client to server
<b>Target/Value</b>	Your server hostname
<b>TTL</b>	Time to live value

The following items can be changed:

- Domain name (feelmorelaw.com)
- Server hostname (mail.feelmorelaw.com)
- TTL (18000)

- Record priority (0)
- Record weight (5)
- Port 5222

# Archiving instant messaging

---

## Overview



To archive chat messages sent through Kerio Connect Client, read [Archiving chat in Kerio Connect Client](#).

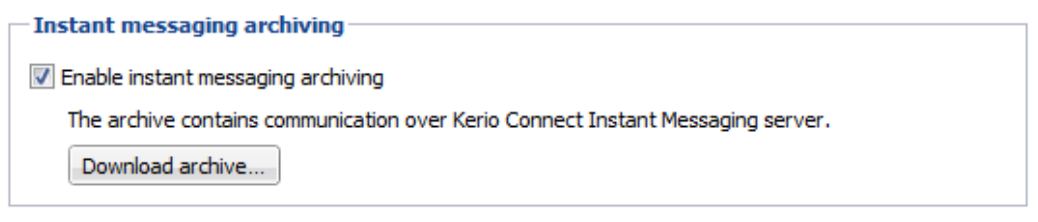
If you want to look at any instant message later, Kerio Connect can archive all [instant messages](#) sent to or from your users.

The archived data include:

- Local messages and messages sent to and received from outside of their domain
- Group chats
- File name and size of all files transferred over instant messaging

## Configuring instant messaging archiving

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → tab **Archiving**.
2. Select **Enable instant messaging archiving**.



3. Save the settings.

### Archive files

There are three types of archive files — \*.txt (current archive files), \*.zip (files which have reached the default file size), \*.part (temporary archive files).

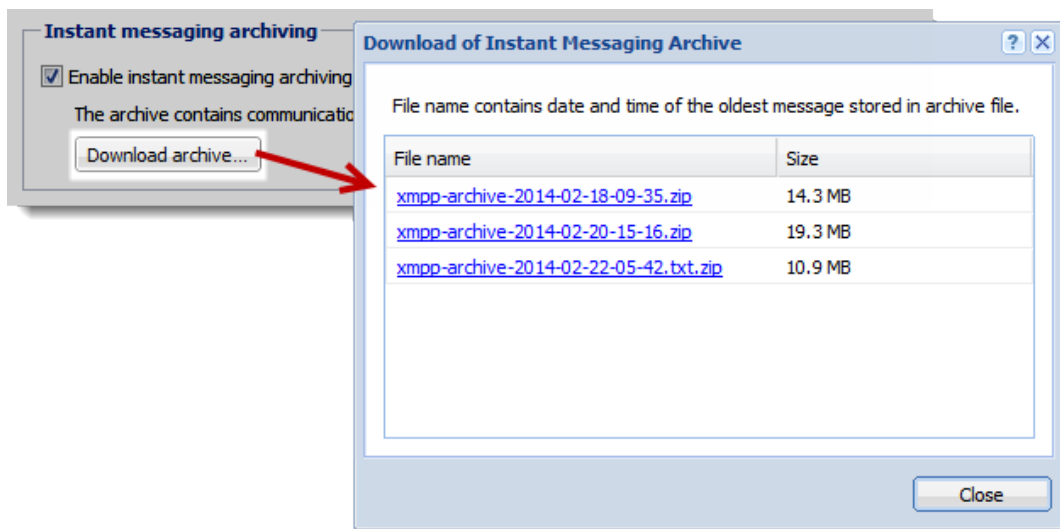
The default maximum size of the archive files is 50 MB. Once the archive file reaches 50 MB, a new file is created.

You can adjust the archive file size in the `mailserver.cfg` file in the installation folder of Kerio Connect (variable = `ArchiveFileSize`).

### Accessing the instant messaging archives

To download the instant messaging archive files from the administration interface:

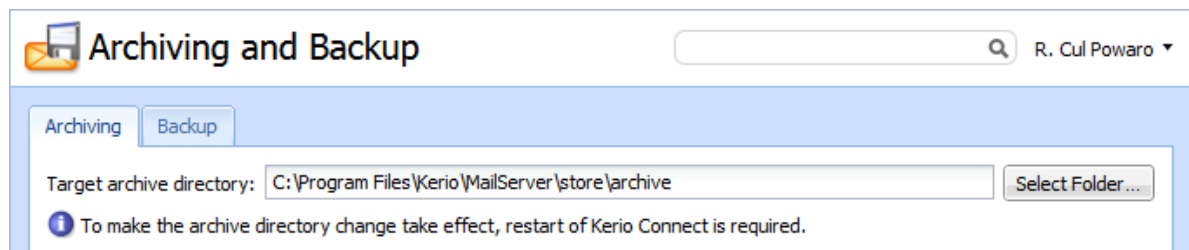
1. Go to **Configuration** → **Archiving and Backup** → **tab Archiving**.
2. In **Instant messaging archiving**, click **Download archive**.



This opens the list of available [archive files](#). The file name contains the date and time of the first message saved in this file.

3. Click any file name and save the file.

The instant messaging archives are stored in the [target archive directory](#) specified in **Configuration** → **Archiving and Backup** → **tab Archiving** in the `xmpp` folder.



# Customizing Kerio Connect

---

## About customization

In Kerio Connect, you can:

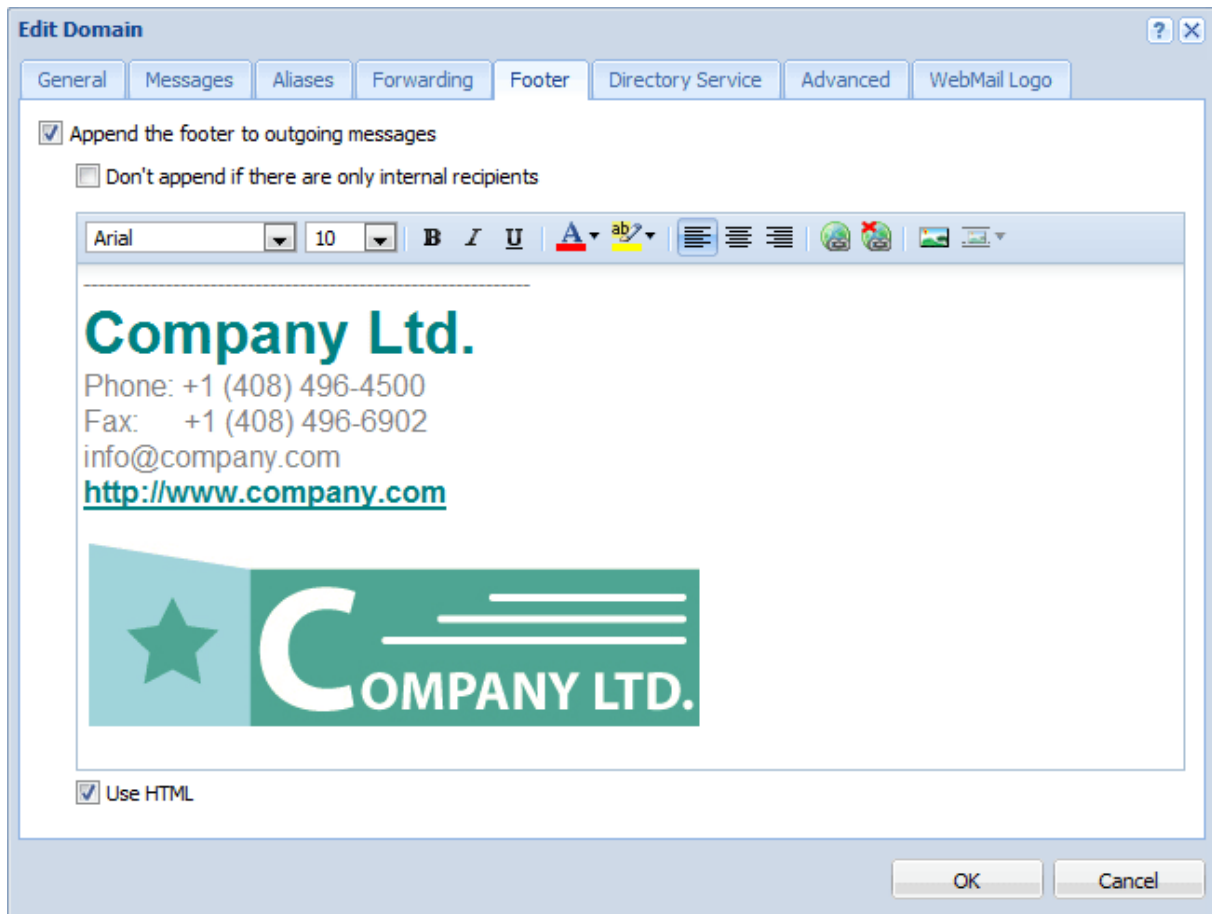
- [Define custom email footers](#)
- [Translate the interfaces into another language](#)
- Create a custom page for Kerio Connect Client (read [Customizing the Kerio Connect Client login page](#))
- [Add a custom logo to Kerio Connect Client](#)

## Defining custom email footers

For each domain, you can customize email footers that are automatically added to all messages sent from this domain.

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





If user defines [their own email signature](#), this domain footer is displayed below the user's signature.

When a user replies to a message, Kerio Connect places the domain footer below the whole conversation and the user's signature below the individual replies.



If users send [digitally signed](#) or [encrypted](#) messages, Kerio Connect does not append any footers to the message.

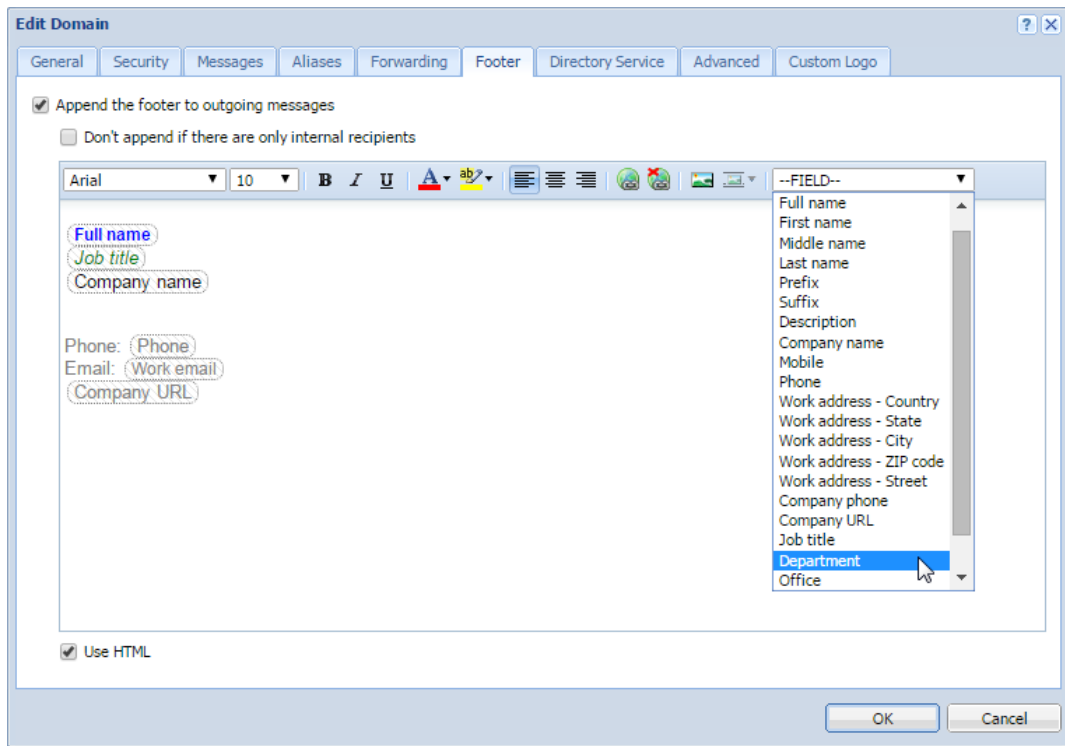
### Adding automatic user and company details to domain footers

You can use special field identifiers to add user and/or company details to the footer:

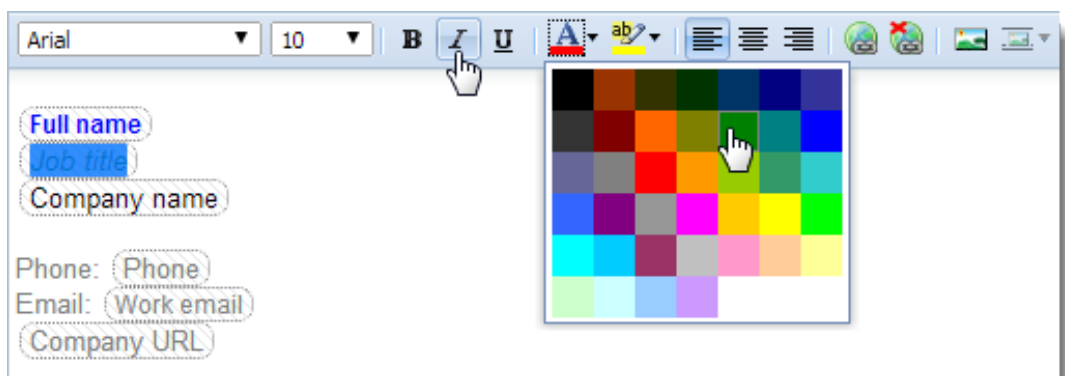
1. Fill in the information in the users' account details.
2. Create company locations.
3. In the administration interface, go to the **Configurations** → **Domains** section.

## Customizing Kerio Connect

4. Select a domain and click **Edit**.
5. Click the **Footer** tab.
6. Define the footer using items in the **Field** drop-down list.

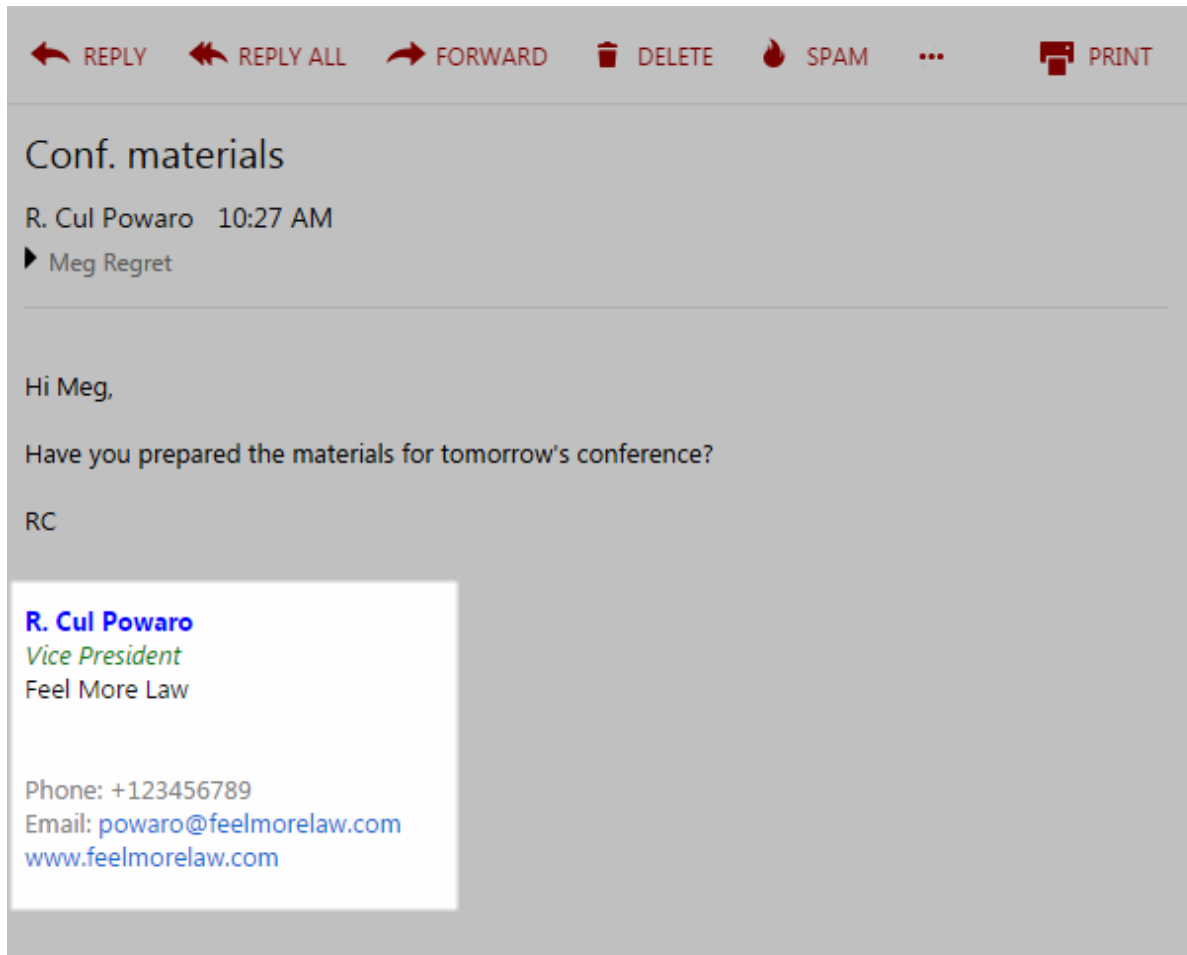


7. If you select the **Use HTML** option, you can format the fields: select the field and apply formatting attributes.



8. Click **OK**.

The final footer might look like this:



If users send **digitally signed** or **encrypted** messages, Kerio Connect does not append any footers to the message.

## Adding a custom logo to Kerio Connect Client

Kerio Connect Client displays a default logo in the top left corner.

For version 8.5 and newer, you can change the logo:

- Globally for all domains
- For each domain separately

If you set both logos, Kerio Connect Client displays the logo configured for a particular domain.

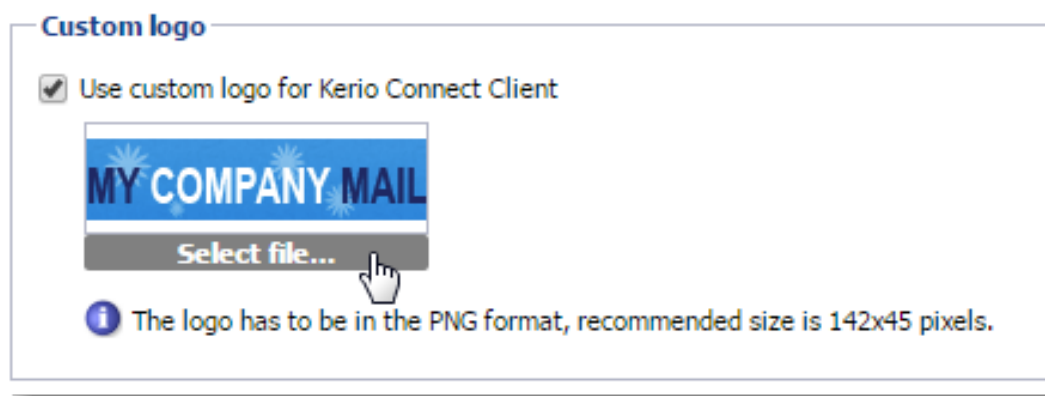
## Customizing Kerio Connect

---



### *Changing the logo for all domains*

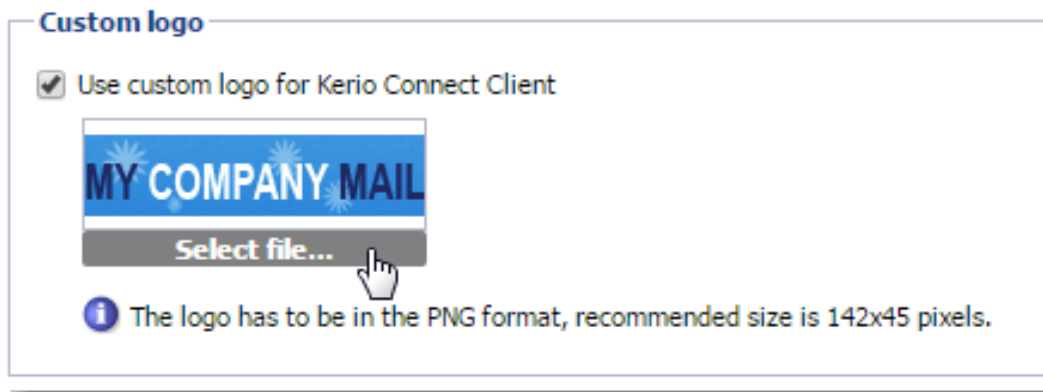
1. In the administration interface, go to **Configuration** → **Advanced Options** → **Kerio Connect Client**.
2. In the **Custom logo** section, select **Use custom logo for Kerio Connect Client**.
3. Click **Select file** and locate your image.



4. Click **Apply**.

### *Changing the logo for individual domains*

1. In the administration interface, go to **Configuration** → **Domains**.
2. Double-click a domain and go to the **Custom Logo** tab.
3. Select the **Use custom logo for Kerio Connect Client** option.
4. Click **Select file** and locate your image.



5. Click OK.

## Localizing the user interface

### Kerio Connect Client 8.1 and later

For detailed information on how to localize Kerio Connect Client, read [Translating Kerio Connect Client into a new language](#).

### Kerio Connect Client 8.0

You cannot add new translations to Kerio Connect Client 8.0. However, you can overwrite one of the existing translations:

1. Go to the installation directory of Kerio Connect.
2. Open the `web\webmail\translations` folder.
3. Select a language file to overwrite and open it in a text editor.  
The file contains both the source language (English) and the target language.
4. Translate into the target language.
5. Save the file and restart Kerio Connect.



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

# Customizing the Kerio Connect Client login page

---

## Overview

In Kerio Connect 8.4 and later, you can customize the login page for Kerio Connect Client.

You can change the login page for all domains created in your Kerio Connect, but not for individual domains.

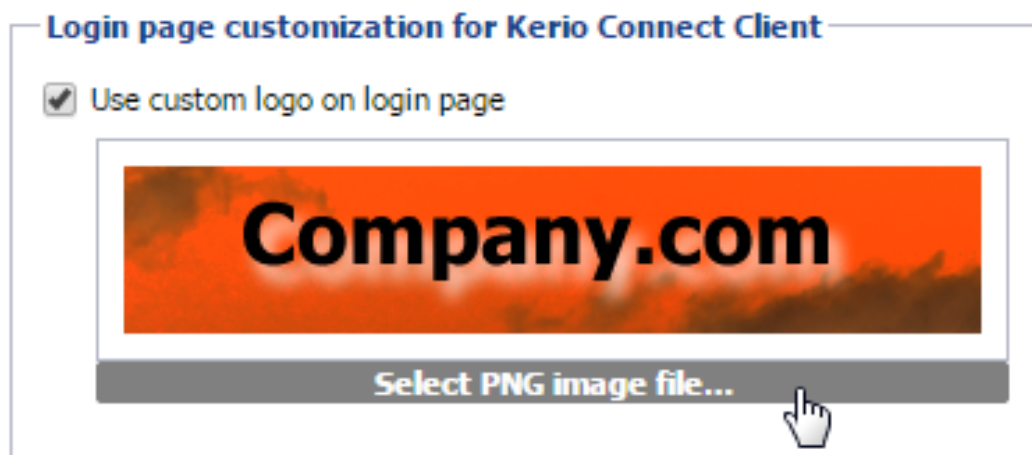


The login page of the administration interface does not change.

## Customizing the login page

1. In the administration interface, go to **Configuration** → **Advanced Options** → **Login Page** (**Configuration** → **Advanced Options** → **Kerio Connect client** in Kerio Connect 8.4).
2. Select the **Use custom logo on login page** option.
3. Click **Select PNG image file** and locate the new logo file.

The logo must be in the PNG format. The recommended maximum size is 328 x 80 pixels.



Kerio Connect immediately displays the login dialog in the **Login page preview**.

4.

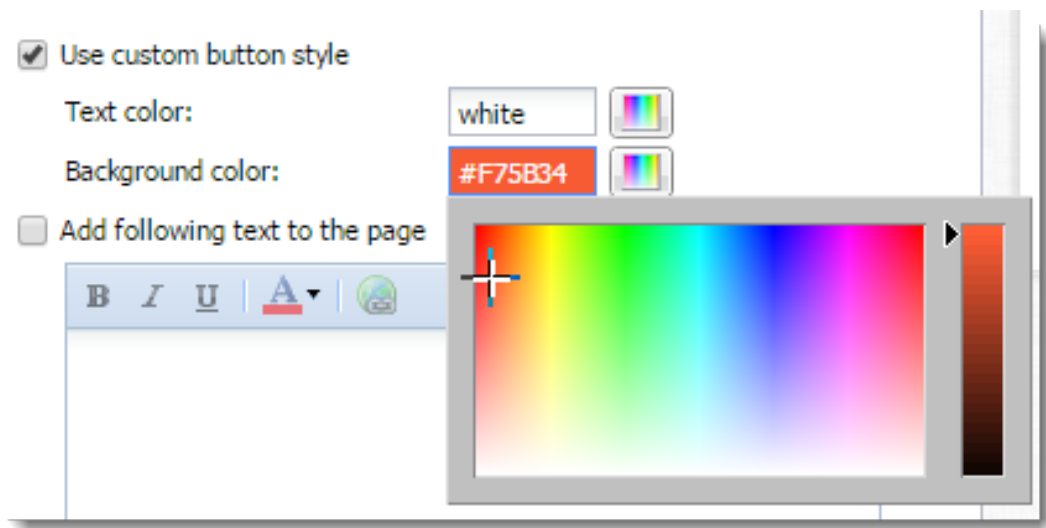


New in Kerio Connect 8.5!

Select **Custom button style** and select colors to change the button and text colors.

You can:

- Use the color picker
- Type a color's hex value
- Type a color name in English



Kerio Connect immediately shows your changes in the **Login page preview**.

5.



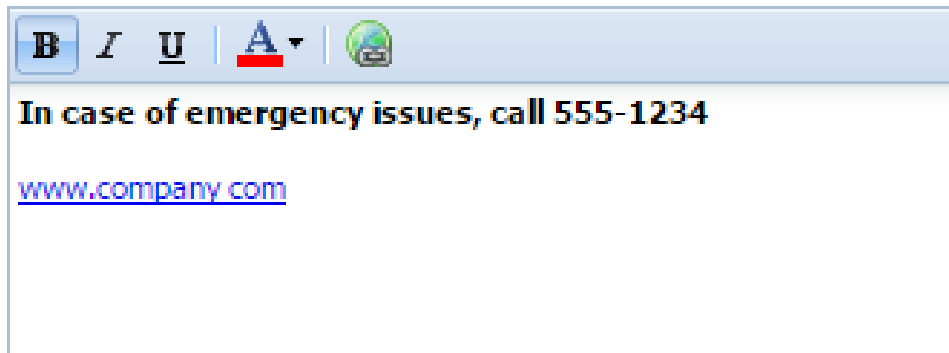
New in Kerio Connect 8.5!

Click **Add the following text to the page** to append text to the bottom of the the login page.

## Customizing the Kerio Connect Client login page

---

Add following text to the page

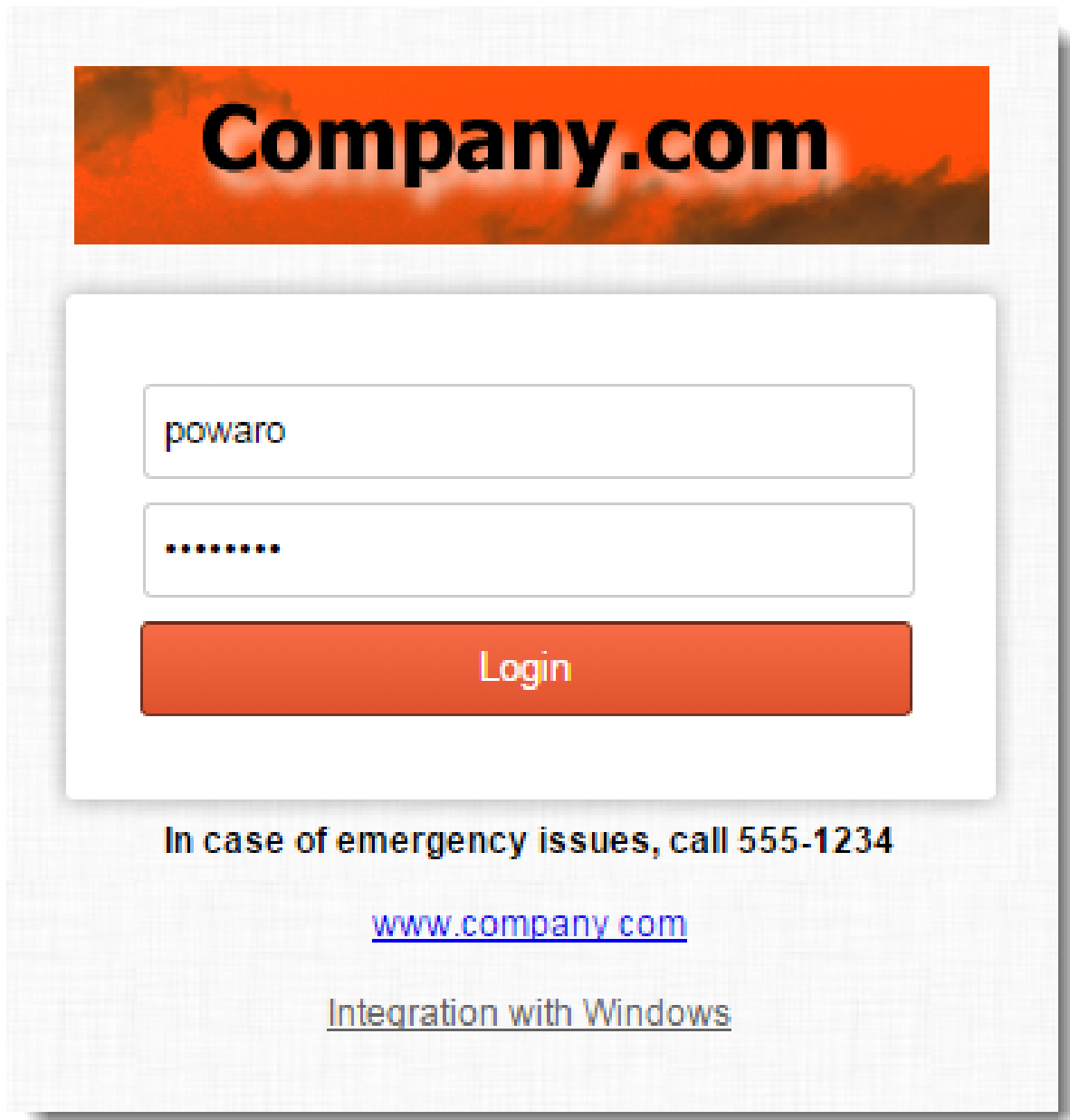


Kerio Connect immediately shows your changes in the **Login page preview**.

6. Save your settings.

Kerio Connect Client login pages for all your domains are now customized.





# Translating Kerio Connect Client to a new language

---

## Translating Kerio Connect Client for web



This article describes Kerio Connect 8.1 and newer. For information on translating Kerio Connect Client in version 8.0, read the [Customizing Kerio Connect](#) article. [Kerio Connect Client for Windows and Mac](#) cannot be translated to additional languages.

Translations of Kerio Connect Client are saved in several files in the installation directory of Kerio Connect. Files with localizations are named using 2-letter language codes.

To add a new language to Kerio Connect Client, follow these steps:

1. Go to the Kerio Connect installation directory to:
  - `web/webmail/translations`
  - `web/integration/translations`
2. Copy all files of one language (except English) and rename them according to the [target language code](#).
3. Rewrite the code and name of the new language in `xx_definitions.xml`.
4. Translate all strings to the new language in:
  - `xx_login.js`
  - `xx.js` from `web/webmail/translations`
  - `xx.js` from `web/integration/translations`



Do not change the structure of any file.

5. Restart Kerio Connect.

The new language is now available in [Kerio Connect Client for web](#).

## **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

---

## Setting the path to the data store directory

You configure the path to the data store during the [installation process](#).

To change the data store folder later:

1. Create a new folder for the data store.

Do not use diacritics and make sure there is enough [free space](#) for the data store.



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

2. In the administration interface, go to **Configuration** → **Advanced Options** → **Store Directory**.
3. Select the new folder.



Do not use a UNC path.

4. Click **Apply**.
5. Stop Kerio Connect.
6. Copy all files from the old store directory to the new one.
7. Run Kerio Connect.

**Advanced Options** Where is ... R. Cul Powaro

Miscellaneous | **Store Directory** | Master Authentication | HTTP Proxy | Software Updates | Kerio Connect Client | Login Page

**Directory location**

Path to the store directory:

**i** 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:

Index status: Rebuilding (26 users remaining)

Index size: 0 MB, 145697 MB of disk space available

**Storage space watchdog (minimum of free disk space required)**

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

Watchdog Hard Limit:    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:  %

If the warning limit is reached, send a message to the user:

If quota is reached, send a message to this address:

## Configuring the full text search

In Kerio Connect, users can search their items using the full text search feature.



The full text search can affect the performance of your server. The index file size is based on the number and size of the mailboxes, so make sure you have sufficient space on your disk before enabling this feature. For example, if you have many users with large mailboxes, the index file may occupy several gigabytes in total.

To enable the full text search feature on the server:

1. In the administration interface, go to **Configuration** → **Advanced Options** → **Store Direc-**

## Configuring data store in Kerio Connect

---

tory.

2. Select the **Enable full text search** option.
3. Specify a folder for storing the fulltext search index.



Do not use a UNC path.

The screenshot shows a window titled "Full text search". It contains the following elements:

- A checked checkbox labeled "Enable full text search".
- An "Index location:" label followed by a text input field containing the path `/opt/kerio/mailserver/store/fulltext` and a "Select Folder..." button.
- An information icon (i) with the text "Network storage is not recommended. [Learn more...](#)".
- An "Index status:" label followed by the text "Up-to-date".
- An "Index size:" label followed by the text "4260 MB".
- A "Rebuild Index..." button.

4. Click **Apply**.
5. To create a new index, click **Rebuild Index**.

You can rebuild the index for:

- All mailboxes from the server
- Single domain
- Single user

The screenshot shows a dialog box titled "Rebuild Index" with a question mark and close button in the top right corner. It contains the following elements:

- Three radio buttons for selection: "All mailboxes", "Domain:", and "User:". The "Domain:" option is selected.
- A dropdown menu next to "Domain:" showing the value "feelmorelaw.com".
- A text input field next to "User:" which is currently empty.
- A "Select..." button to the right of the "User:" input field.
- At the bottom, there are two buttons: "Start" and "Cancel". A mouse cursor is pointing at the "Start" button.

## Setting the data store notification limits

Kerio Connect can notify you when the free space in your data store folder has decreased.

Set the limits in the administration interface in the **Configuration** → **Advanced Options** → **Store Directory** section.

### Watchdog Soft Limit

If the free space on disk with the data store drops below this value, Kerio Connect displays a message in the administration interface.

### Watchdog Hard Limit

If the free space on disk with the data store drops below this value, Kerio Connect stops and displays a message in the administration interface.

Information about reached limits is logged in the [Error log](#).

Storage space watchdog (minimum of free disk space required)		
Watchdog Soft Limit:	<input type="text" value="1"/> GB	If the available disk space drops below this value, a warning message is displayed.
Watchdog Hard Limit:	<input type="text" value="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.

# Archiving in Kerio Connect

---

## Overview

Kerio Connect can archive messages on a local hard drive or to a remote email address.

You can archive:

- Local messages — local sender and local recipient
- Incoming messages — remote sender and local recipient
- Outgoing messages — local sender and remote recipient
- Relayed messages — remote sender and remote recipient

If you later need an old or deleted message, you can recover it by using [email recovery](#).



Archiving saves messages users send or receive after archiving is enabled. To save older messages, use the [backup](#) feature. Also use backups to store additional data (configuration, licenses, SSL certificates, etc.).

For information on archiving other types of communications, see:

- [Accessing the mailing list archive](#)
- [Archiving instant messaging](#)
- [Archiving chat in Kerio Connect Client](#)

## Configuring archiving

You can archive the whole server to a local hard drive and a remote email address.



Archiving to network drives is not supported.

In Kerio Connect 9.1 and newer, you can also archive each domain separately to a remote email address.

## Archiving the whole server

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → **Archiving**.
2. Select **Enable email archiving**.



3. To send the archive files to an email address, select **Archive to the remote email address** and type the address.
4. To save the archive files to a local hard drive, select **Archive to the local subfolder**, select the archiving interval, and specify the folder at the top of the section by clicking on **Select Folder**.
5. Select the types of messages you want to archive: local, incoming, outgoing, and/or relayed (see above).
6. To avoid the antispam and antivirus checks before archiving, select **Archive messages before applying the content filter check**.
7. Click **Apply** to save your settings.
8. Restart Kerio Connect if you have changed the archive folder.

**Archiving and Backup** Where is ...  R. Cul Powaro ▾

Archiving Backup

Target archive directory:  Select Folder...

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

**Email archiving**

Enable email archiving

Archive to the remote email address:

Archive to the local subfolder

Interval used for creating of new archive folders:  ▾

Compress old archive folders at:  (hh:mm)

---

Archive local messages (local sender, local recipient)

Archive incoming messages (remote sender, local recipient)

Archive outgoing messages (local sender, remote recipient)

Archive relayed messages (remote sender, remote recipient)

---

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

Enable additional archiving to a remote email address for domains

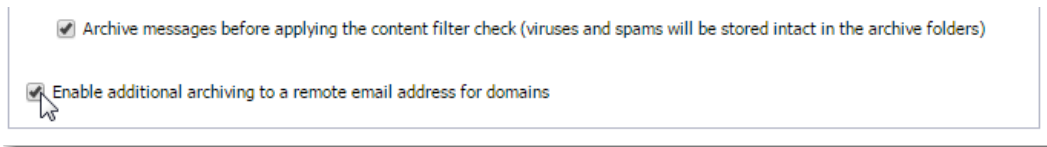
### Archiving individual domains



New in Kerio Connect 9.1!

## Archiving in Kerio Connect

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → **Archiving**.
2. Select **Enable additional archiving to a remote email address for domains**.

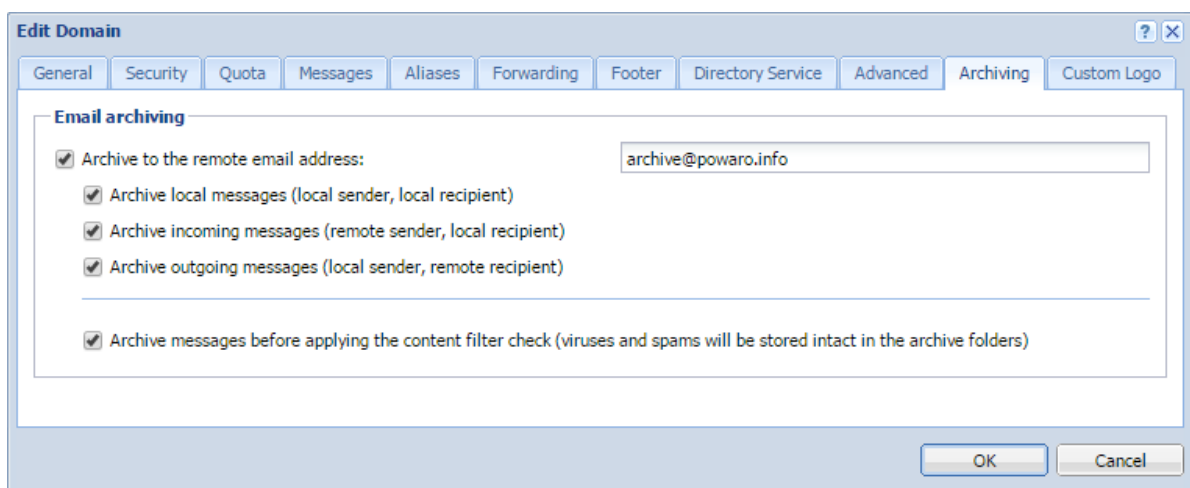


3. Click **Apply**.
4. Go to **Configuration** → **Domains**.
5. Double-click the domain you want to archive, and go to the **Archiving** tab.
6. Select **Archive to the remote email address** and type the email address.
7. Select the types of messages you want to archive: incoming, outgoing, and/or outgoing.



You cannot archive relayed messages.

8. To avoid the antispam and antivirus checks before archiving, select **Archive messages before applying the content filter check**.
9. Click **OK**.



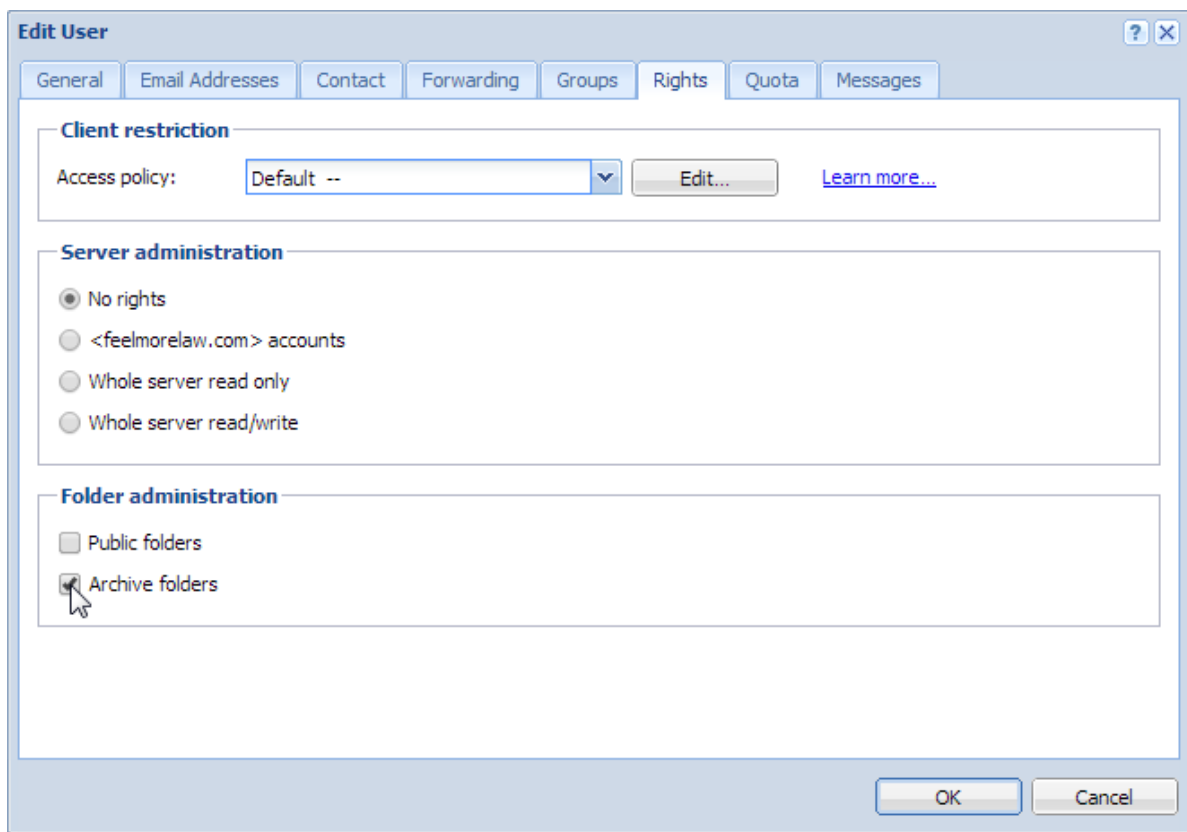
## Assigning administrator rights to view archive folders

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



Because all users' messages are archived, only trusted users should have access to the archive folders.

1. In the administration interface, go to **Accounts** → **Users**.
2. Double-click a trusted user and go to the **Rights** tab.
3. Select the **Public folders** option.
4. Click **OK**.



### Viewing archive folders

Whenever an archive folder is available for viewing, it is automatically displayed in the Kerio Connect Client of users with appropriate access rights.

# Configuring backup in Kerio Connect

---

## Overview

You can backup the following items in Kerio Connect:

- User mailboxes
- [Public folders](#)
- [Mailing lists](#)
- [Configuration files](#)
- [Licenses](#)
- [SSL certificates](#)
- [SpamAssassin database](#)
- [Contact lists in instant messaging](#)

You can use any removable or network disk for storing backups.

Configure backups in section **Configuration** → **Archiving and Backup**.



[Temporarily disabled users](#) are not included in the backups.

## Types of backups

In Kerio Connect, there are two types of backups:

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

You can schedule any number of full and differential backups. Consider the following:

- Size of the data store

The size influences the time each backup takes and its size.

- Importance of the data

When email communication and storing messages is important for your company, schedule more frequent backups.

## Configuring backup in Kerio Connect

**Archiving and Backup** Logout

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
<input checked="" type="checkbox"/> Differential	Wednesday	15:16	Differential backup
<input type="checkbox"/> Differential	Thursday	01:00	Differential backup
<input type="checkbox"/> Differential	Friday	01:00	Differential backup
<input type="checkbox"/> Differential	Saturday	01:00	Differential backup
<input checked="" type="checkbox"/> Full	Sunday	01:00	Full backup

**Target backup directory**

Backup directory:

**Notification**

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

**Current status**

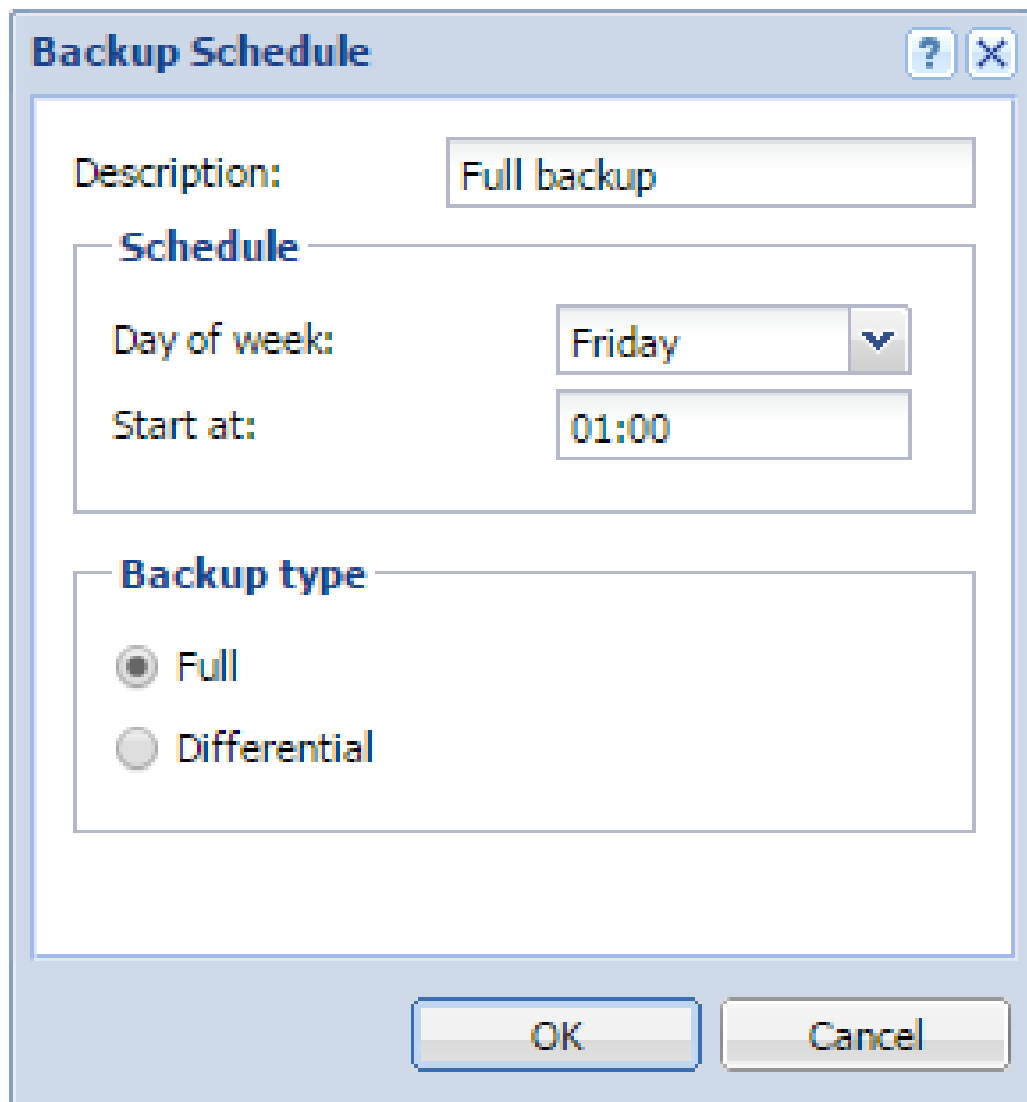
Last backup finished successfully.

### Configuring backups

You must have full access rights to administration or you can use the built-in administrator account. For more information on access rights, read the [Accessing Kerio Connect administration](#).

To configure the backup schedule:

1. In the administration interface, go to **Configuration** → **Archiving and Backup** → **Backup**.
2. Select the **Enable message store and configuration recovery backup** option.
3. Click **Add**.
4. Type a description for the backup.
5. Select the time and the type of the backup and click **OK**.

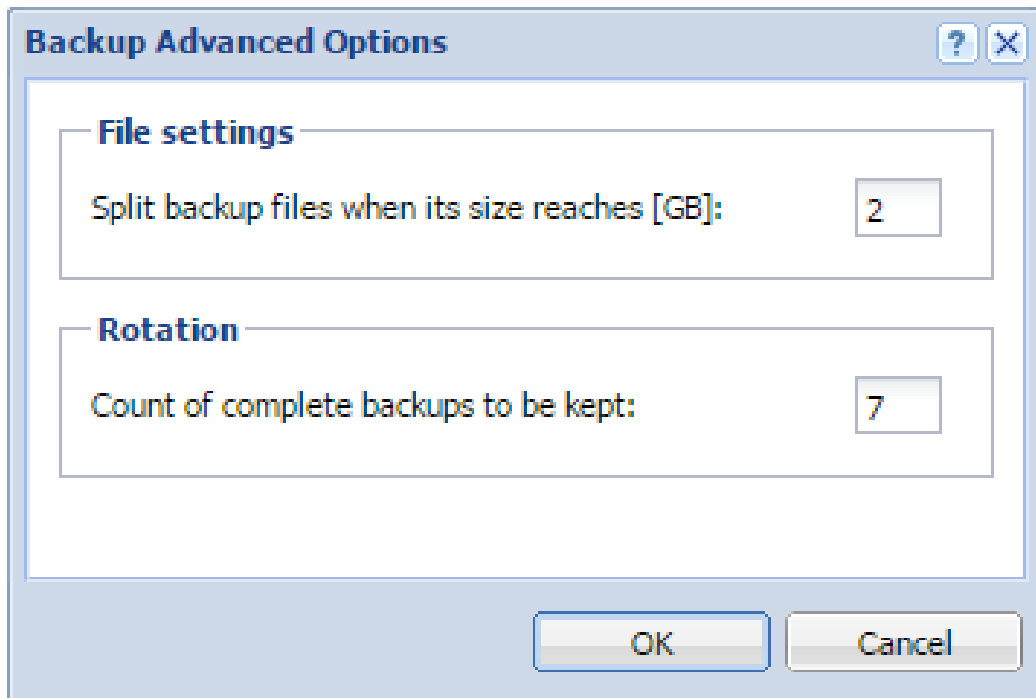


The image shows a Windows-style dialog box titled "Backup Schedule". It has a light blue border and standard window controls (help, close) in the top right corner. The dialog is divided into three sections:

- Description:** A text box containing "Full backup".
- Schedule:** A section containing:
  - Day of week:** A dropdown menu currently showing "Friday".
  - Start at:** A time input field showing "01:00".
- Backup type:** A section containing two radio buttons:
  - Full
  - Differential

At the bottom of the dialog are two buttons: "OK" and "Cancel".

- Repeat steps 3-5 for additional backups.
- Click the **Advanced** button and specify the maximum size and number of backups. Click **OK**.



8. In the **Target backup directory** section, specify the folder where to store all backups.

If the network drive requires authentication, click **Specify** and type the username and password (Microsoft Windows only).



No special characters allowed in the folder name.

9. In the Notification section, type your email address to receive notifications about backups.
10. Click **Apply**.

If you want to make an immediate full backup which is independent of your other backups, click the **Start Now** button.

### Recovering data from backups

To get instructions for data recovery, read [Data recovery in Kerio Connect](#).

### Data recovery examples

To read through some examples of data recovery, see [Examples of data recovery in Kerio Connect](#).



## Troubleshooting

If any problem with backups occurs, consult the [Debug log](#) (Right-click the Debug log area, click **Messages**, and select the **Store Backup** option).

# 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

#### Conditions:

- The configuration data is stored at the default location:  
C:\Program Files\Kerio\MailServer
- The store directory is located in directory on a separate disk:  
D:\store
- The backup directory is stored on an external disc:  
E:\backup

#### Solution:

1. Go to the Kerio Connect installation directory.

C:\Program Files\Kerio\MailServer

2. Run the `kmsrecover` command.

To recover from the **last complete backup** (the most recent full backup and all subsequent differential backup, or the most recent backup copy):

```
kmsrecover E:\backup
```

To recover from a **particular backup**:

```
kmsrecover E:\backup\F20051009T220008Z.zip
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.



If a parameter contains a space in the directory name, enclose it in quotes:  
`kmsrecover "E:\backup 2"`

### Recovering a single user's mailbox

#### Conditions:

- The configuration data is stored at the default location:  
`C:\Program Files\Kerio\MailServer`
- The backup directory is stored on an external disc:  
`E:\backup`
- The mailbox will be saved out of the Kerio Connect's store folder in the `D:\tmp` directory.

#### Solution:

1. Go to the Kerio Connect installation directory.

`C:\Program Files\Kerio\MailServer`

2. Run the `kmsrecover` command.

To recover from the **last complete backup** (the most recent full backup and all subsequent differential backup, or the most recent backup copy):

```
kmsrecover -d company.com -u smith -s D:\tmp E:\backup
```

To recover from a **particular backup**:

```
kmsrecover -d company.com -u smith -s D:\tmp E:\backup\F20051009T220008Z.zip
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.



If a parameter contains a space in the directory name, enclose it in quotes:  
`kmsrecover "E:\backup 2"`

### Recovering a single folder of a user

#### Conditions:

- The configuration data is stored

## Examples of data recovery in Kerio Connect

---

at the default location:

C:\Program Files\Kerio\MailServer

- The backup directory is stored on an external disc:  
E:\backup
- The Sent Items folder will be recovered.
- The recovery process will be monitored through the verbose mode.

### Solution:

1. Go to the Kerio Connect installation directory.

C:\Program Files\Kerio\MailServer

2. Run the kmsrecover command.

To recover from the **last complete backup** (the most recent full backup and all subsequent differential backup, or the most recent backup copy):

```
kmsrecover -v -d company.com -u smith -f "Sent Items" E:\backup
```

To recover from a **particular backup**:

```
kmsrecover -v -d company.com -u smith -f "Sent Items" E:\backup\F20051009T220008Z.zi
```

3. The kmsrecover detects the path to the store automatically in the Kerio Connect's configuration file and recovers the Sent Items folder.



If a parameter contains a space in the directory name, enclose it in quotes:  
kmsrecover "E:\backup 2"

## Recovering public folders of a particular domain

### Conditions:

- The configuration data is stored  
at the default location:  
C:\Program Files\Kerio\MailServer
- The backup directory is stored on an external disc:  
E:\backup
- The original public folders will also be kept.

**Solution:**

1. Go to the Kerio Connect installation directory.  
C:\Program Files\Kerio\MailServer
2. Run the kmsrecover command  
kmsrecover -b -d company -m public E:\backup
3. The kmsrecover detects the path to the store automatically in the Kerio Connect's configuration file and recovers the public folders.



If a parameter contains a space in the directory name, enclose it in quotes:  
kmsrecover "E:\backup 2"

**Examples for Mac OS X****Full backup recovery****Conditions:**

- The configuration data is stored at  
at the default location:  
/usr/local/kerio/mailserver
- The store directory is located in directory on a separate disk:  
/store
- The backup directory is stored on an external disc:  
/Volumes/backup

**Solution:**

1. Go to the Kerio Connect installation directory.

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

2. Run the kmsrecover command.

If the path to the Kerio Connect installation directory is included in the path variable:

```
kmsrecover /Volumes/backup
```

If the path to the Kerio Connect installation directory is NOT included in the path variable:

## Examples of data recovery in Kerio Connect

---

```
./kmsrecover /Volumes/backup
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

### Recovery of a single user's mailbox

#### Conditions:

- The configuration data is stored at the default location:  
`/usr/local/kerio/mailserver`
- The backup directory is stored on an external disc:  
`/Volumes/backup`
- The mailbox will be saved out of the Kerio Connect's store folder in the `/Temp` directory.

#### Solution:

1. Go to the Kerio Connect installation directory.

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

2. Run the `kmsrecover` command.

```
./kmsrecover -d company.com -u wsmith -s /Volumes/Temp /Volumes/backup/F20051009T220
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

### Recovery of a single folder of a user

#### Conditions:

- The configuration data is stored at the default location:  
`/usr/local/kerio/mailserver`
- The backup directory is stored on an external disc:  
`/Volumes/backup`
- The `Sent Items` folder will be recovered.
- The recovery process will be monitored through the verbose mode.

**Solution:**

1. Go to the Kerio Connect installation directory.

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

2. Run the kmsrecover command.

```
./kmsrecover -v -d company.com -u wsmith -f "Sent Items" /Volumes/backup/F20051009T2
```

3. The kmsrecover detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

**Recovery of public folders of a particular domain****Conditions:**

- The configuration data is stored at the default location:  

```
/usr/local/kerio/mailserver
```
- The backup directory is stored on an external disc:  

```
/Volumes/backup
```
- The original public folders will also be kept.

**Solution:**

1. Go to the Kerio Connect installation directory.

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

2. Run the kmsrecover command.

```
./kmsrecover -b -d company.com -m public /Volumes/backup
```

3. The kmsrecover detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

**Examples for Linux****Full backup recovery****Conditions:**

- The configuration data is stored at at the default location:

## Examples of data recovery in Kerio Connect

---

`/opt/kerio/mailserver`

- The store directory is located in directory on a separate disk:

`/store`

- The backup directory is stored on an external disc:

`/mnt/backup`

### Solution:

1. Go to the Kerio Connect installation directory.

`/opt/kerio/mailserver`

2. Run the `kmsrecover` command.

If the path to the Kerio Connect installation directory is included in the path variable:

```
kmsrecover /mnt/backup
```

If the path to the Kerio Connect installation directory is NOT included in the path variable:

```
./kmsrecover /mnt/backup
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

## Recovery of a single user's mailbox

### Conditions:

- The configuration data is stored at the default location:

`/opt/kerio/mailserver`

- The backup directory is stored on an external disc:

`/mnt/backup`

- The mailbox will be saved out of the Kerio Connect's store folder in the `/temp` directory.

### Solution:

1. Go to the Kerio Connect installation directory.

`/opt/kerio/mailserver`

2. Run the `kmsrecover` command.



```
./kmsrecover -d company.com -u wsmith -s /mnt/temp /mnt/backup/F20051009T220008Z.zip
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

### Recovery of a single folder of a user

#### Conditions:

- The configuration data is stored at the default location:  
`/opt/kerio/mailserver`
- The backup directory is stored on an external disc:  
`/mnt/backup`
- The `Sent Items` folder will be recovered.
- The recovery process will be monitored through the verbose mode.

#### Solution:

1. Go to the Kerio Connect installation directory.

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

2. Run the `kmsrecover` command.

```
./kmsrecover -v -d company.com -u wsmith -f "Sent Items" /mnt/backup/F20051009T22000
```

3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

### Recovery of public folders of a particular domain

#### Conditions:

- The configuration data is stored at the default location:  
`/opt/kerio/mailserver`
- The backup directory is stored on an external disc:  
`/mnt/backup`
- The original public folders will also be kept.

## Examples of data recovery in Kerio Connect

---

### Solution:

1. Go to the Kerio Connect installation directory.

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

2. Run the kmsrecover command.

```
./kmsrecover -b -d company.com -m public /mnt/backup
```

3. The kmsrecover detects the path to the store automatically in the Kerio Connect's configuration file and recovers all items.

# Data recovery in Kerio Connect

---

## Recovering data from backup

To recover the [backup data](#), use a special tool, **Kerio Connect Recover**. The tool extracts the backed-up data and saves the data in their original locations.

To launch Kerio Connect Recover:

1. Stop Kerio Connect.
2. Go to the Kerio Connect installation directory.
3. Run the following command from the directory:

```
kmsrecover [advanced options] <directory_name>|<file_name>
```

For Mac OS X and Linux, use `./kmsrecover [advanced options] <directory_name>|<file_name>` if the path to the Kerio Connect installation directory is included in the path variable.



If you don't specify any advanced options, , all items in the Kerio Connect's data store are overwritten.

4. To see details and example of individual options, run:

```
kmsrecover -h or kmsrecover --help
```

## 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		Recovers the specified folder of the user (requires setting of the -d and -u options).
-s	--store		Sets where SpamAssassin databases, mailing lists and emails (including events, notes, contacts, and so on) are unpacked and stored. By default, the <code>store</code> folder in the Kerio Connect installation directory is used.
-c	--cfgdir		Sets a directory for configuration files, SSL certificates and licenses. By default, the installation directory is used.
-m	--mask		Specifies which parts of the backup will be recovered. You must set the value of the mask with <code>-m &lt;value&gt;</code> or <code>--mask=&lt;value&gt;</code> . Example: <code>-m cfg,license,sslca,sslcert</code> . See the table below for values.
		cfg	This argument recovers only configuration files <code>mailserver.cfg</code> and <code>users.cfg</code> .

Abbreviation	Full option	Mask	Description
		mail	Recovers only the \store\mail directory.
		lists	Recovers only the configuration of mailing lists, the \store\lists directory.
		spamassassin	Recovers only the SpamAssassin database.
		license	Recovers the Kerio Connect license.
		sslca	Recovers SSL certificates issued by certification authorities.
		sslcert	Recovers the Kerio Connect certificates.
		public	Recovers public folders.
-b	--backup		Performs an additional back-up before the recovery starts. The original directory will have the BAK extension. If such file already exists, it is replaced by the new version. Verify that you have enough free disk space available, as this backup doubles the store size.
-g	--noprogess		Hides information about the recovery progress. (Recommended if the recovery is recorded in the log.)
-l	--listing		Lists the backup store content. You can also use additional parameters, such as -d and -u, which list only specific content.
-q	--quiet		Hides the recovery progress information in the command line.
-v	--verbose		Displays the recovery progress information in the command line.
-h	--help		Prints out the help file.

## Backup files

### File names

Each backup archive (ZIP) file name consists of the backup type abbreviation and the date when it was created:

### ***Full backup (F)***

F20120118T220007Z.zip

F — full backup

2012 — year

01 — month

18 — day

T220007Z — GMT timestamp (22:00:07); always starts with T and ends with Z.

### ***Differential backup (D)***

D20120106T220006Z.zip

D — differential backup

2012 — year

01 — month

06 — day

T220006Z — GMT timestamp (22:00:06); always starts with T and ends with Z.

### ***Backup copy/Manual backup (C)***

C20120117T084217Z.zip

2012 — year

01 — month

17 — day

T084217Z — GMT timestamp (08:42:17); always starts with T and ends with Z.

## **File content**

Each backup archive (ZIP) file includes the following files and directories:

- `.version.txt` is created at the start of the backup process and includes the following information:
  - `started` — Time the backup started (YYYY-MM-DD hh:mm:ss).
  - `version` — Version of the backup tool.
  - `hostname` — DNS name of the Kerio Connect host for which the backup was created.
- `@backup` is the main directory of the backup and includes the following items:

- `license` — License backup.
  - `sslca` — Backup of certificates of certification authorities.
  - `sslcert` — Backup of Kerio Connect's SSL certificates.
  - `store` — Backup of the data store
- `mailserver.cfg` is a file with the Kerio Connect and configuration contains all settings done in the administration interface.
  - `users.cfg` is a file with user configuration and contains all users and their parameters set in the Kerio Connect's administration interface.
  - `.summary.txt` is created at the end of the backup creation process and includes the following information:
    - `started` — Time the backup started (YYYY-MM-DD hh:mm:ss).
    - `finished` — Time the backup ended 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 between the creation of files `.version.txt` and `.summary.txt`.
    - `duration` — Total time of the backup creation process (hh:mm:ss:msms).

## Data recovery examples

To read through some examples of data recovery, see [this article](#).

## Troubleshooting

If any problem with backups occurs, consult the [Debug log](#) (Right-click the Debug log area, click **Messages**, and select the **Store Backup** option).

# Configuring SSL certificates in Kerio Connect

## Overview

To secure Kerio Connect by SSL/TLS encryption, you need a [SSL](#) certificate. SSL certificates authenticate an identity on a server.

Kerio Connect creates the first [self-signed certificate](#) during the installation. Upon the first login, users must confirm 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.

You can have one or more certificates for each domain configured in Kerio Connect.



If you want to use an existing SSL certificate from another service, export the existing SSL certificate and the public key in the PEM format and import them to Kerio Connect.

Manage certificates in the **Configuration** → **SSL Certificates** section .

Type ▲	Issuer	Subject	Expires
Active Certificate	mail.feelmorelaw.com	mail.feelmorelaw.com	2017-02-21
Active Certificate	*.feelmorelaw.com	*.feelmorelaw.com	2013-03-28
Request		feelmorelaw.eu	
Default Certificate	DigiCert High Assurance CA-3	*.feelmorelaw.com	2017-02-21



To make the communication as secure as possible, you can:

- Disable all unsecured [services](#) or
- Set an appropriate [security policy](#)



## Supported 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.

## Multiple certificates



New in Kerio Connect 9.0.2!

Since Kerio Connect 9.0.2, you can import certificates for different domains to Kerio Connect. Kerio Connect then selects and uses the appropriate certificate.

If multiple certificates exist for a single domain, Kerio Connect selects a certificate according to the following order:

1. Trusted certificate for the domain hostname.
2. Self-signed certificate for the domain hostname.
3. Valid certificate for the domain hostname.
4. Expired certificate for the domain hostname.
5. Trusted wildcard certificate.
6. Self-signed wildcard certificate.
7. Valid wildcard certificate.
8. Expired wildcard certificate.
9. Default server certificate.



If a certificate expires and you have already imported a new valid certificate to Kerio Connect for the same domain, delete the old certificate or restart the server to use the new valid certificate.

### Creating certificates

#### 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.
4. Click **OK**.

To enable the server to use this certificate, select the certificate and click on the **Set as Default** button (**Set as Active** in older versions).

#### Creating certificates signed by certification authority

To use a certificate signed by a trustworthy certification authority, you must first generate a certificate request, send it to a certification authority and import a signed certificate upon receiving it.

1. Open section **Configuration** → **SSL Certificates** and click on **New** → **New Certificate Request**.
2. Fill in the information and save.
3. Select the certificate and click on the **Export** → **Export Request** button.
4. Save the certificate to your disk and send it to a [certification authority](#).

Once you obtain your certificate signed by a certification authority, and click on **Import** → **Import Signed Certificate from CA**.

1. Go to section **Configuration** → **SSL Certificates**.
2. Click on **Import** → **Import Signed Certificate from CA**.
3. To enable the server to use this certificate, select the certificate and click on the **Set as Active** button.

#### Intermediate certificates

Kerio Connect allows authentication by **intermediate** certificates. To make authentication by these certificates work, follow these steps to add the certificates to Kerio Connect:

1. In a text editor, open the server certificate and the intermediate certificate.
2. Copy the intermediate certificate below the server certificate into the server certificate file (\*.crt) and save.

The file may look like this:

```
-----BEGIN CERTIFICATE-----
MIID0jCCAqOgAwIBAgIDPmR/MA0GCSqGSIb3DQEBAUAMFMxCzAJBgNVBAYTAI
MSUwIwYDVQQKEExUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMR0wGwYDVQ
    .... this is a server SSL certificate ...
ukrkDt4cgQxE6JSEprDiP+nShuh9uk4aUCKMg/g3VgEMu1kR0zF16zinDg5grz
Qsp0QTEYoqrc3H4Bwt8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDMzCCApYgAwIBAgIEMAAAATANBgkqhkiG9w0BAQUFADCBxDELMAkGA1UEBh
WkExFTATBgNVBAGTDFd1c3R1cm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
    .... this is an intermediate SSL certificate which
        signed the server certificate...
5BjLqgQRk82bFi1uoG9bNm+E6o3tiUEDywrgrVX60CjbW1+y0CdMaq7d1pszRB
t14EmBxKYw==
-----END CERTIFICATE-----
```

3. In the administration interface, go to section **Configuration** → **SSL Certificates**.
4. Import the modified server certificate by clicking on **Import** → **Import New Certificate**.
5. Save the settings.



If you have multiple intermediate certificates, add them one by one to the server certificate file.

# Configuring SSL/TLS in Kerio Connect

---

## Overview



New in Kerio Connect 8.5!

Kerio Connect allows you to enable or disable specific security protocols and ciphersets manually for:

- Kerio Connect server in general
- SMTP services separately (for SMTP on port 25 and SMTPS on port 465)

You might need to adjust the security settings when a flaw in a security protocol is found or to get a good security rating for your server. (You can test your server, for example, at [Qualys SSLlabs test site](#)).

## Changing the SSL/TLS configuration

Kerio Connect uses different variables for the SSL/TLS protocols configuration. To change the configuration:

1. Stop the Kerio Connect engine.
2. Open the configuration file `mailserver.cfg` for editing  
See [Configuration files](#) for the default location.
3. Change the settings in the `Security` or `SmtpSecurity` sections.  
See the [list of variables](#) below.
4. Save the file.
5. Start Kerio Connect.

## Resetting the SSL/TLS configuration

To reset the SSL/TLS configuration in the configuration file:

1. Stop the Kerio Connect engine.
2. Open the configuration file `mailserver.cfg` for editing.

See [Configuration files](#) for the default location.

3. Delete any variable in the `Security` or `SmtpSecurity` sections.
4. Save the file.
5. Start Kerio Connect.

Kerio Connect sets the default values of all the SSL/TLS variables.

## List of variables

Kerio Connect uses eight variables for the SSL/TLS protocols configuration.

### *AllowEphemeralDH*



Changed in Kerio Connect 9.0.2!

The default value, **1**, enables the use of DHE (Ephemeral Diffie-Hellman) for key exchange.

The server generates a random ephemeral public key for each session so that attackers cannot decipher past sessions (this is also called “forward secrecy”).



This variable replaces **DisableEphemeralDH** in Kerio Connect 9.0.0 and 9.0.1. Set the **DisableEphemeralDH** to **0** to enable the use of DHE.

### *EphemeralDHParamSize*



New in Kerio Connect 9!

The default value, **0**, sets the size of DHE to 2048 (1024 for SMTP services). Make sure the **DisableEphemeralDH** is enabled.

You can change the default value to **1024**, **2048**, or **4096**

### *AllowEphemeralECDH*

The default value, **1**, enables ECDHE for key exchange.

## Configuring SSL/TLS in Kerio Connect

---

The server generates a random ephemeral public key for each session so that attackers cannot decipher past sessions. ECDHE is more efficient than [DHE](#) and uses shorter keys.

### *SSLDontInsertEmptyFragments*

The default value, **1**, disables the OpenSSL workaround for the CVE-2011-3389 vulnerability.

If you set the variable to **0**, some older implementations of SSL may not connect to Kerio Connect servers.

### *ServerTlsProtocols*

In this variable, you can change the SSL/TLS protocols used by Kerio Connect.

Leave the variable empty to use a default set of SSL/TLS protocols: TLSv1, TLSv1.1, TLSv1.2

To use a custom set of protocols, list the protocol names, separated by commas, in the variable.

For example: `<variable name="ServerTlsProtocols">SSLv3,TLSv1,TLSv1.1,TLSv1.2</variable>`■

### *ServerTlsCiphers*

In this variable, you can change the cipher list used by Kerio Connect.

Leave the variable empty to use a default cipher list:  
AESGCM:HIGH:+EDH-RSA-DES-CBC3-SHA:+EDH-DSS-DES-CBC3-SHA:+DES-CBC3-SHA

To use a custom cipher list, type the cipher list in the variable.

For the full syntax of cipher lists, see the [OpenSSL website](#).

### *ClientTlsProtocols*

In this variable, you can change the SSL/TLS protocols used when Kerio Connect acts as a client, for example, when sending messages via the SMTP protocol.

Leave the variable empty to use a default set of SSL/TLS protocols: TLSv1, TLSv1.1

To use a custom set of protocols, list the protocol names, separated by commas, in the variable.

For example: `<variable name="ClientTlsProtocols">SSLv3,TLSv1,TLSv1.1,TLSv1.2</variable>`■

### *ClientTlsCiphers*

In this variable, you can change the client cipher list.

Leave the variable empty to use a default cipher list.

To use a custom cipher list, type the cipher list in the variable.

For the full syntax of cipher lists, see the [OpenSSL website](#).

***PreferServerCipherOrder***

The default value, **1**, allows Kerio Connect decide which cipherset to use regardless of the client preferences.

# Adding trusted root certificates to the server

---

## Overview

If you want to send or receive messages signed by root authorities and these authorities are not installed on the server, you must add a trusted root certificate manually.

Use the following steps to add or remove trusted root certificates to/from a server.

## Mac OS X

### Add

Use command:

```
sudo security add-trusted-cert -d -r trustRoot -k
/Library/Keychains/System.keychain ~/new-root-certificate.crt
```

### Remove

Use command:

```
sudo security delete-certificate -c "<name of existing certificate>"
```

## Windows

### Add

Use command:

```
certutil -addstore -f "ROOT" new-root-certificate.crt
```

### Remove

Use command:

```
certutil -delstore "ROOT" serial-number-hex
```

## Linux (Ubuntu, Debian)

### Add

1. Copy your CA to dir `/usr/local/share/ca-certificates/`
2. Use command:  

```
sudo cp foo.crt /usr/local/share/ca-certificates/foo.crt
```
3. Update the CA store:  

```
sudo update-ca-certificates
```



### Remove

1. Remove your CA.
2. Update the CA store:  
`sudo update-ca-certificates --fresh`



Restart Kerio Connect to reload the certificates in the 32-bit versions or Debian 7.

### Linux (CentOs 6)

#### Add

1. Install the ca-certificates package:  
`yum install ca-certificates`
2. Enable the dynamic CA configuration feature:  
`update-ca-trust force-enable`
3. Add it as a new file to /etc/pki/ca-trust/source/anchors/:  
`cp foo.crt /etc/pki/ca-trust/source/anchors/`
4. Use command:  
`update-ca-trust extract`



Restart Kerio Connect to reload the certificates in the 32-bit version.

### Linux (CentOs 5)

#### Add

Append your trusted certificate to file /etc/pki/tls/certs/ca-bundle.crt  
`cat foo.crt >> /etc/pki/tls/certs/ca-bundle.crt`



Restart Kerio Connect to reload the certificates in the 32-bit version.

# Managing logs in Kerio Connect

---

## About Kerio Connect logs

Logs are files where Kerio Connect records information about certain events, for example, error and warning reports and debugging information. Each item represents one row starting with a timestamp (date and time of the event).

Messages in logs are displayed in English for every language version of Kerio Connect.

See the section [Types of logs](#) for detailed information about each log.

## Configuring logs

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

When you right-click in a log area, you can configure the following settings (available in all logs):

### Save log

You can save whole logs or a selected part in a txt or HTML format.

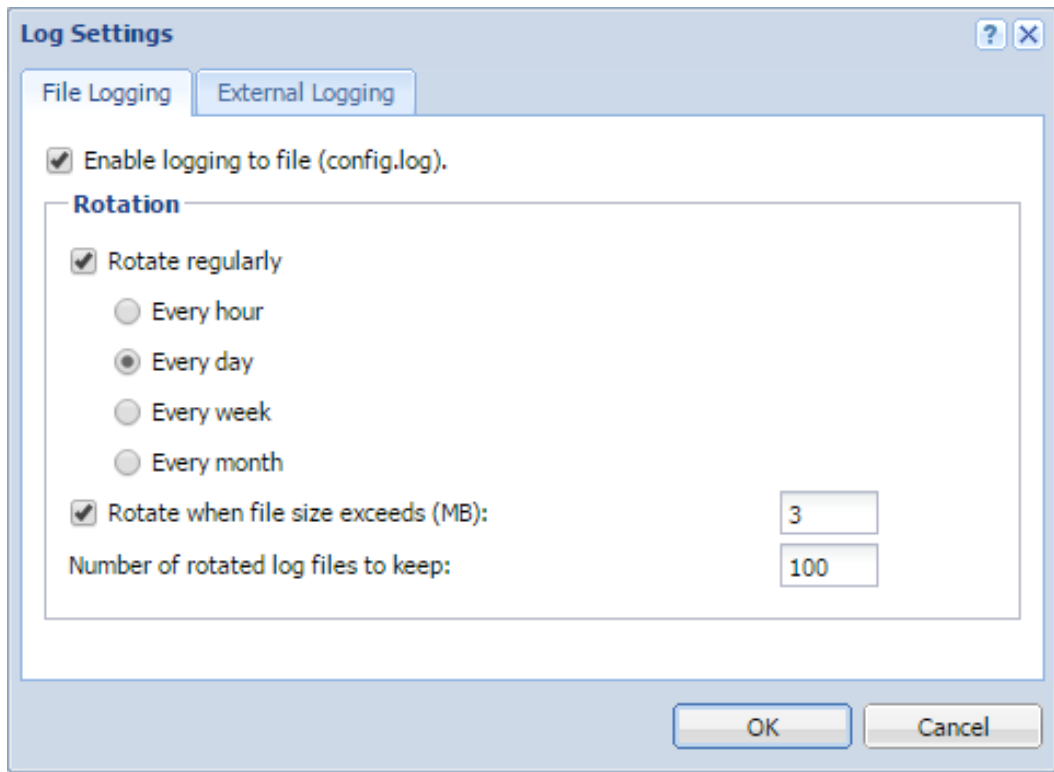
### Highlighting

You can highlight any part of text in logs for better reference. Specify a substring or regular expression and all rows containing such text will be highlighted.

### Log Settings

You can configure regular saves of individual logs, specifying the size and number of saved files.

You can also enable external logging to a Syslog server.



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

The default location of the log files varies by platform:

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

## Types of logs

### Config log

The **Config** log keeps complete history of configuration changes. It tells you which user performed individual administration tasks and when.

### Debug log

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

You can select which information it displays.

1. Right-click in the log window and click **Messages**.
2. Select any option you want to monitor.
3. Click **OK**.



Too much information can be confusing and slows Kerio Connect's performance. Switch off the logging if you solve your problem.

### Mail log

The **Mail** log contains information about individual messages processed by Kerio Connect.

### Security log

The **Security** log contains information related to Kerio Connect's security. It also contains records about all messages that failed to be delivered.

### Warning log

The **Warning** log displays warning messages about errors of little significance. Events causing display of warning messages in this log do not greatly affect Kerio Connect's operation. However, they can , indicate certain (or possible) problems.

For example, the Warning log can help if a users complain that certain services are not working.

### Operations log

The **Operations** log gathers information about removed and moved items (folders, messages, contacts, events, tasks and notes) in user mailboxes. It is helpful especially if a user cannot find a particular message in their mailbox.

### Error log

The **Error** log displays errors of great significance that usually affect the mailserver's operation (in contrast to the [Warning](#) log).

Typical error messages displayed in the Error log concern service initiation (usually due to port conflicts), disk space allocation, antivirus check initialization, improper authentication of users, and so on.

### Spam log

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

### Audit log



### New in Kerio Connect 9!

The **Audit** log displays information about all successful authentication attempts to Kerio Connect accounts, including Kerio Connect Administration, Kerio Connect Client, Microsoft Outlook with KOFF, etc.

# Integrating Kerio Connect with Kerio Operator

---

## Overview

If you have both Kerio Connect and Kerio Operator, you can use the **Click to Call** feature to place calls through Kerio Connect Client.

With **Click to Call**, users can dial numbers from their Kerio Connect Client using Kerio Operator.

## Configuring Kerio Connect

An administrator with full access rights must connect Kerio Connect to Kerio Operator.



Users must have identical usernames in both Kerio Connect and Kerio Operator to use the **Click to Call** feature.

1. Login to Kerio Connect Administration.
2. Go to the **Configuration** → **Advanced Options** section.
3. On the **Kerio Connect Client** tab, type the name of the Kerio Operator server.

The screenshot shows the 'Advanced Options' configuration window for Kerio Operator, specifically the 'Kerio Connect Client' tab. The window has a search bar at the top right with the text 'Where is ...' and a user name 'R. Cul Powaro'. Below the search bar are several tabs: 'Miscellaneous', 'Store Directory', 'Master Authentication', 'HTTP Proxy', 'Software Updates', 'Kerio Connect Client', and 'Login Page'. The 'Kerio Connect Client' tab is active.

Under the 'Kerio Connect Client' tab, the 'Default web client' is set to 'Kerio Connect Client' with a dropdown arrow and a 'Learn more...' link. Below this is the 'Message size limit' section, which includes a text input field for 'Maximum size of a message that can be sent from the Kerio Connect Client interface (HTTP POST size) [MB]' with the value '20'. An information icon indicates that a restart of Kerio Connect is required for this change to take effect.

The 'Session security' section contains two rows of settings: 'Session expiration timeout' set to '1' hours and 'Maximum session duration' set to '2' hours. A checkbox is checked for 'Force logout from Kerio Connect Client if user's IP address changes (prevents from session hijacking and session fixation attacks)'. Below this is the 'Custom logo' section, which has an unchecked checkbox for 'Use custom logo for Kerio Connect Client' and a 'Select file...' button. An information icon notes that the logo must be in PNG format and recommended size is 142x45 pixels.

The 'Kerio Operator integration' section has a checked checkbox for 'Enable Click to Call in Kerio Connect Client' with a 'Learn more...' link. Below it is a text input field for 'Kerio Operator server address' containing the value 'operator.feelmorelaw.com'. At the bottom right of the window are 'Apply' and 'Reset' buttons.

## Configuring Kerio Operator

No special configuration is necessary in Kerio Operator. If you use an outgoing prefix in your environment, you must [add a number transformation rule to Kerio Operator](#).



See [Making calls from Kerio Connect Client](#) for more information on using Click to Call.

# Kerio Active Directory Extension

---

## How to use Kerio Active Directory Extension

You install Kerio Active Directory Extension into the Microsoft Active Directory and items containing specific Kerio Connect information are added to Active Directory.

User account will be managed in one place — in Microsoft Active Directory.

Kerio Active Directory Extension is available only in English.

## How to install Kerio Active Directory Extension

Download Kerio Active Directory Extension at the [Kerio Connect product pages](#).

It can be installed on [supported operating systems](#) on the Schema Master 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](#).



Username must be in ASCII or users will not be able to login to their accounts.



## **Troubleshooting**

If you encounter any problems during KADE installation, view/save the log during the installation process (View Log/Save Log File).

# Kerio Open Directory Extension

---

## How to use Kerio Open Directory Extension

You install Kerio Open Directory Extension into the Apple Open Directory and items containing specific Kerio Connect information are added to Open Directory.

User account will be managed in one place — in Apple Open Directory.

## How to install Kerio Open Directory Extension

Download Kerio Open Directory Extension at the [Kerio Connect product pages](#).

It can be installed on [supported operating systems](#) using a standard installation wizard.



When using configurations of Mac OS X servers of Master/Replica type, Kerio Open Directory Extension must be installed to the "master" server, as well as to all "replica" servers, otherwise the account mapping will not work.

If the configuration is as follows:

- you use Kerio Open Directory Extension 6.6 and newer,
- servers run on OS X 10.5.3 and newer,
- Replica servers were created after installation of Kerio Open Directory Extension on the "master" server,

then "replica" servers download the extension automatically from the "master" server during the creation process.

If you install Kerio Open Directory Extension on "replica" servers by hand, the configuration will not be affected.

## Setting user account mapping in Kerio Connect

In Mac OS X Server, no other settings than Kerio Open Directory Extension installation are usually necessary.



The usernames must be in ASCII. If the username includes special characters or symbols, it might happen that the user cannot log in.

In Kerio Connect the following settings must be specified:

- [Enable user mapping in domain settings.](#)
- Set user authentication via Kerberos in domain settings.
- Set user authentication via Kerberos in user settings.

## **Troubleshooting**

If you encounter any problems during KODE installation, view/save the log during the installation process (View Log/Save Log File).

# Managing user mobile devices

---

## Managing mobile devices in Kerio Connect

Each user can synchronize their Kerio Connect account with an unlimited number of mobile devices which support Exchange ActiveSync 2.5-14.1.



You can disable Exchange ActiveSync 14 for older devices. Read [Setting a compatible Exchange ActiveSync version for specific mobile devices](#) for more details.

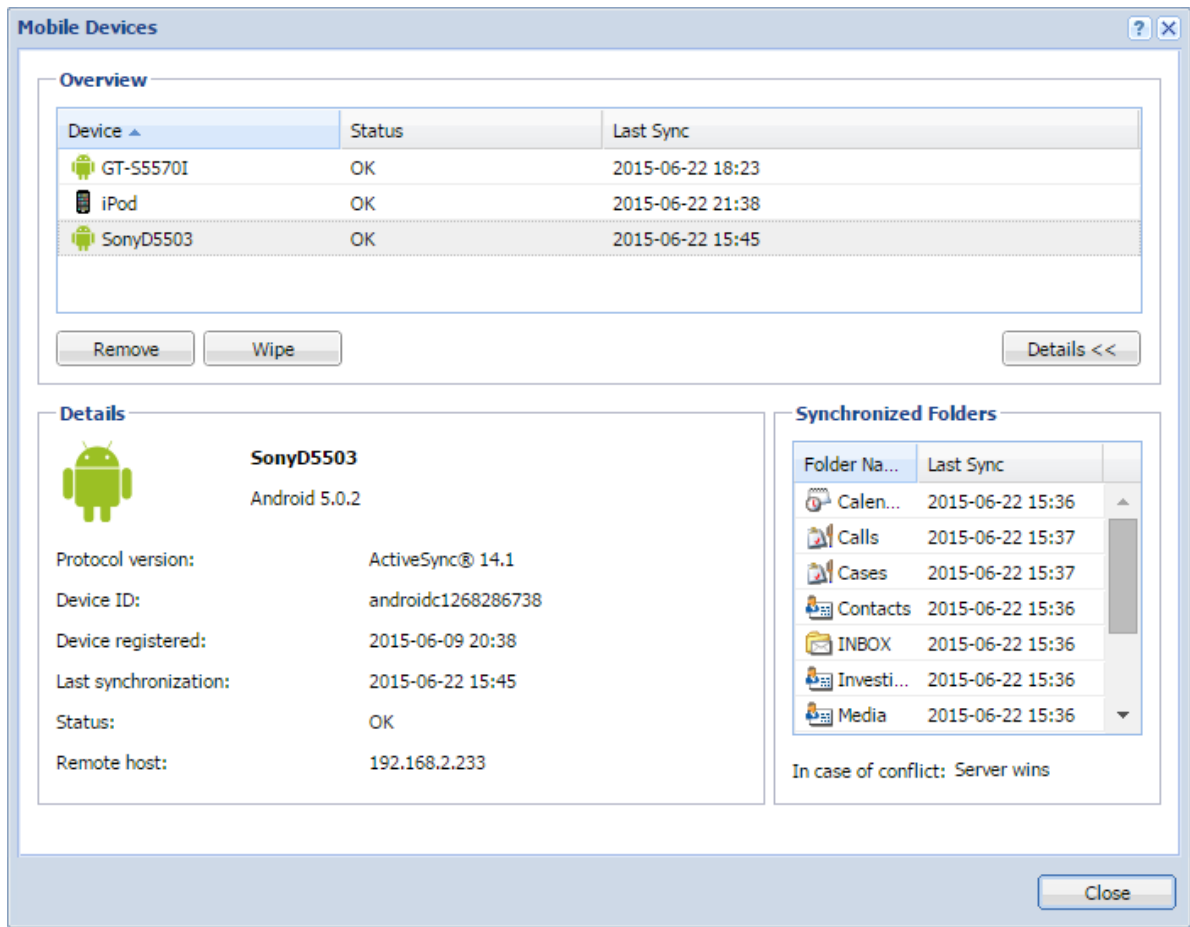


In Kerio Connect 8.4 and older, you must select the **Allow synchronization of unsupported Exchange ActiveSync devices** option in **Configuration** → **Advanced Options** → **Miscellaneous** to allow synchronization of all devices.

## Viewing users devices

In the administration interface, you can view information about all devices connected to user accounts.

1. Go to **Accounts** → **Users**.
2. Select a user and click **More Actions** → **Mobile Devices**.  
This displays a list of user's devices.
3. Select a device and
  - Click **Details** to view information about the device
  - Click **Remove** to delete unused devices from the list
  - Click [Wipe](#) to delete data from the device



## Blocking specific types of devices

In Kerio Connect, you can block all devices of a specific type by editing the configuration file.

1. Stop the Kerio Connect engine.
2. Open the **mailserver.cfg** file in a text editor.
3. Locate the **BlockedDevices** section.
4. Add the device types you want to block in the following format:

```
<variable name="DeviceType">iPod</variable>
```

The list may look like this:

```
<list name="BlockedDevices">
<listitem>
<variable name="DeviceType">iPod</variable>
</listitem>
<listitem>
```

## Managing user mobile devices

---

```
<variable name="DeviceType">WP8</variable>
</listitem>
</list>
```



You can find the device type string in the [Debug log](#).

To start logging information about Exchange ActiveSync devices, right-click in the log area and select **Messages** → **ActiveSync Synchronization**.

The line to search for may look like this:

```
[22/Jun/2015 21:38:58][4892] {activesync} Receiving request from 192.168.0.113:4916
Version: 12.1, Command: Ping, Device Id: App19C8303NA14N, Policy
Key: 1, Device Type: iPod, User: powaro, User Agent: Apple-iPod/705.18
```

To avoid low performance of your server, disable ActiveSync Synchronization logging after you acquire the UserAgent strings.

5. Save the **mailserver.cfg** file.
6. Start Kerio Connect.

Kerio Connect now blocks connections from all devices of the types you added in the file.

### Remotely deleting data from users' device

If users lose their devices, you can delete all the account data from the devices.

1. In the administration interface, go to **Accounts** → **Users**.
2. Select a user and click **More Actions** → **Mobile Devices**.
3. Select a device and click **Wipe**.

Once the device connects to the Kerio Connect server, Kerio Connect removes all the account data from the device.



Based on the device type and its operating system, you reset the device completely or you only clear out the account. If the device stores email attachments on a memory card, Kerio Connect deletes the attachments as well.

You can cancel the wipe before the device connects to the Kerio Connect server (click **Cancel Wipe**).

You can find details of the wipe process in the [Security log](#).

Users can also [wipe their own devices](#) from their Kerio Connect Client.

### ***User confirmation of the wipe action - windows mobile***

On Windows Mobile operating systems, users must agree that the administrator performs the wipe action. They must confirm a dialog during the first data synchronization between the device and Kerio Connect. If they don't confirm, it is not possible to complete the synchronization process.

# Setting a compatible Exchange ActiveSync version for specific mobile devices

---

## Overview



New in Kerio Connect 8.5.1!

Kerio Connect supports Exchange ActiveSync 14. Some older mobile devices may experience problems with this version of Exchange ActiveSync (EAS) — for example, duplicated messages in their mailboxes, empty message folders, and so on.

If users have such problems, you can disable EAS 14 for individual devices in the configuration file. These devices then work with earlier versions of EAS and they do not:

- Synchronize notes
- Synchronize read/forward flags
- Show free/busy information

## Editing the configuration file

1. Stop the Kerio Connect server.
2. Open the `mailserver.cfg` file.

The default location is:

- **Windows:** `C:\Program Files\Kerio\MailServer`
  - **Mac:** `/usr/local/kerio/mailserver`
  - **Linux:** `/opt/kerio/mailserver`
3. In the **LegacyDevices** list, add the devices for which you want to disable EAS 14 in the following format:

```
<variable name="UserAgent">[device UserAgent string]</variable>
```

Example for Android 4.1.1 and iPod devices:



```
<list name="LegacyDevices">
  <listitem>
    <variable name="UserAgent">Android/4.1.1-EAS-1.3</variable>
  </listitem>
  <listitem>
    <variable name="UserAgent">Apple-iPod/705.18</variable>
  </listitem>
</list>
```



You can find the device **User Agent** string in the [Debug log](#).

To start logging information about Exchange ActiveSync devices, right-click in the log area and select **Messages** → **ActiveSync Synchronization**.

The line to search for may look like this (you find the string at the end of the line):

```
[22/Jun/2015 21:38:58][4892] {activesync} Receiving request from 192.168.0.113:4916
Version: 12.1, Command: Ping, Device Id: App19C8303NA14N, Policy
Key: 1, Device Type: iPod, User: powaro, User Agent: Apple-iPod/705.18
```

To avoid low performance of your server, disable ActiveSync Synchronization logging after you acquire the User Agent strings.



Some devices may have identical **User Agent** strings. If you disable such string, you disable Exchange ActiveSync 14 and newer for all such devices.

4. Save the file.
5. Start the Kerio Connect server.
6. Recreate the Kerio Connect account on the user's device.

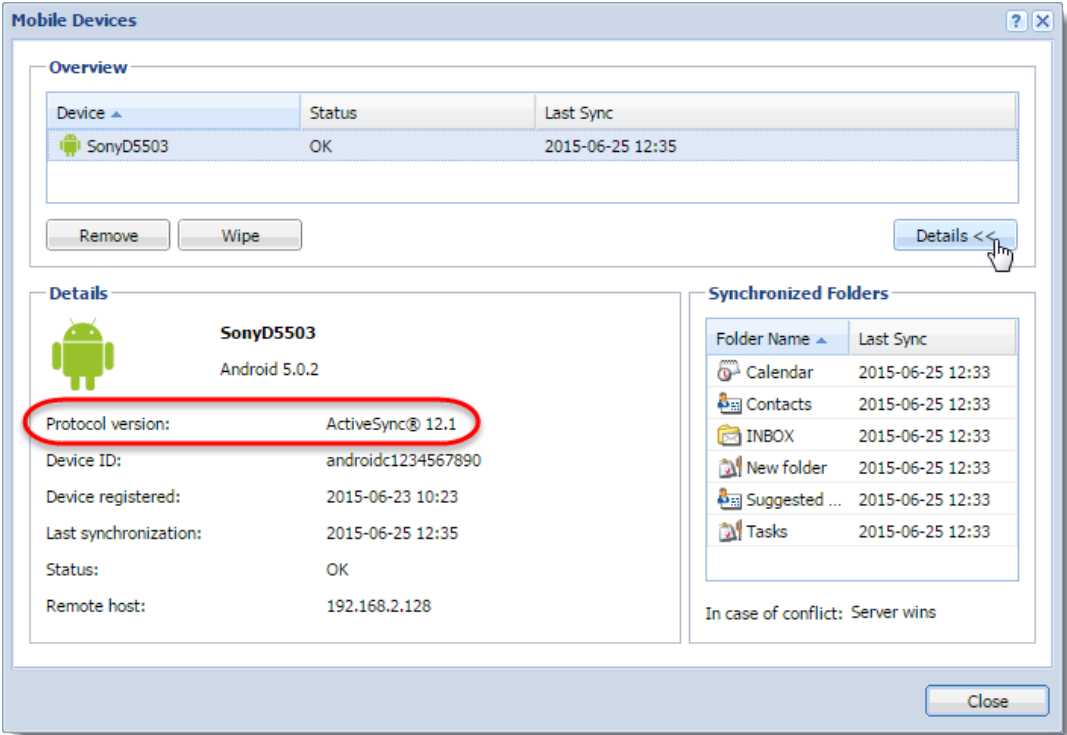
Now the listed devices do not use Exchange ActiveSync version 14 and newer; they use any previous version available for them.

To verify the device uses a lower version of EAS:

1. In the administration interface, go to the **Accounts** → **Users**.
2. Select the users and click **More Actions** → **Mobile Devices**.
3. Select the device and click **Details**.

The details show the protocol version the devices uses.

Setting a compatible Exchange ActiveSync version for specific mobile devices



# Changing the time zone definitions in timezones.xml file in Kerio Connect

---

## About time zones

Time zones are defined in the `timezones.xml` definition file in Kerio Connect.

Each version of Kerio Connect includes a new version of the `timezones.xml` file. However, you can [edit the file directly](#) or [download the latest time zone definition file](#) attached to this article.



On October 26, 2014, Russia changes their time zones. A new file including these changes is available in the attachment section below this article.

## Important notes

If you **change** the `timezones.xml` file, note the following:

- Calendar events and tasks have time zone definitions saved within the event/task itself. You must create the event/task again to apply the new time zones.
- All newly created events/tasks use the new time zone definitions.
- Client applications (MS Outlook, Apple Calendars) use their own or system time zone definitions. Make sure you have everything updated in order to have the correct time zone definitions in all your email clients.

## Updating the timezones.xml file automatically

To update the `timezones.xml` automatically, [upgrade your Kerio Connect](#).

## Updating the timezones.xml file manually

The `timezones.xml` file is located in the installation directory of the Kerio Connect server.

The default path is:

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

## Changing the time zone definitions in timezones.xml file in Kerio Connect

---

To update the file, follow these steps:

1. Stop the Kerio Connect server.
2. Replace the `timezones.xml` with a new one.



Backup the original `timezones.xml` file.

3. Start the Kerio Connect server.

Kerio Connect starts using the new time zone definitions for all newly created events.

### Editing the `timezones.xml` file

You can edit the `timezones.xml`. The file contains two parts enclosed in the following tags: `<abbr></abbr>` and `<zone></zone>`.



All date and time definitions used in this description are defined in the [RFC 2445](#).

#### *Editing the `<abbr>` section*

This section describes the time shift. This part is optional although it helps you to simplify reading of the configuration file.

The `<abbr>` section has the following properties:

- `<name>` — The name of the time shift definition (the GMT/UTC offset)
- `<offset>` — The value of the time shift in  $\pm PThhHmM$  format (hh means hours and mm means minutes, other letters are reserved).
- `<daylight>` — If this value is true, the time zone definition uses the daylight saving time. If the value is false, the time zone does not use the daylight saving time.

#### *Editing the `<zone>` section*

This section defines the time zone.

The `<zone>` section has the following mandatory properties:

- `<name>` — The name of the time zone. Kerio Connect uses this string when searching for the appropriate time zone.
- `<stdAbbr>` — Name of the time shift defined in the `<abbr>` section or a direct value in  $\pm hhmm$  (hh means hours and mm means minutes).
- `<cdoTimeZoneId>` — This option is usually required by synchronization devices and maps the time zone definition to the appropriate time zone definition in the Microsoft

definition table. This mapping table can be found on the Microsoft web page. This line can be specified multiple times to assign all appropriate time zone Ids to the time zone definition.

The following attributes are optional:

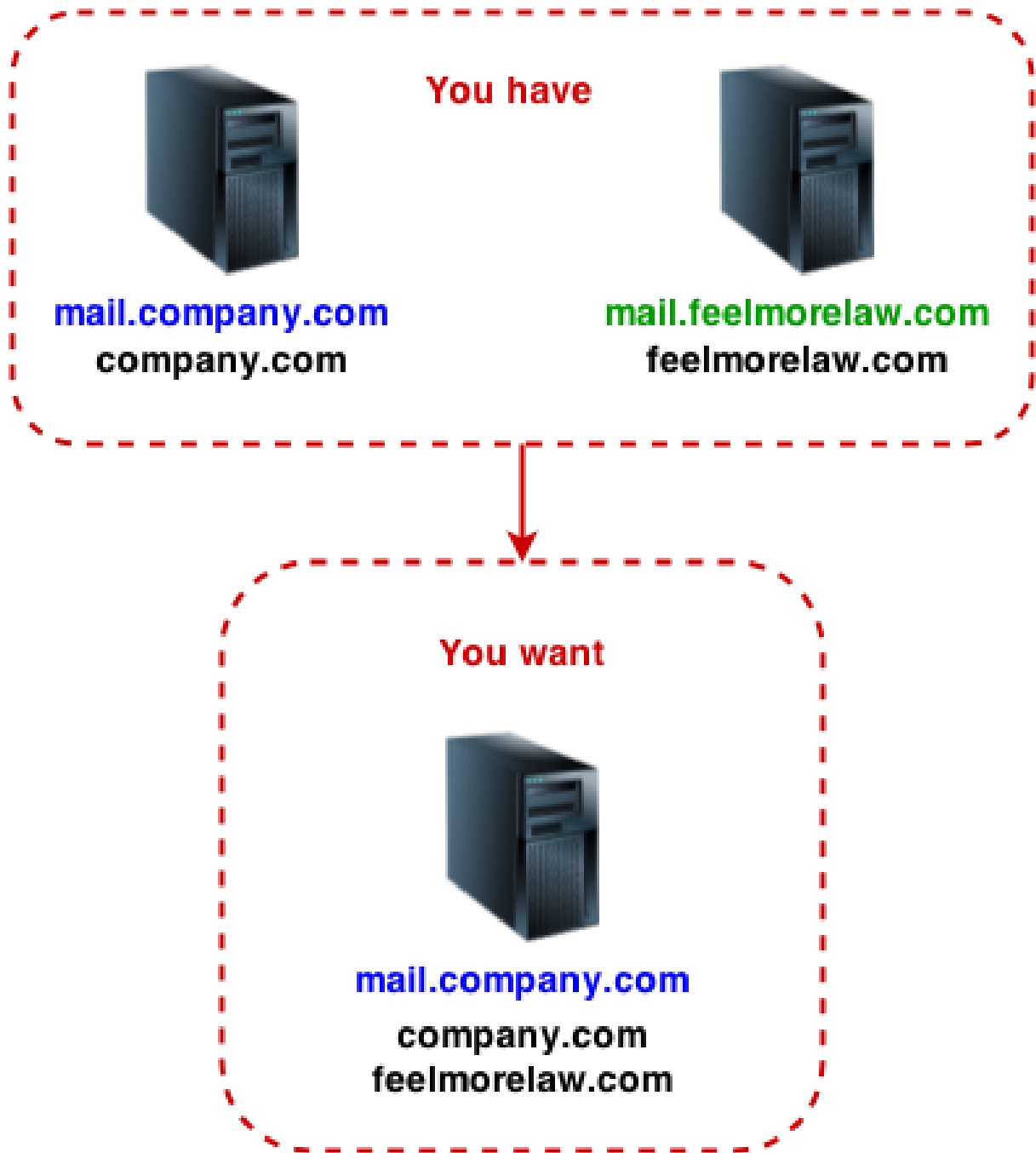
- `<daylightAbbr>` — This is a time shift definition for the daylight saving time in the same format as the mandatory `stdAbbr` attribute.
- `<stdStart>` — The date and time this definition becomes valid for the first time for the specified location. The format is `yyyymmddThhmmss` where `y` is year, `m` is month, `d` is day, `h` is hour, `m` is minute and `s` is second.
- `<daylightStart>` — The date and time the daylight savings time becomes valid for the first time for the location. The format is `yyyymmddThhmmss` where `y` is year, `m` is month, `d` is day, `h` is hour, `m` is minute and `s` is second.
- `<stdRRule>` — This option defines periodicity and frequency of changing to standard time. `FREQ` is the frequency of the change, `BYMONTH` is the month when the change occurs, `BYMONTHDAY` is the day when the change occurs (you can also use `BYDAY` which is the `x`-th day in a week or month). Example: `FREQ=YEARLY;BYMONTH=9;BYMONTHDAY=22`

# Joining two servers with different domains into one server

---

## Details

You have two Kerio Connect servers. Each server has one different domain. You want to join the domains in one server.



### Joining two Kerio Connect servers into one

With regard to the introduced scenario, follow these steps:

1. [Export users](#) from domain **feelmorelaw.com** on the **mail.feelmorelaw.com** server.
2. [Run a full backup](#) on the **mail.feelmorelaw.com** server.
3. On **mail.company.com** server, [create domain](#) **feelmorelaw.com**.

## Joining two servers with different domains into one server

---

4. [Import users](#) from the **mail.feelmorelaw.com** server, to the newly created domain **feelmorelaw.com** on the **mail.company.com** server.

Use the export file from step 1.

5. On the **mail.company.com** server, [restore domain feelmorelaw.com](#) from the backup of the **mail.feelmorelaw.com** server.

Use the full backup file from step 2.



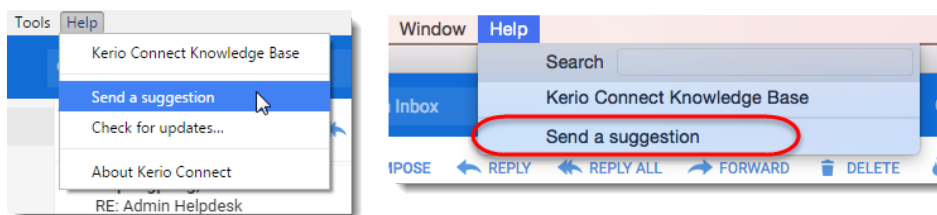
# Providing feedback for Kerio products

---

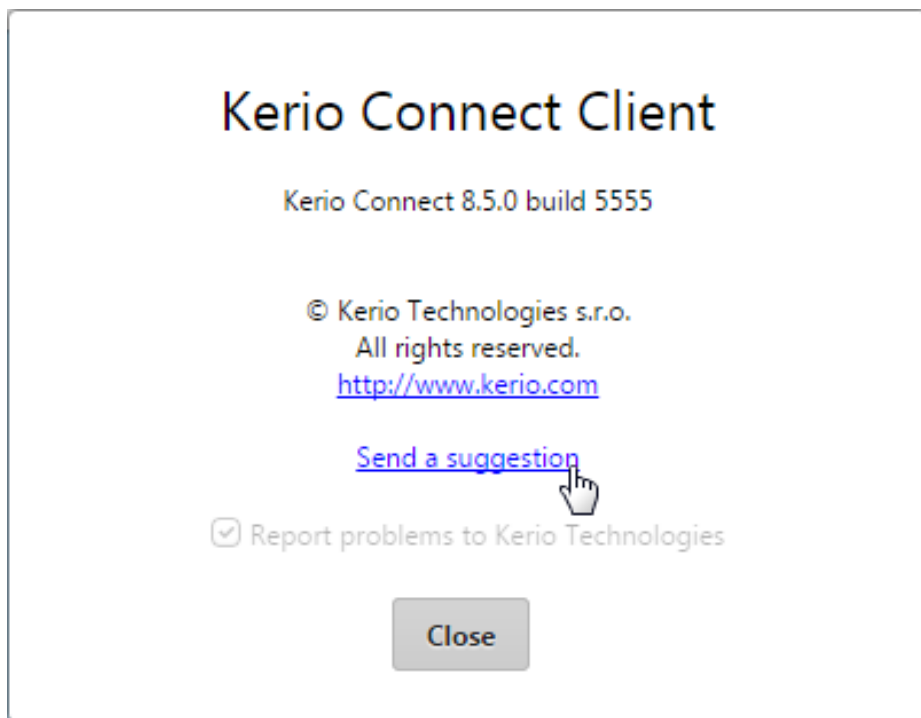
## Giving feedback through Kerio Connect Client

To give an opinion about [Kerio Connect Client](#):

- In **Kerio Connect for Windows and Mac**, click **Help** → **Send a suggestion**.



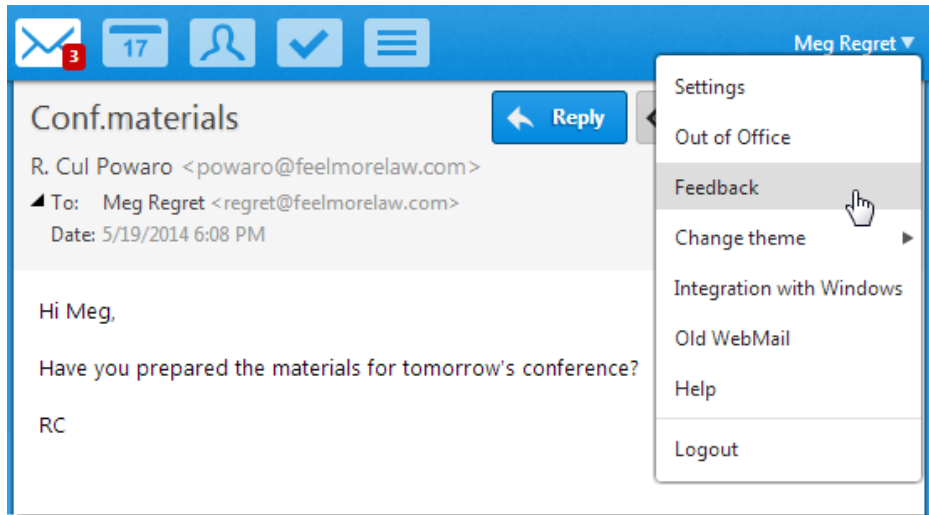
- In **Kerio Connect for web 8.5 and newer**, click your name, select **About** → **Send a suggestion**.



## Providing feedback for Kerio products

---

- In **Kerio Connect for web 8.4** and older, click your name in Kerio Connect Client and select **Feedback**.



The feedback forum is displayed. It provides the same features as the admin forum (see the image above).

# Kerio Connect — Legal notices

---

## Trademarks and registered trademarks

Microsoft<sup>®</sup>, Windows<sup>®</sup>, Windows NT<sup>®</sup>, Windows Vista<sup>®</sup>, Internet Explorer<sup>®</sup>, Active Directory<sup>®</sup>, Outlook<sup>®</sup>, ActiveSync<sup>®</sup>, Entourage<sup>®</sup> and Windows Mobile<sup>®</sup> are registered trademarks of Microsoft Corporation.

Apple<sup>®</sup>, iCal<sup>®</sup>, macOS<sup>®</sup>, Mac OS<sup>®</sup>, OS X<sup>®</sup>, Safari<sup>™</sup>, Tiger<sup>™</sup>, Panther<sup>®</sup>, Open Directory logo<sup>™</sup>, Leopard<sup>®</sup>, Snow Leopard<sup>®</sup> and Lion<sup>®</sup> are registered trademarks or trademarks of Apple, Inc.

Palm<sup>®</sup>, Treo<sup>™</sup>, Pre<sup>™</sup> and VersaMail<sup>®</sup> are registered trademarks or trademarks of Palm, Inc.

Red Hat<sup>®</sup> and Fedora<sup>™</sup> are registered trademarks or trademarks of Red Hat, Inc.

SUSE<sup>®</sup>, openSUSE<sup>®</sup> and the openSUSE logo are registered trademarks or trademarks of Novell, Inc.

Mozilla<sup>®</sup> and Firefox<sup>®</sup> are registered trademarks of Mozilla Foundation.

Linux<sup>®</sup> is registered trademark of Linus Torvalds.

Kerberos<sup>™</sup> is trademark of Massachusetts Institute of Technology (MIT).

avast!<sup>®</sup> is registered trademark of AVAST Software.

eTrust<sup>™</sup> is trademark of Computer Associates International, Inc.

ClamAV<sup>™</sup> is trademark of Tomasz Kojm.

Cybertrust<sup>®</sup> is registered trademark of Cybertrust Holdings, Inc. and/or their filials.

Thawte<sup>®</sup> is registered trademark of VeriSign, Inc.

Entrust<sup>®</sup> is registered trademark of Entrust, Inc.

Sophos<sup>®</sup> is registered trademark of Sophos Plc.

ESET<sup>®</sup> and NOD32<sup>®</sup> are registered trademarks of ESET, LLC.

AVG<sup>®</sup> is registered trademark of AVG Technologies.

IOS<sup>®</sup> is registered trademark of Cisco Systems, Inc.

NotifyLink<sup>®</sup> is registered trademark of Notify Technology Corporation.

BlackBerry<sup>®</sup> is registered trademark of Research In Motion Limited (RIM).

RoadSync<sup>™</sup> is trademark of DataViz Inc.

Nokia<sup>®</sup> and Mail for Exchange<sup>®</sup> are registered trademarks of Nokia Corporation.

Symbian<sup>™</sup> is trademark of Symbian Software Limited.

Sony Ericsson<sup>®</sup> 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.

Bitdefender® is registered trademark of BitDefender IPR Management Ltd.

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.

### Used open source software

This product contains the following open-source libraries:

#### **Appliance OS sources - Debian**

Kerio Connect appliance is based on Debian GNU/Linux - Linux distribution composed of open source software from various sources.

Please refer to /usr/share/doc/\*/copyright files installed inside the appliance for exact licensing terms of each package the appliance is built from.

The source package itself can be downloaded from <http://kerio.com/...>

#### **Berkeley DB**

Berkeley DB (BDB) is a computer software library that provides a "high-performance" embedded database, with bindings in C, C++, Java, Perl, Python, Ruby, Tcl, Smalltalk, and many other programming languages.

The Regents of the University of California. All rights reserved.

#### **bindlib**

DNS resolver library, linked by PHP on Windows.

Copyright © 1983, 1993 The Regents of the University of California. All rights reserved.

Portions Copyright © 1993 by Digital Equipment Corporation.

#### **bluff**

Bluff is a JavaScript port of the Gruff graphing library for Ruby. The Gruff library is written in Ruby.

Copyright © 2008-2009 James Coglan.

Original Ruby version © 2005-2009 Topfunky Corporation.

#### **cfgwizard**

Tool for initial configuration of Kerio Mailserver for Linux.

Distributed and licensed under GNU General Public License version 3.

Copyright © Kerio Technologies s.r.o.

Homepage: <http://kerio.com/>

Complete source code of the executable is available from <http://kerio.com/...>

**Chromium**

The Chromium engine running Electron applications.

<https://chromium.googlesource.com/chromium/src.git/+/master/LICENSE>

**CppSQLite**

A C++ wrapper around the SQLite embedded database library.

Copyright ©2004 Rob Groves. All Rights Reserved.

**Electron**

Electron is a framework for creating native applications with web technologies like JavaScript, HTML, and CSS.

Copyright © 2014 GitHub Inc.

**excanvas**

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

Copyright © 2006 Google Inc.

**Firebird 2**

This software embeds modified version of Firebird database engine distributed under terms of IPL and IDPL licenses.

All copyright © retained by individual contributors — original code Copyright © 2000 Inprise Corporation.

Modified source code is available from <http://kerio.com/>

**gettext**

Gettext is a software translation toolkit. It is distributed under GNU General Public License version 3. Its libintl subpart is distributed under GNU Lesser General Public License version 2.1 or newer.

Copyright © 1984, 1989, 1990, 1991, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010 Free Software Foundation, Inc.

Complete source code is available at: <http://kerio.com/...>

**glib**

GLib is a cross-platform software utility library. It is distributed under GNU Lesser General Public License version 2 or later.

Copyright © 2006-2010 Red Hat, Inc., Kerio Technologies s.r.o. and others.

Copyright © 1998-2010 Tim Janik, Red Hat, Inc., Kerio Technologies s.r.o. and others

Copyright © 1995-2010 Peter Mattis, Spencer Kimball, Josh MacDonald, Sebastian Wilhelmi, Kerio Technologies s.r.o. and others.

Complete source code is available at: <http://kerio.com/...>

**gmime**

GMime is a C/C++ library which may be used for the creation and parsing of MIME messages. It is distributed under GNU Lesser General Public License version 2.1 or later.

Copyright © 2000-2009 Jeffrey Stedfast and Michael Zucchi

Complete source code is available at: <http://kerio.com/...>

### **Heimdal Kerberos**

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

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

Copyright ©1995-1997 Eric Young. All rights reserved.

Copyright ©1990 by the Massachusetts Institute of Technology

Copyright ©1988, 1990, 1993 The Regents of the University of California. All rights reserved.

Copyright ©1992 Simmule Turner and Rich Salz. All rights reserved.

### **ICU — International Components for Unicode (C/C++)**

ICU is a mature, widely used set of C/C++ and Java libraries providing Unicode and Globalization support for software applications.

Copyright © 1995-2009 International Business Machines Corporation and others

### **Inferno**

An extremely fast React-like JavaScript library for building modern user interfaces.

Copyright © 2013-2016 Dominic Gannaway

### **intl — windows**

libintl for Windows is a software library for native language support. It is released under LGPL license version 2 or later.

Copyright © 2008 Tor Lillqvist

The source code is available at: <http://kerio.com/...>

### **JSColor**

JSColor is a simple and user-friendly color picker for your HTML forms. It extends all desired <input> fields of a color selection dialog.

Jan Odvarko, <http://odvarko.cz>

### **libcurl**

Libcurl is a free and easy-to-use client-side URL transfer library. This library supports the following protocols: FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP.

Copyright ©1996-2008, Daniel Stenberg.

### **libiconv**

Libiconv converts from one character encoding to another through Unicode conversion. This product contains customized version of this library which is distributed and licensed under GNU Lesser General Public License version 3.

Copyright © 1999-2003 Free Software Foundation, Inc.

Author: Bruno Haible

Homepage: <http://www.gnu.org/software/libiconv/>

Complete source code is available at: <http://kerio.com/...>

### **libIDL**

LibIDL is a front-end for CORBA 2.2 IDL and Netscape's XPIDL.

Copyright © 1998, 1999 Andrew T. Veliath.

**libdkim++**

libdkim++ is a lightweight and portable DKIM (RFC4871) library for \*NIX, supporting both signing and SDID/ADSP verification sponsored by Halon Security. libdkim++ has extensive unit test coverage and aims to fully comply with the current RFC.

Copyright © 2009,2010,2011 Halon Security <support@halon.se>

**libmbfl**

libmbfl is a streamable multibyte character code filter and converter library. The libmbfl library is distributed under LGPL license version 2.

Copyright ©1998-2002 HappySize, Inc. All rights reserved.

The library is available for download at: <http://download.kerio.com/archive/>

**libMemcached**

libMemcached is an open source C/C++ client library and tools for the memcached server. It has been designed to be light on memory usage, thread safe, and provide full access to server side methods.

Copyright © 2006-2010 Brian Aker

Copyright © 2012-2013 Brian Aker

Copyright © 2010 Brian Aker, Trond Norbye

Copyright © 2011-2013 Data Differential, <http://datadifferential.com/>

Copyright © 2009, Schooner Information Technology, Inc.  
<http://www.schoonerinfotech.com/>

Copyright © 2008, Sun Microsystems, Inc.

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

**libnewt**

Newt is a programming library for color text mode, widget-based user interfaces. It is distributed and licensed under GNU Lesser General Public License.

Copyright © 1996-2003 Red Hat, Inc. Written by Erik Troan

Complete source code is available at: <http://kerio.com/...>

**libslang**

S-lang is a C-like programming language, designed to be embedded in programs. It is distributed and licensed under GNU General Public License.

Copyright © 1992, 1995 John E. Davis

Homepage: <http://www.s-lang.org>

Complete source code is available at: <http://kerio.com/...>

**libspf2**

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

Copyright © 2004 by 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.

**libtiff**

Libtiff is a library for reading and writing Tagged Image File Format files.

Copyright © 1988-1997 Sam Leffler

Copyright © 1991-1997 Silicon Graphics, Inc.

Copyright © 2007-2009 Richard Nolde

Copyright © Joris Van Damme

Copyright © 1990, 1995 Frank D. Cringle

Copyright © 1996 USAF Phillips Laboratory

Copyright © 1985, 1986 The Regents of the University of California

Copyright © 1990 by Sun Microsystems, Inc.

Copyright © 1996 Pixar

Copyright © 1999, Frank Warmerdam

Copyright © 2002, Andrey Kiselev

Copyright © 2003 Ross Finlayson

Copyright © 2009 Frank Warmerdam

Copyright © Copyright 1990 by Digital Equipment Corporation, Maynard, Massachusetts.

Copyright © 2004 Free Software Foundation, Inc.

Copyright © 1994 X Consortium

Copyright © 2003 Ross Finlayson

Copyright © 1996 BancTec AB

Copyright © 1996 Mike Johnson

**libxml2**

XML parser and toolkit.

Copyright ©1998-2003 Daniel Veillard. All Rights Reserved.

Copyright ©2000 Bjorn Reese and Daniel Veillard.

Copyright ©2000 Gary Pennington and Daniel Veillard

Copyright ©1998 Bjorn Reese and Daniel Stenberg.

**myspell**

Spellcheck library.

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

**MariaDB Connector/C**

MariaDB Connector/C is used to connect applications developed in C/C++ to MariaDB and MySQL databases.

Copyright © 2010 Michael Bell <michael.bell@web.de>

Copyright © 2000 MySQL AB & MySQL Finland AB & TCX DataKonsult AB

Copyright © 1989, 90, 91, 92, 93, 94 Free Software Foundation, Inc.

Copyright © 2000 MySQL AB



Copyright © 2010 - 2012 Sergei Golubchik and Monty Program Ab  
Copyright © 2013 by MontyProgram AB  
Copyright © 2012 Monty Program AB  
Copyright © 2011, Monty Program Ab  
Copyright © 2011,2013 Monty Program Ab;  
Copyright © 2010 Sergei Golubchik and Monty Program Ab  
Copyright Abandoned 1996, 1999, 2001 MySQL AB  
Copyright © 2006-2011 The PHP Group  
Copyright © 2000, 2011 MySQL AB & MySQL Finland AB & TCX DataKonsult AB  
Copyright © 2011, Oleksandr Byelkin  
Copyright © 2011,2012 Oleksandr Byelkin  
Copyright © 1995-2003, 2010 Jean-loup Gailly.  
Copyright © 1995-2005 Jean-loup Gailly.  
Copyright © 1995-2006 Jean-loup Gailly.  
Copyright © 1995-2010 Jean-loup Gailly  
Copyright © 1995-2010 Jean-loup Gailly and Mark Adler  
Copyright © 1995-2003, 2010 Mark Adler  
Copyright © 1995-2005, 2010 Mark Adler  
Copyright © 1995-2006, 2010 Mark Adler  
Copyright © 1995-2007 Mark Adler  
Copyright © 1995-2003, 2010 Mark Adler  
Copyright © 1995-2009 Mark Adler  
Copyright © 1995-2010 Mark Adler  
Copyright © 2004, 2005, 2010 Mark Adler  
Copyright © 2004, 2010 Mark Adler  
Copyright © 2006-2011 The PHP Group

**Nginx**

nginx [engine x] is an HTTP and reverse proxy server, as well as a mail proxy server, written by Igor Sysoev.

Copyright © 2002-2014 Igor Sysoev  
Copyright © 2011-2014 Nginx, Inc.  
Copyright © Maxim Dounin  
Copyright © Unbit S.a.s. 2009-2010  
Copyright © 2008 Manlio Perillo (manlio.perillo@gmail.com)  
Copyright © Austin Appleby  
Copyright © Roman Arutyunyan  
Copyright © Unbit S.a.s. 2009-2010  
Copyright © Valentin V. Bartenev  
Copyright © Yichun Zhang (agentzh)  
Copyright © 2009-2014, Yichun "agentzh" Zhang <agentzh@gmail.com>, CloudFlare Inc.  
Copyright © 2010-2013, Bernd Dorn.

### **OpenLDAP**

Freely distributable LDAP (Lightweight Directory Access Protocol) implementation.

Copyright © 1998-2007 The OpenLDAP Foundation

Copyright ©1999, Juan C. Gomez, All rights reserved

Copyright ©2001 Computing Research Labs, New Mexico State University

Portions Copyright©1999, 2000 Novell, Inc. All Rights Reserved

Portions Copyright ©PADL Software Pty Ltd. 1999

Portions Copyright ©1990, 1991, 1993, 1994, 1995, 1996 Regents of the University of Michigan

Portions Copyright ©The Internet Society (1997)

Portions Copyright ©1998-2003 Kurt D. Zeilenga

Portions Copyright ©1998 A. Hartgers

Portions Copyright ©1999 Lars Uffmann

Portions Copyright ©2003 IBM Corporation

Portions Copyright ©2004 Hewlett-Packard Company

Portions Copyright ©2004 Howard Chu, Symas Corp.

### **OpenSSL**

An implementation of Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocol.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young.

This product includes cryptographic software written by Tim Hudson.

### **PHP**

PHP is a widely-used scripting language that is especially suited for Web development and can be embedded into HTML.

Copyright ©1999-2006 The PHP Group. All rights reserved.

This product includes PHP software, freely available from <http://www.php.net/software/>

### **proxy-libintl**

proxy-libintl is a small static library. It acts as a proxy for the the DLL from gettext.

Tor Lillqvist <tml@iki.fi>, July 2008

Complete source code is available at: <http://kerio.com/...>

### **sdbm**

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

### **slf4j**

slf4j is a simple logging facade for Java.

Copyright ©2004-2010 QOS.CH

Copyright ©2004-2005 SLF4J.ORG

Copyright ©2005 - 2010, James Auldridge

Copyright ©1999-2005 The Apache Software Foundation.

**Tigase**

The Tigase Jabber/XMPP Server is Open Source and Free (GPLv3) {Java} based server.

Copyright ©2004 Tigase.org. <<http://www.tigase.org/>>

Copyright ©2001-2006 Tigase Developers Team. All rights Reserved.

Copyright ©2004-2011 "Artur Hefczyc" <[artur.hefczyc@tigase.org](mailto:artur.hefczyc@tigase.org)>

Copyright ©2009 "Tomasz Sterna" <[tomek@xiaoka.com](mailto:tomek@xiaoka.com)>

Copyright ©2001-2008 Julien Ponge, All Rights Reserved.

Copyright© 2008 "Bartosz M. Małkowski" <[bartosz.malkowski@tigase.org](mailto:bartosz.malkowski@tigase.org)>

**Windows Template Library 9.0**

The use and distribution terms for this software are covered by the Common Public License 1.0 (<http://opensource.org/licenses/cpl1.0.php>) which can be found in the file CPL.TXT at the root of this distribution. By using this software in any fashion, you are agreeing to be bound by the terms of this license. You must not remove this notice, or any other, from this software.

Copyright© 2014 Microsoft Corporation, WTL Team. All rights reserved.

**zlib**

General-purpose library for data compressing and decompressing.

Copyright ©1995-2005 Jean-Loup Gailly and Mark Adler.