

A large, modern building with a dark, angular facade and many windows is visible in the background, partially obscured by a blue diagonal band.

KerioConnect

ADMINISTRATOR GUIDE

Find out how to install and configure Kerio Connect in different environments and how to set up advanced features.



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and Kerio Connect are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

Kerio Connect is copyright of Kerio. - 1999-2019 Kerio. All rights reserved.

Document Version: 9.2.3

Last updated (month/day/year): 12/31/2019

Contents

1 Introduction	8
2 Getting started	9
2.1 System requirements for Kerio Connect	9
2.2 Licenses in Kerio Connect	9
2.2.1 Users mapped from a directory service	10
2.2.2 Checking the number of users in your license	10
2.2.3 Optional components in Kerio Connect	11
2.2.4 Installing Kerio Connect licenses	11
2.2.5 Updating licenses	11
2.3 License Expiration	11
2.3.1 Reduced functionality in Kerio Connect	12
2.3.2 End of Grace Period	12
2.3.3 Renewal of Subscription	12
2.4 Installation	12
2.4.1 Installing Kerio Connect	13
2.4.2 Performing initial configuration in Kerio Connect	15
2.4.3 Installing Kerio Connect on Debian 7	20
2.4.4 Installing Kerio Connect on Debian 8/9	21
2.4.5 Installing Kerio Connect on Ubuntu Server 14.04 LTS	22
2.4.6 Installing Kerio Connect on Mac OS X 10.10 Yosemite and above	22
2.4.7 Registering Kerio Connect	26
2.4.8 How do I apply renewals or add-ons to my Kerio product?	31
2.4.9 Switching from a 32-bit installation of Kerio Connect to 64-bit	31
2.4.10 Switching from 64-bit Kerio Connect back to 32-bit on Microsoft Windows	35
2.4.11 Uninstalling Kerio Connect	36
2.5 Upgrade	37
2.5.1 Upgrading to the latest version	37
2.5.2 Upgrading from versions older than Kerio Connect 8.0	40
2.6 Kerio Connect Multi-Server	44
2.6.1 Current version limitations	44
2.6.2 Configuring Kerio Connect Multi-Server	44
2.6.3 Installing Kerio Connect Multi-Server	45
2.6.4 Upgrading and downgrading Kerio Connect Multi-Server	51
2.6.5 Migrating from current installations to Kerio Connect Multi-Server	53
2.6.6 Securing Kerio Connect Multi-Server	56
2.6.7 Enforcing HTTPS in Kerio Connect Multi-Server	57
2.6.8 Licensing Kerio Connect Multi-Server	58
2.6.9 Managing Kerio Connect Multi-Server	58
2.6.10 Creating users in Kerio Connect Multi-Server	58
2.6.11 Accessing the Kerio Connect mailboxes	60
2.6.12 Monitoring Kerio Connect Multi-Server with the Zabbix server	60
2.6.13 Troubleshooting Kerio Connect Multi-Server	61
2.7 Kerio Cloud	61
2.7.1 Creating accounts in Kerio Cloud	65
2.7.2 Configuring domains in Kerio Cloud	66
2.7.3 Verifying domains for Kerio Cloud	67
2.7.4 DNS records for Kerio Cloud	68
2.7.5 Managing Kerio Connect domain	70

2.7.6 Anti-spam protection in Kerio Cloud71
2.7.7 Upgrading your Kerio Cloud account73
2.7.8 Canceling services in the Kerio Cloud74
2.7.9 Accounts created before May 10, 201674
2.8 Virtual Appliance and Linux	93
2.8.1 Kerio Connect VMware Virtual Appliance	93
2.8.2 Installation on CentOS 6.4 - 64-bit (both i386 and x86_64)	96
2.8.3 Installation on openSUSE 11.4 - 32-bit	97
2.8.4 Installation on openSUSE 11.4 - 64-bit (x86_64)	98
2.8.5 Joining Kerio Connect running on Linux to Open Directory or Active Directory	98
2.8.6 Kerio Connect Virtual Appliance Networking (Debian Edition - Kerio Connect 7.3.x and later)	103
2.8.7 How to make PHP's mail() command work with Kerio MailServer on Linux	104
2.8.8 Working with the Kerio Connect Virtual Appliance (CentOS Edition - Kerio Connect 7.2.x and earlier)	105
2.8.9 Working with the Kerio Connect Virtual Appliance (Debian Edition - Kerio Connect 7.3.x and later)	106
2.8.10 PAM authentication is not working in SuSE	111
2.9 Hosting	112
2.9.1 Preparing an environment for Hosting	112
2.9.2 Configuring Kerio Connect for multitenancy	113
2.9.3 Assigning domain level rights to tenant accounts	113
2.9.4 Differentiating services to tenant accounts	114
2.9.5 Branding your service	115
2.9.6 Automating configuration via Kerio Connect API	115
2.9.7 Protecting the server from mail abuse	116
2.9.8 Preparing the server for client access	116
2.10 OS X	117
2.10.1 Kerio Connect Account Assistant	118
2.10.2 Configuring a Microsoft Exchange Internet account on Mac OS X	121
2.10.3 Support for Apple iCal/Calendar using the CalDAV standard	122
2.10.4 Contacts folders in Apple Addressbook/Contacts app via CardDAV	125
2.10.5 Delegation in Microsoft Outlook 2011	126
2.10.6 Enabling logging for synchronization with Outlook for Mac	128
2.10.7 Enabling PHP's mail() command to work with Kerio Connect on Mac OS X?	129
2.10.8 How to manually create a CardDAV account in Apple Address Book	131
2.10.9 Logging iCal and AddressBook communication	133
2.10.10 Kerio Connect Account Assistant handling on OS X 10.8 Mountain Lion	134
2.10.11 Viewing events in delegated Calendars when using iCal with CalDAV	134
2.10.12 Getting iCal Auto Complete to work	135
2.10.13 Moving mail to a public folder in Apple Mail deletes the mail	137
2.11 Kerio Connect API	137
3 Using	138
3.1 Monitoring Kerio Connect	138
3.1.1 Monitoring incoming and outgoing messages	138
3.1.2 Traffic charts	140
3.1.3 Viewing statistics	140
3.1.4 Displaying users currently connected to Kerio Connect	141
3.1.5 Monitoring CPU and RAM usage	142
3.2 Export and Migration	142
3.2.1 Importing users in Kerio Connect	143
3.2.2 Exporting users in Kerio Connect	145
3.2.3 Kerio Connect Migration Service	145
3.2.4 Kerio Exchange Migration Tool	150
3.2.5 KerioIMAP Migration Tool	153

3.2.6 Transferring an installation of Kerio Connect to another server or Operating System	156
3.2.7 Migrating users from directory service to local database	158
3.3 Archiving	159
3.3.1 Archiving in Kerio Connect	159
3.3.2 Archiving chat in Kerio Connect Client	163
3.3.3 Archiving emails using GFI Archiver	164
3.4 Backup	165
3.4.1 Configuring backup in Kerio Connect	165
3.4.2 Data recovery in Kerio Connect	168
3.4.3 Examples of data recovery in Kerio Connect	170
3.5 Data store	176
3.5.1 Configuring data store in Kerio Connect	176
3.5.2 Automatic data consistency check and fix in Kerio Connect	179
3.6 Instant Messaging	180
3.6.1 Configuring instant messaging in Kerio Connect	180
3.6.2 Configuring DNS for instant messaging	184
3.6.3 Archiving instant messaging	186
3.6.4 Enabling chat in Kerio Connect Client	187
3.6.5 Configuring clients for instant messaging	189
3.6.6 Initiating group chat in instant messaging	194
4 Settings	202
4.1 Basic configuration	202
4.1.1 Accessing Kerio Connect	203
4.1.2 Authenticating users through PAM	204
4.1.3 Public folders in Kerio Connect	205
4.1.4 Setting access rights in Kerio Connect	209
4.1.5 Creating time ranges in Kerio Connect	212
4.1.6 Configuring IP address groups	213
4.1.7 Managing logs in Kerio Connect	215
4.1.8 Customizing Kerio Connect	217
4.1.9 Customizing the Kerio Connect Client login page	222
4.1.10 Filtering messages on the server	224
4.1.11 Integrating Kerio Connect with Kerio Operator	234
4.1.12 Joining two servers with different domains into one server	235
4.1.13 Changing the time zone definitions in <code>timezones.xml</code> file in Kerio Connect	236
4.1.14 How to change from individual public folders to global public folders and keep your existing public folder data	238
4.1.15 Upgrading the MAPI property database in Kerio Connect 9.1	239
4.1.16 Using Kerio Assist tool	241
4.2 Administration	242
4.2.1 Accessing Kerio Connect administration	242
4.2.2 Navigating through the Kerio Connect administration interface	244
4.2.3 Using Dashboard in Kerio Connect	245
4.2.4 Gathering usage statistics	246
4.2.5 What ports are used by Kerio Connect for remote administration?	248
4.3 Domains	248
4.3.1 Domains in Kerio Connect	248
4.3.2 Creating domains in Kerio Connect	251
4.3.3 Adding company and user contact information in Kerio Connect	255
4.3.4 Renaming domains in Kerio Connect	257
4.3.5 Distributed domain	258
4.3.6 How to change a user's authentication method from internal, to Active Directory or Open Directory	268

4.4 Accounts268
4.4.1 Creating user accounts in Kerio Connect269
4.4.2 Creating user groups in Kerio Connect272
4.4.3 Maintaining user accounts in Kerio Connect275
4.4.4 Creating mailing lists in Kerio Connect281
4.4.5 Creating aliases in Kerio Connect283
4.4.6 Configuring resources in Kerio Connect287
4.4.7 Renaming user account289
4.4.8 How do I create a catch-all email address?290
4.4.9 How do I move a user to a different domain?290
4.4.10 How do I re-index a user's folder if it has become corrupt?291
4.4.11 Is there a convenient way for a list moderator or administrator to mass subscribe people?291
4.4.12 Resource calendars hide the event subject. Can this behavior be modified?292
4.5 Directory service293
4.5.1 Connecting Kerio Connect to directory service293
4.5.2 Kerio Active Directory Extension298
4.5.3 Kerio Open Directory Extension298
4.5.4 How do I configure KMS on a child Active Directory domain?299
4.5.5 How do I get the LDAP server in Kerio Connect to work with Microsoft Outlook?300
4.5.6 How to configure LDAP access in Evolution302
4.5.7 How to map users from a specific Organizational Unit (ou) only303
4.5.8 Migrating user accounts from local database to directory service304
4.5.9 Kerberos Authentication with OSX 10.7 against an OpenDirectory Server305
4.5.10 Mapping different name from Active Directory307
4.5.11 Mapping users/groups from an OpenLDAP or Generic LDAP server309
4.5.12 What ports should be open on my Active Directory controller for synchronization with Kerio Connect/MailServer?323
4.5.13 Accessing LDAP with LinkSys SPA942323
4.6 Security323
4.6.1 Securing Kerio Connect324
4.6.2 Configuring anti-spoofing in Kerio Connect328
4.6.3 Password policy in Kerio Connect329
4.6.4 Authenticating messages with DKIM332
4.6.5 Configuring DNS for DKIM334
4.6.6 Configuring SSL/TLS in Kerio Connect338
4.6.7 PCI DSS Compliance341
4.6.8 Antispam342
4.6.9 Antivirus369
4.6.10 SSL certificates377
4.7 Mail delivery and DNS records390
4.7.1 Essential DNS Records for Mail Delivery and Spam Protection391
4.7.2 Scheduling email delivery393
4.7.3 Configuring POP3 connection394
4.7.4 Receiving email via ETRN397
4.7.5 Configuring Autodiscover in Kerio Connect399
4.7.6 What is an MX record, and how is it created?401
4.8 Services403
4.8.1 Services in Kerio Connect403
4.8.2 Configuring the SMTP server407
4.8.3 Securing the SMTP server411
4.8.4 Can I run Kerio Connect and IIS web services on the same computer?412

5.1 Common issues	414
5.1.1 Cannot start HTTP or HTTPS services on Mac OS	415
5.1.2 Detecting that Kerio Connect has been compromised and used for spamming	415
5.1.3 Browser extensions or add-ons may interfere with Kerio products	417
5.1.4 Distributed Sender Blackhole List Errors (DSBL)	417
5.1.5 How do I get older versions of Kerio software?	418
5.1.6 How do I get the .eml source for an email?	418
5.1.7 How do I reset the password for a user if I've lost access to the WebAdmin of Kerio Connect?	419
5.1.8 Active Directory/LDAP error: Unable to search in dc=example,dc=domain,dc=com (Size limit exceeded)	420
5.1.9 How to fix a malformed .journal.db with a SQLite error	420
5.1.10 How to repair or reset Anti-Virus in Kerio Connect	421
5.1.11 I can't send outgoing mail if I'm using Open Directory or Active Directory	422
5.1.12 I can't use national characters in my password.	423
5.1.13 I have created a custom rule to allow an email address or domain through but it is still being blocked	423
5.1.14 I've been training the spam filter but I'm still receiving the same spam emails	423
5.1.15 Kerio Connect Client is not displayed correctly in Internet Explorer	424
5.1.16 Kerio Connect user cannot login to their email account	424
5.1.17 Moving user from active directory service to local user database or vice versa causes synchronization errors with Outlook 2011	425
5.1.18 POP3 connection fails during download	426
5.1.19 SMTP Status and Reply codes	426
5.1.20 Users folder size is reporting incorrectly in WebAdmin	427
5.1.21 Why am I getting multiple copies of an email?	428
5.1.22 Why does Kerio Connect automatically expunge messages marked for deletion through IMAP?	428
5.1.23 Why does the Exchange migration tool state I am not an administrator?	429
5.2 General errors	429
5.2.1 Kerio Connect shows disk space warnings	430
5.2.2 550 5.7.1 Relaying to <email@address.com> denied (authentication required)	431
5.2.3 Cannot send to some mail servers with the explanation that the SMTP greeting failed	431
5.2.4 I get an error that says 'create_time < install_time'	432
5.2.5 I get the error 'Error: unable to save settings' when updating settings in the old Webmail	432
5.2.6 I'm receiving errors and bounces when sending email, what do they mean?	433
5.2.7 I receive a 'script error' message	433
5.2.8 I receive the error "Failed to detect the installation setup requirements (code: -5)" when I install the Outlook Connector.	434
5.2.9 Login problem on 64bit Windows when using Kerberos	434
5.2.10 Message body is garbled when email is received by Microsoft Exchange server	435
5.2.11 My Calendar/Contacts/Tasks/Notes folders are now showing as Mail folders. How do I fix this?	436
5.2.12 Outlook generates MAPI_E_TIMEOUT error during certain operations	436
5.2.13 Some POP3 clients generate an authentication error in the security log, but successfully download new email	437
5.2.14 Some services, for example WebMail, do not start. How do I fix this?	437
5.2.15 Why am I getting multiple copies of an email?	438
5.2.16 Why do I see 'IP address x.x.x.x rejected: too many connections' in the warning log?	438
5.2.17 Why is a new attendee created when the original attendee accepts a meeting invitation?	439
5.3 Vulnerabilities	439
6 Glossary	440
7 Legal notices	446
7.1 Trademarks and registered trademarks	446
7.2 Used open source software	447

1 Introduction

Kerio Connect is a messaging and collaboration solution for small and mid-sized businesses. With Kerio Connect you can manage your company emails, chats, calendars, contacts, and tasks easily and from anywhere.

It offers deployment flexibility (Microsoft Windows, macOS, Linux, virtual appliance, on-prem, cloud) and broad mobile support. Users can access their mailboxes through their favorite email client, Kerio Connect Client, web browsers, or mobile devices.

Kerio Connect is secured against malicious attacks with SSL encryption, S/MIME, antispam and antivirus. You can easily archive and backup the whole server, and restore it back when necessary.

Kerio Connect web based administration is clean and simple, and you can upgrade to the latest version with just one click.

If you have multiple Kerio products, stay in control of all your Kerio deployments through a single centralized web interface – [MyKerio](#).

2 Getting started

Kerio Connect is an email and instant messaging server that features multiple deployment options, Microsoft Outlook integration, web based email access, and mobile device access.

This guide provides general step-by-step instructions for deploying Kerio Connect in a common on-premises scenario. Note that Kerio Connect is also available as a hosted service in the event that you cannot deploy it within your own infrastructure.

1 Select a deployment type

Kerio Connect is available as a 64-bit Debian virtual appliance for VMware, or as a software application for current versions of Microsoft Windows, Mac OS X, and Linux. The product features and functionality are nearly identical across all versions.

2 Install and upgrade Kerio Connect

You can download Kerio Connect from the [Kerio website](#). For instructions on Kerio Connect installation, see [Installing Kerio Connect](#).

After installation, the software automatically checks for updates. The web administration notifies you when an update is ready. For more information, refer to [Upgrading to the latest version](#) (page 37).

3 Access Kerio Connect

After installation, the administrator performs the initial configuration from a web browser by going to the name or IP address of the Kerio Connect server. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

4 Create user accounts

If you do not use a directory service, administrators can create and manage users directly in the administration interface. For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).

5 Secure Kerio Connect and mail flow

Kerio Connect includes many security features to protect against misconduct, unauthorized access, harmful attachments, identity spoofing, and tampering of content. For more information, refer to [Securing Kerio Connect](#) (page 324).

6 Access emails

Kerio Connect supports mailbox synchronization with a variety of mobile platforms, browsers, and desktop applications, including the Kerio Connect Client [web](#) and [desktop](#) applications, [mobile devices](#), [Kerio Connect Account Assistant](#) and [Kerio Outlook Connector](#)

2.1 System requirements for Kerio Connect

You can find detailed and up-to-date **system requirements** for Kerio Connect on our website:

[Kerio Connect System Requirements](#)

2.2 Licenses in Kerio Connect

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 are count as 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.

2.2.1 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.

2.2.2 Checking the number of users in your license

The Kerio Connect Administration interface displays information on the number of users you have and the number of licenses you hold.

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

Number of users active from the last server restart

Number of users created and enabled

License Details	
License number:	12345-123-5-12345
Software Maintenance expiration date:	2014-07-16
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
Install license...	
Update registration info...	

You can always remove inactive users to make space for new users in your license:

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

The screenshot shows a user management screen in the Kerio Connect web interface. At the top, there's a search bar labeled 'Where is ...' and a dropdown for 'admin'. Below the search bar is a table header with columns: 'on', 'Last Login', and 'Groups'. The 'Last Login' column contains dates: '2015-01-22 08:21', '2014-02-10 11:21', and '2014-05-05 11:21'. A context menu is open over the 'Last Login' column, with 'Sort Ascending' and 'Sort Descending' options visible. To the left of the table, a sidebar lists user attributes with checkboxes: 'Username' (checked), 'Full Name' (checked), 'Description' (checked), 'Access Policy' (unchecked), 'Last Login' (checked), and 'Groups' (checked). A hand cursor is pointing at the 'Last Login' checkbox in the sidebar.

3. Sort users based on **Last Login** and accordingly [remove users](#) who do not use Kerio Connect.

2.2.3 Optional components in Kerio Connect

Kerio Connect has the following optional components:

- » Kerio Antivirus. For more information, refer to [Antivirus protection in Kerio Connect](#) (page 370).
- » Exchange ActiveSync
- » Kerio Anti-spam. For more information, refer to [Kerio Anti-spam filter](#) (page 345).

These components are licensed individually. For more information, refer to [Registering Kerio Connect](#) (page 26).

2.2.4 Installing Kerio Connect licenses

License registration binds customer details to a license and specifies the anniversary date of Software Maintenance. You can register a license from the support area of the Kerio website during the software purchase or from the administration interface. License activation binds a license to an installation of the product. You can activate (install) a license in the dashboard of the web administration interface. For more information, refer to [Registering Kerio Connect](#) (page 26).

2.2.5 Updating licenses

If you purchase additional users or components, your license gets updated automatically within 24 hours.

2.3 License Expiration

When the Kerio Connect subscription expires, the functionality of product becomes limited, making it less effective in its function as an email server. It is highly recommended that subscription must be renewed to maintain all important functions. For more information, refer to [Renewal of Subscription](#) (page 12).

IMPORTANT

Once Kerio Connect subscription expires, the product and definition updates for Anti-virus and Anti-Spam stops working, increasing the risk of your system being exposed to latest threats.

2.3.1 Reduced functionality in Kerio Connect

The following functions and operations are terminated when subscription of Kerio Connect reaches the grace period:

- » ActiveSync. For more information refer to [Support for ActiveSync](#).
- » Anti-virus updates. For more information, refer to [Antivirus protection in Kerio Connect](#) (page 370).
- » Anti-spam updates. For more information, refer to [Configuring spam control in Kerio Connect](#) (page 342).

2.3.2 End of Grace Period

During the grace period, Kerio Connect allows user to use web and desktop client interface with reduced functionality. At the time when grace period elapses, Kerio Connect clients get blocked until the subscription is renewed.

2.3.3 Renewal of Subscription

To renew your Kerio Connect subscription, please reach out to your preferred reseller or go to [Ordering GFI Solutions](#).

2.4 Installation

Kerio Connect is available as:

- » Windows Installer
- » Mac OS X Installer
- » Linux RPM Installer
- » Linux Debian Installer
- » Virtual appliance for VMware products

For detailed system requirements, see the product pages.

2.4.1 Installing Kerio Connect	13
2.4.2 Performing initial configuration in Kerio Connect	15
2.4.3 Installing Kerio Connect on Debian 7	20
2.4.4 Installing Kerio Connect on Debian 8/9	21
2.4.5 Installing Kerio Connect on Ubuntu Server 14.04 LTS	22
2.4.6 Installing Kerio Connect on Mac OS X 10.10 Yosemite and above	22
2.4.7 Registering Kerio Connect	26
2.4.8 How do I apply renewals or add-ons to my Kerio product?	31
2.4.9 Switching from a 32-bit installation of Kerio Connect to 64-bit	31
2.4.10 Switching from 64-bit Kerio Connect back to 32-bit on Microsoft Windows	35
2.4.11 Uninstalling Kerio Connect	36

2.4.1 Installing Kerio Connect

Kerio Connect is available as a standard installation package for **Windows**, **Mac OS X**, **Linux RPM** and **Linux Debian**.

Kerio Connect can also be downloaded as a **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. For more information, refer to [Kerio Connect VMware Virtual Appliance](#) (page 93).

Windows

Refer to the [product pages](#) to know the prerequisites before installation. Once everything is set up, you can start with the installation process as explained below:

1. Download the [Kerio Connect installation file](#).
2. Run the installer. 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. Kerio Connect engine starts (immediately or after restart) and runs as a service.

NOTE

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

5. Perform the initial configuration before you start using Kerio Connect. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

Mac OS X

Refer to the [product pages](#) to learn about the prerequisites before installation. Once everything is set up, you can start with the installation process as explained below:

1. Download the [Kerio Connect installation file](#).
2. Run the installer. 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 start-up and runs as a service.
5. Perform the initial configuration before you start using Kerio Connect. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

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`

IMPORTANT

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

Linux RPM

Refer to the [product pages](#) to learn about the prerequisites before installation. Once everything is set up, you can start with the installation process as explained below:

1. Download the [Kerio Connect installation file](#).
2. Run the installer. 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 before you start using Kerio Connect. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

New installation

Start the installation using this command:

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

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

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

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

Kerio Connect engine

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

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

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

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

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

Linux DEB

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

1. Download the [Kerio Connect installation file](#).
2. Run the installer. Kerio Connect must be installed under the user with `root` rights.
3. Follow the steps in the installation wizard. Kerio Connect gets installed in the `/opt/kerio/mailserver` folder.
4. Click **Finish** to complete the installation.
5. Perform the initial configuration before you start using Kerio Connect. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

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** (located in the installation directory in folder doc) file carefully and immediately after installation.

Kerio Connect engine

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

Alternatively, use the following commands to start or stop the daemon manually. To run these commands, Kerio Connect must be run by a `root` user

- » **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`

NOTE

When installing on Debian with a graphical user interface, open the installation package with the `gdebi`. To do this, right-click the file and click **Open with**.

2.4.2 Performing initial configuration in Kerio Connect

Before you start using Kerio Connect, you must perform an initial configuration to configure the basic parameters for Kerio Connect. These parameters 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` - an XML file with the UTF-8 coding which includes information of user accounts, groups and aliases.
- » `mailserver.cfg` - 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 etc.

The default location of these configuration files is:

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

NOTE

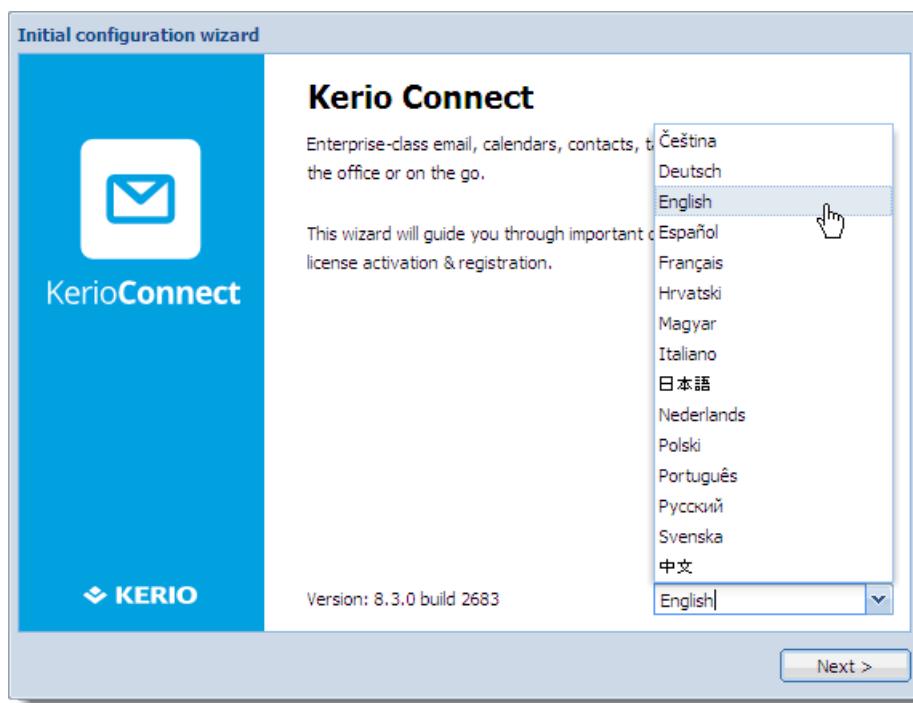
On Mac OS X and Linux systems, files can only be maintained if the user is logged in as the `root` user.

Configuring initial parameters

NOTE

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

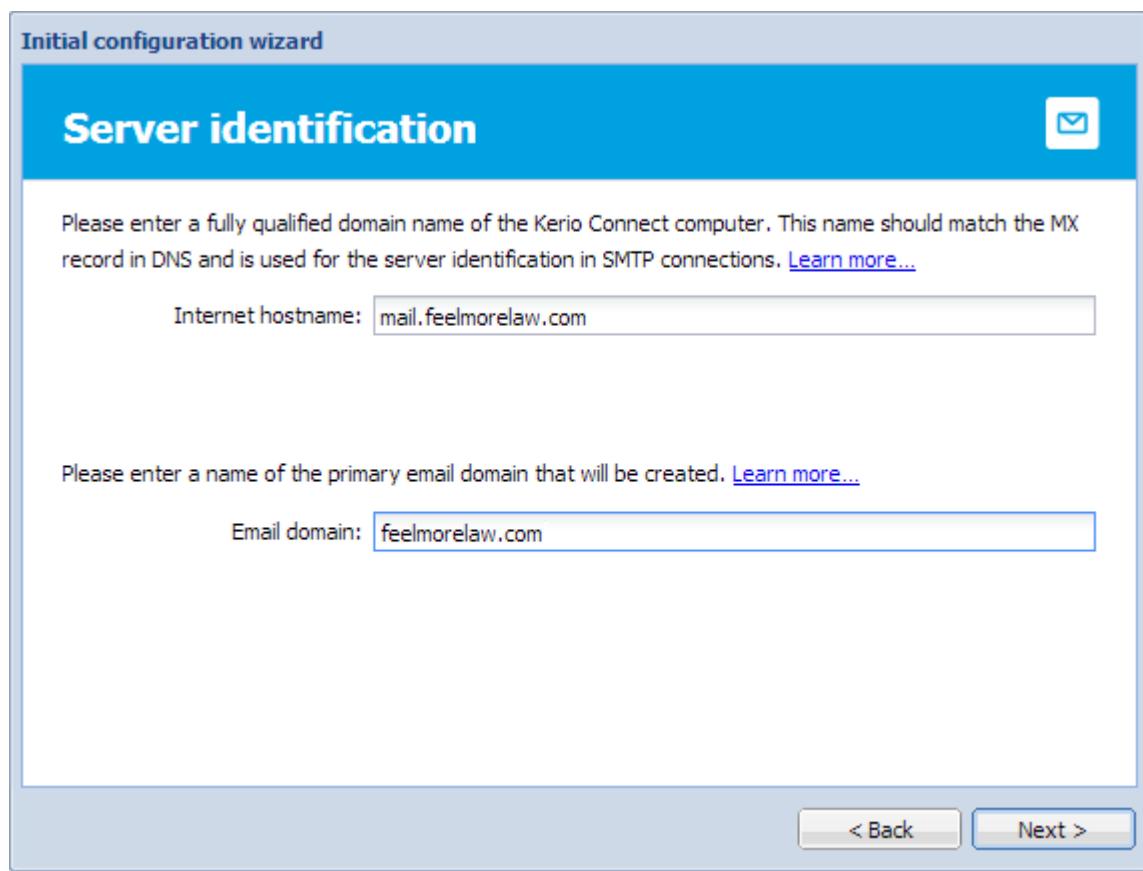
1. [Install Kerio Connect](#).
2. Open the following address in your web browser: `https://kerio_connect_server:4040/admin`
3. Select a language for the initial configuration wizard and click **Next**.



NOTE

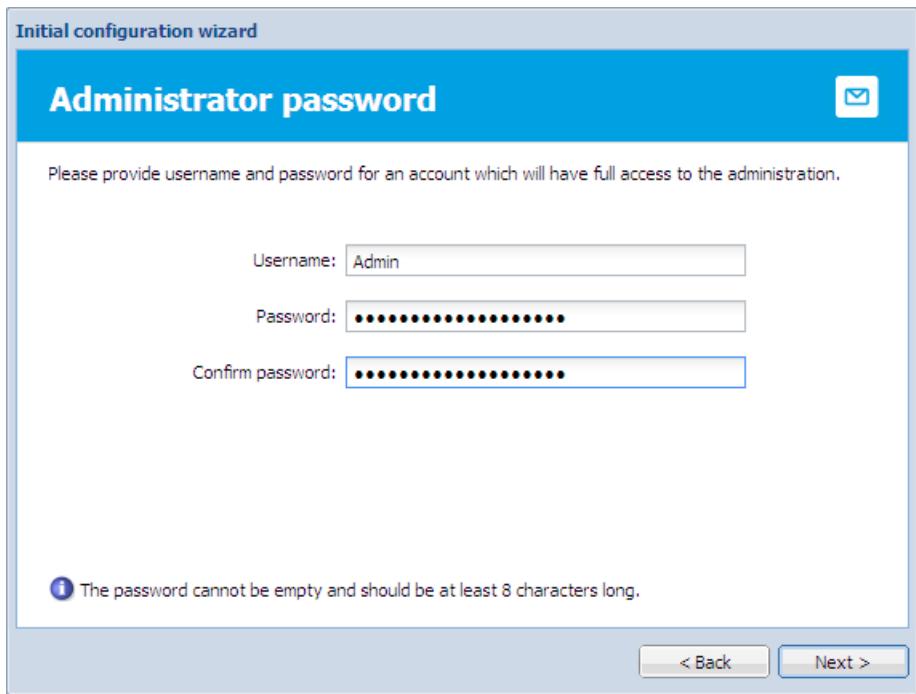
This language gets set as the default language.

- Accept **License Agreement** and click **Next**.
- Specify **Internet hostname** and **Email domain**.



Field	Description
Internet hostname	Enter a fully qualified domain name of the Kerio computer. The name should match the MX record in DNS and is used for the server identification in SMTP connections.
Email domain	Enter a name of the primary email domain that will be created. For more information, refer to Domains in Kerio Connect (page 248).

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

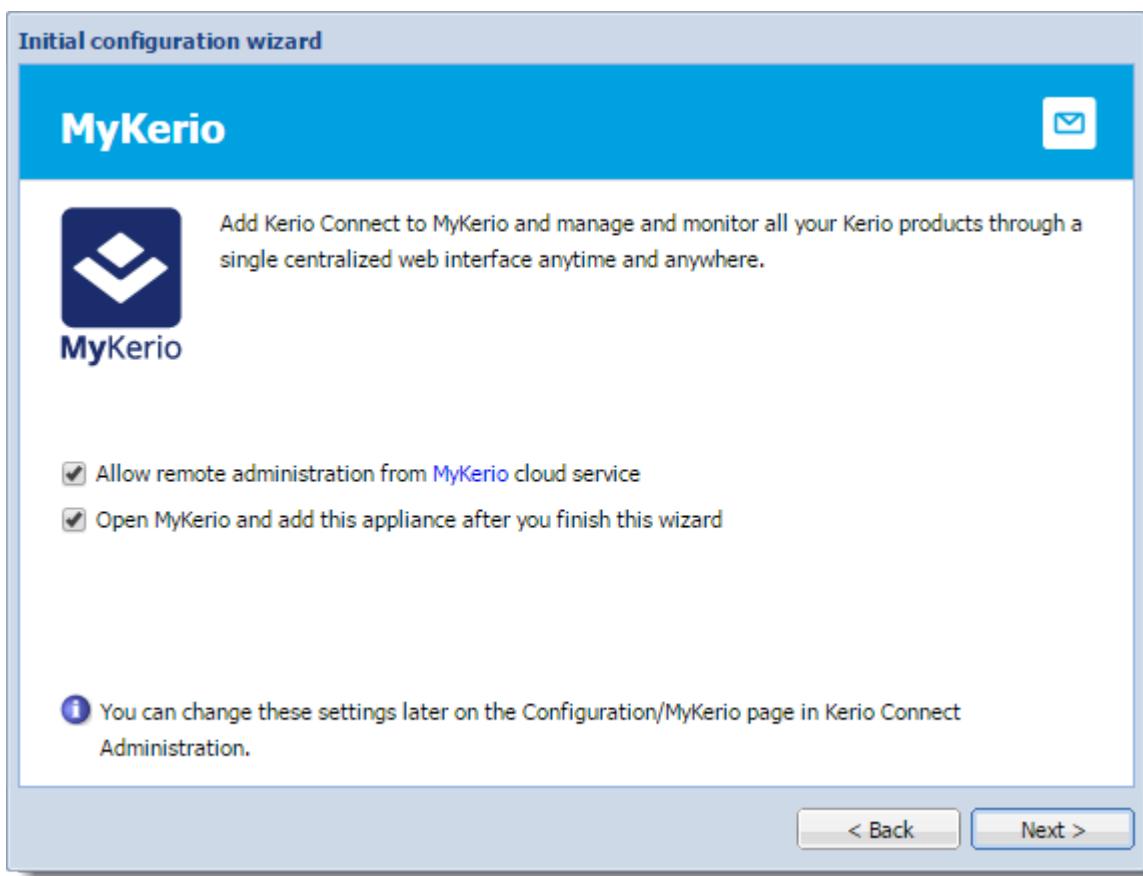


NOTES

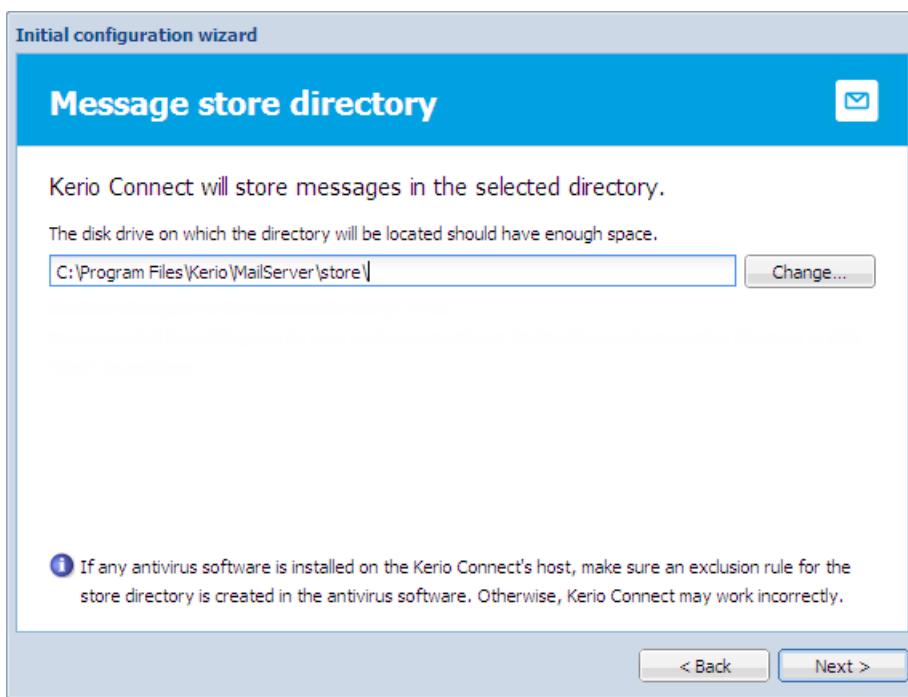
This first administration account consumes one license, you can later switch to the [built-in admin account](#) in the administration interface.

For more information, refer to [Setting access rights in Kerio Connect](#) (page 209).

8. 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](#).



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



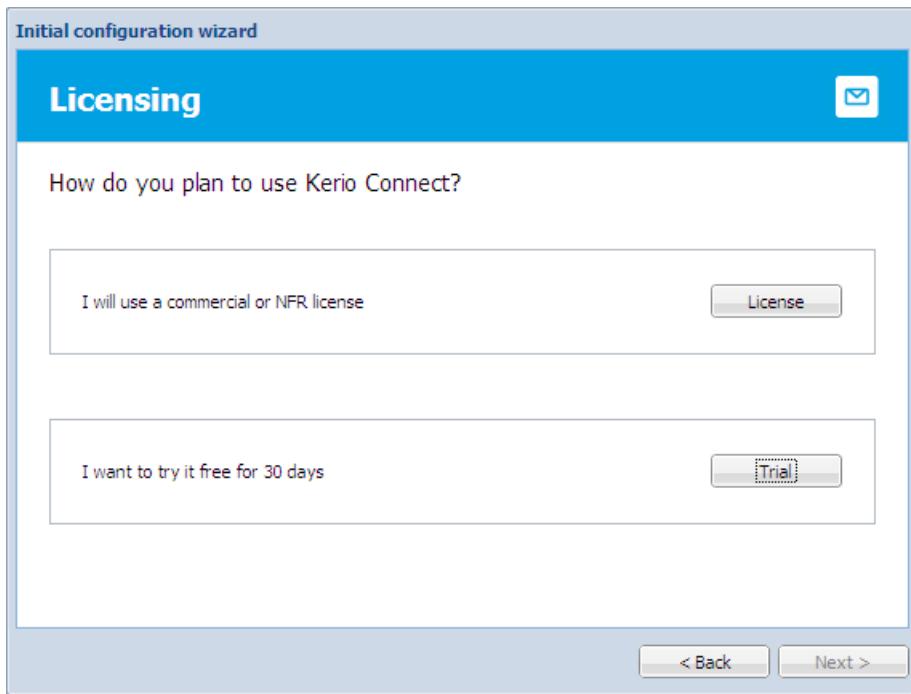
Kerio Connect verifies if you have enough free disk space available.

For more information, refer to [Configuring data store in Kerio Connect](#) (page 176).

NOTE

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

10. Register the product or continue without the registration. Click **Next**.



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](#).

2.4.3 Installing Kerio Connect on Debian 7

Learn how to install Kerio Connect 8.3 on Debian 7 (i386 and x86_64).

1. On Linux Debian 7, disable **exim4 MTA** using the following command: `sudo apt-get remove exim4-base`
2. Install the support for the international locales using the following command: `sudo apt-get install locales-all`
3. Download the **.deb** installation package from the [Kerio Connect website](#) and install Kerio Connect using the following command: `dpkg -i kerio-connect-8.3.x-xxxx-linu-x-xxxx.deb`

NOTE

Do not forget to replace `x-xxx` and `xxxx` with appropriate version numbers.

4. In your browser, use `https://servername:4040/admin` to open the Kerio Connect administration and perform the initial configuration. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).
5. Install missing dependencies if necessary: `apt-get update apt-get -f install`
6. Optionally, replace sendmail with the binary from Kerio Connect: `sudo mv /usr/sbin/sendmail /usr/sbin/sendmail-old sudo cp /opt/kerio/mailserver/sendmail`

```
/usr/sbin/sendmail sudo cp /opt/kerio/mailserver/lib* /lib/
```

NOTE

Do not forget to add appropriate A and MX records to your DNS server.

Kerio Connect users can authenticate against PAM with the /etc/pam.d/kerio-connect PAM module.

Example of missing dependencies

The following script suggests that the sysstat dependency is not installed.

```
root@debian7:~# dpkg -i kerio-connect-8.3.0-2355-b2-linux-amd64.deb
...
dpkg: dependency problems prevent configuration of kerio-connect:
  kerio-connect depends on sysstat; however:
    Package sysstat is not installed.
dpkg: error processing kerio-connect (--install):
  dependency problems - leaving unconfigured
Errors were encountered while processing:
  kerio-connect
root@debian7:~# apt-get update
root@debian7:~# apt-get -f install
The following NEW packages will be installed:
  libsensors4 sysstat
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 446 kB of archives.
After this operation, 1,442 kB of additional disk space will be used.
Do you want to continue [Y/n]?
...
Setting up kerio-connect (8.3.0.2355.0.beta2-1) ...
[ ok ] Starting Kerio Connect: Engine .
```

2.4.4 Installing Kerio Connect on Debian 8/9

Learn how to install Kerio Connect on Debian 8/9 (amd64).

1. On Linux Debian 8/9, disable **exim4 MTA** using the following command: `sudo apt-get remove exim4-base`.
2. Install the required system packages using the following command: `sudo apt-get install locales-all libsensors4 sysstat`.
3. Download the deb installation package from the [Kerio Connect web site](#) and install Kerio Connect using the following command: `sudo dpkg -i kerio-connect-9.0.x-xxxx-linu-x-xxxx.deb`.

NOTE

Do not forget to replace `x-xxx` and `xxxx` with appropriate version numbers.

4. Optionally, replace sendmail with the binary from Kerio Connect using the following command: `sudo mv /usr/sbin/sendmail /usr/sbin/sendmail-old sudo cp /opt/kerio/mailserver/sendmail /usr/sbin/sendmail sudo cp /opt/kerio/mailserver/lib* /lib/`

5. Open Kerio Connect Administration using <https://servername:4040/admin>.

NOTE

Do not forget to add appropriate A and MX records to your DNS server.

Kerio Connect users can authenticate against PAM with the `/etc/pam.d/kerio-connect` PAM module.

Starting and stopping the server

- » To start Kerio Connect: `sudo service kerio-connect start`
- » To stop Kerio Connect: `sudo service kerio-connect stop`

2.4.5 Installing Kerio Connect on Ubuntu Server 14.04 LTS

Learn how to install Kerio Connect 8.3 on Ubuntu 14.04 LTS Server (amd64).

1. On Ubuntu Server 14.04 LTS, install the necessary libraries using the following command: `sudo apt-get install sysstat`
2. Generate system locales for different language in Kerio Connect client using the following command: `sudo locale-gen *.*UTF-8`
3. Download the deb installation package from the [Kerio Connect web site](#) and install Kerio Connect using the following command: `dpkg -i kerio-connect-8.3.0-xxxx-linu-x-amd64.deb`

NOTE

Do not forget to replace `xxxx` with appropriate version number.

4. In your browser, open the Kerio Connect administration <https://servername:4040/admin> and perform the initial configuration. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

NOTE

Do not forget to add appropriate A and MX records to your DNS server.

5. Optionally replace sendmail with the binary from Kerio Connect: `sudo mv /usr/sbin/sendmail /usr/sbin/sendmail-old sudo cp /opt/kerio/mailserver/sendmail /usr/sbin/sendmail sudo cp /opt/kerio/mailserver/libkt* /lib/`

Kerio Connect users can authenticate against PAM with the `/etc/pam.d/kerio-connect` PAM module.

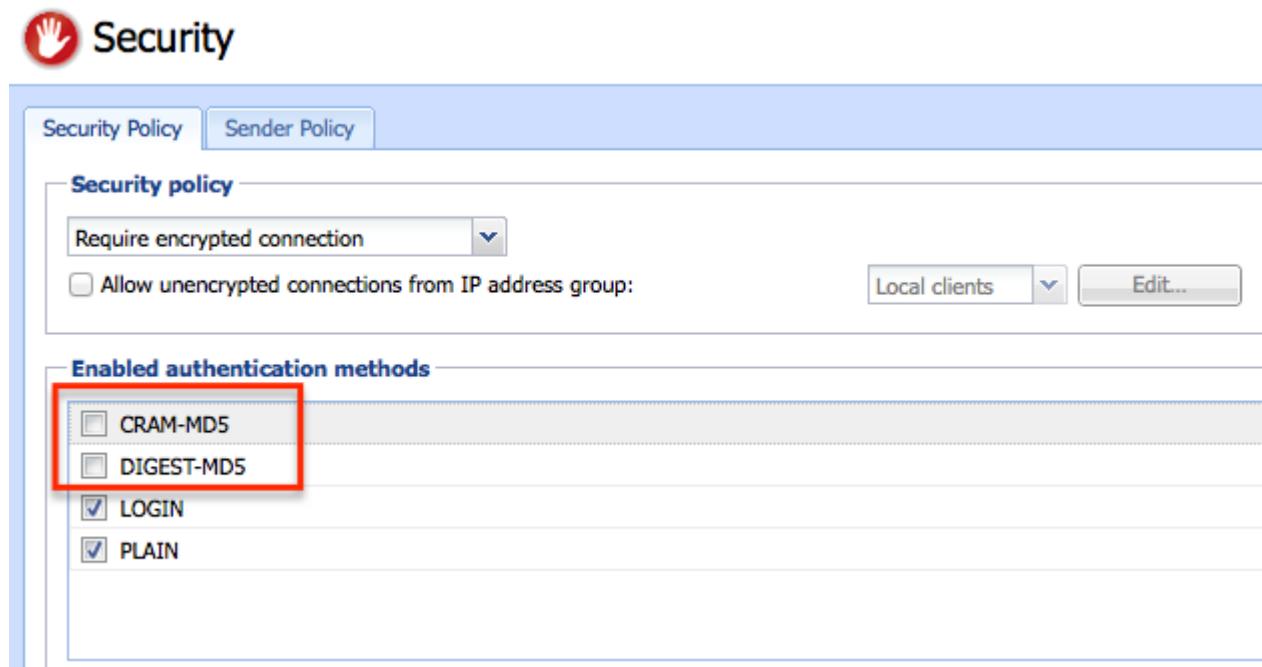
2.4.6 Installing Kerio Connect on Mac OS X 10.10 Yosemite and above

For optimal support of Mac OS X 10.10 (Yosemite) and above, you must install the current version of Kerio Connect. Additional configuration may be necessary to address the items as described in this topic.

Sending email or performing other operations in Apple Mail application may be slower than usual

Apple Mail application in Yosemite introduces a new option in your account settings to regularly attempt secure authentication. This secure authentication attempt fails and results in mail processing delays if your Kerio Connect server stores passwords in SHA format or uses a directory service.

Administrators can resolve this issue by disabling the MD5 authentication methods located in **Configuration > Security > Security Policy**.



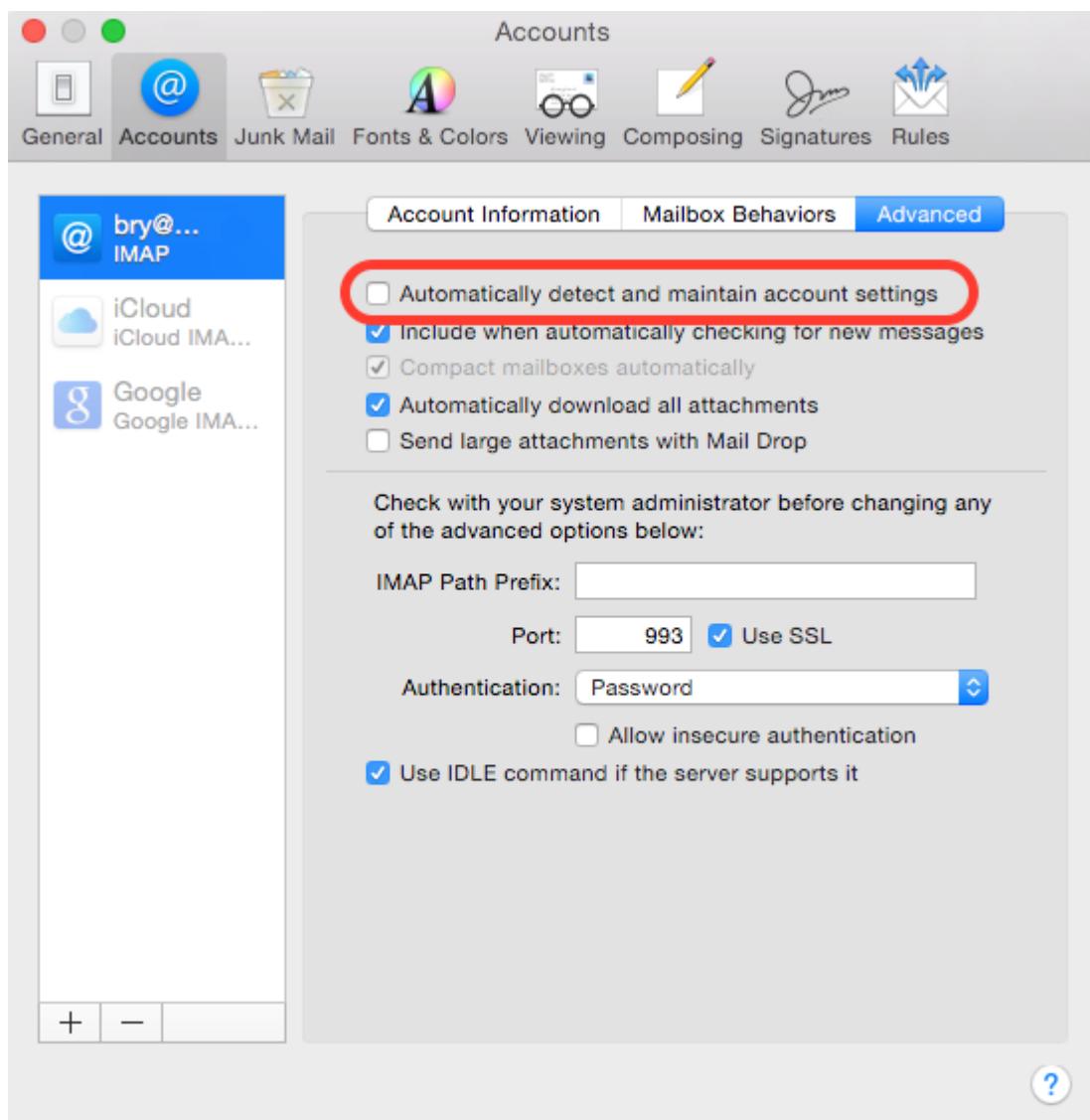
The screenshot shows the 'Security' configuration screen. The 'Security Policy' tab is active. In the 'Enabled authentication methods' section, the 'DIGEST-MD5' checkbox is selected and highlighted with a red box. Other methods listed are CRAM-MD5, LOGIN, and PLAIN.

Screenshot 1: Authentication methods available

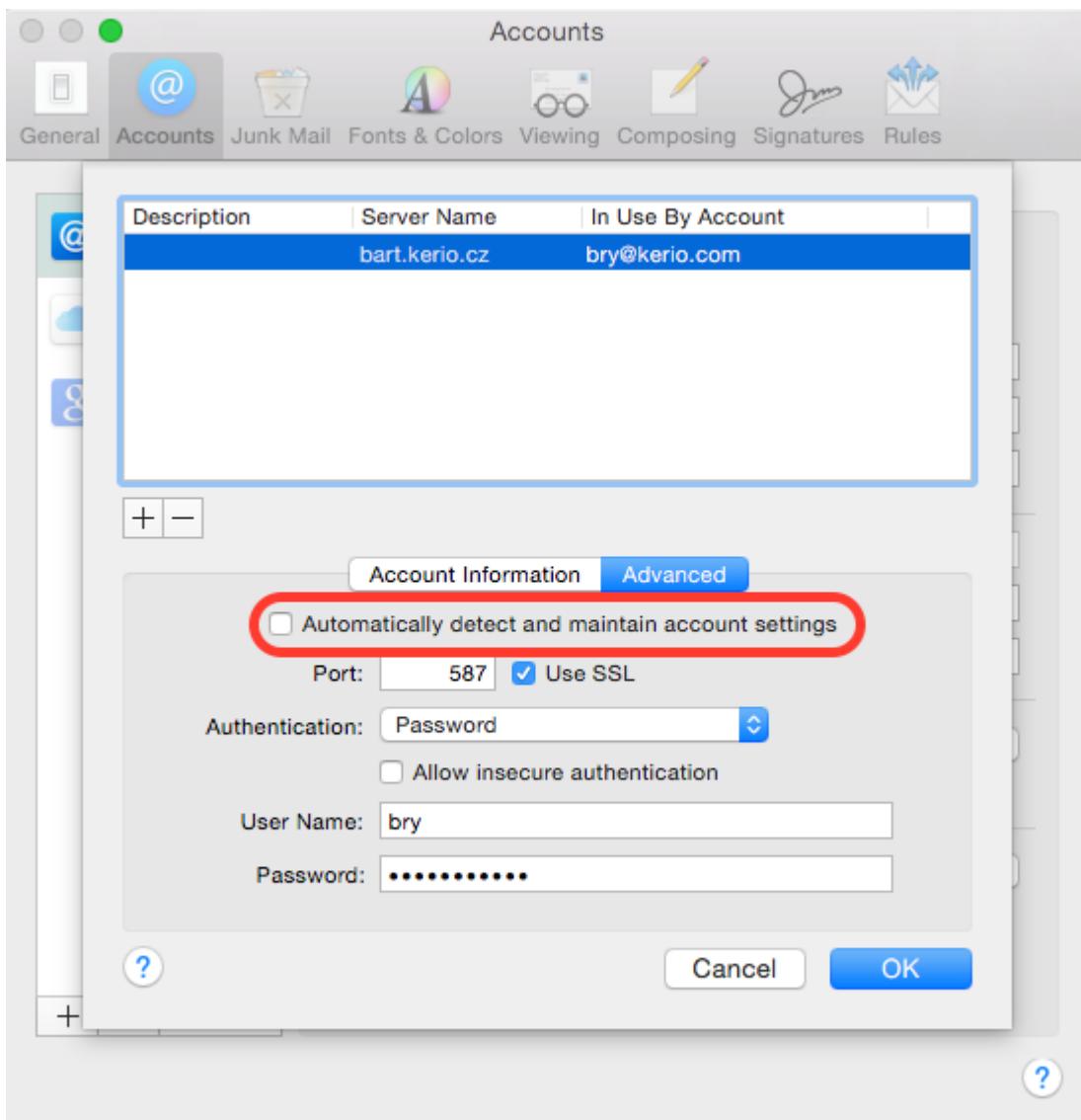
NOTE

To ensure security of passwords and data, set the security policy to **Require encrypted connection**. This option ensures that users connect via SSL.

You can resolve this issue by disabling the option **Automatically detect and maintain account settings** in your account settings. This setting applies to both the SMTP and IMAP/POP configuration.



Screenshot 2: IMAP settings



Screenshot 3: SMTP settings

Upgrading the Kerio Connect server from previous versions of Mac OS X

The Mac OS X installer moves all data located in `/usr` to a temporary **Recovered Items** folder during the upgrade process.

If Kerio Connect message store is located in the default location (`/usr/local/kerio/mailserver/store`) this action causes significant delays in the OS X upgrade.

If there is insufficient space available in the temporary folder, the data may be removed during the upgrade. Prior to performing the upgrade, move your mail store data to different physical storage device (e.g., USB drive or network location) to prevent data loss and to expedite the upgrade process.

Installing Oracle Java 8 JDK

Kerio Connect requires prior installation of the [Java 8 JDK](#) for specific features including full text searching and instant messaging.

2.4.7 Registering Kerio Connect

Why register Kerio Connect?

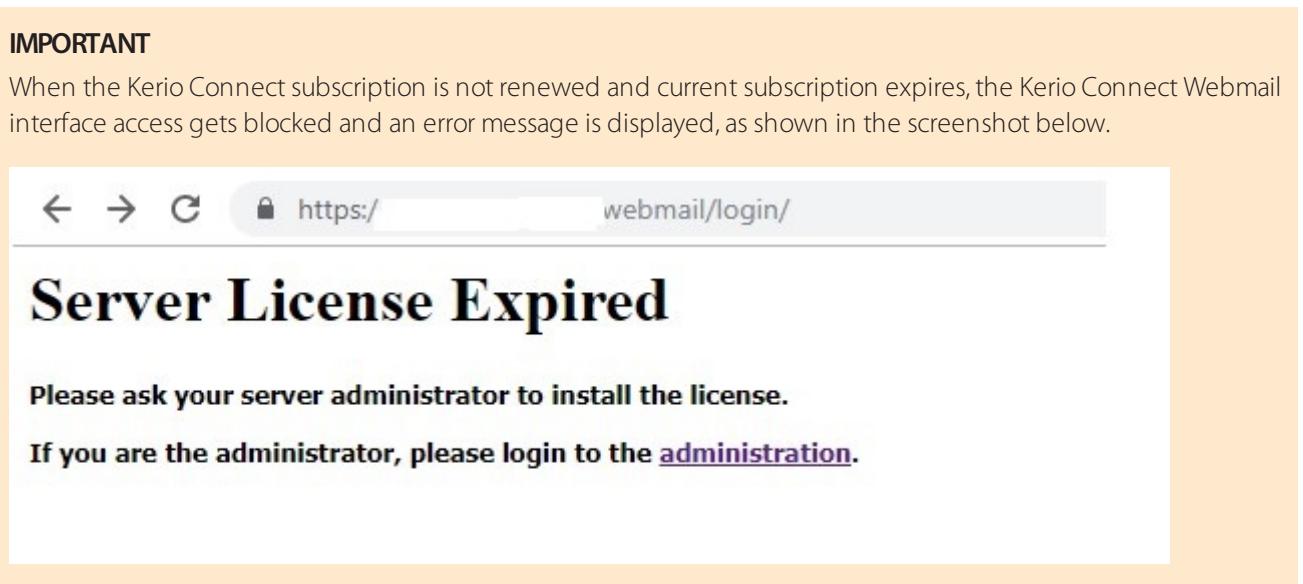
Until you register Kerio Connect, it behaves as an unregistered trial version and have the following limitations:

- » 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 while performing the initial configuration or using the administration interface.

IMPORTANT

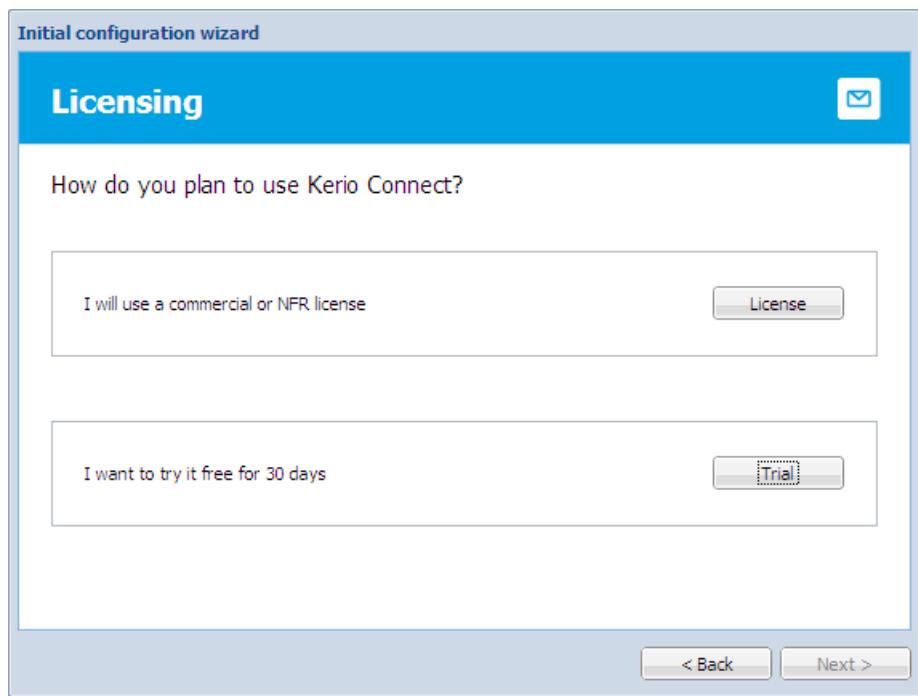
When the Kerio Connect subscription is not renewed and current subscription expires, the Kerio Connect Webmail interface access gets blocked and an error message is displayed, as shown in the screenshot below.



A screenshot of a web browser window. The address bar shows 'https://webmail/login/'. The main content area displays a large, bold, black text 'Server License Expired'. Below this, there are two lines of smaller text: 'Please ask your server administrator to install the license.' and 'If you are the administrator, please login to the [administration](#)'.

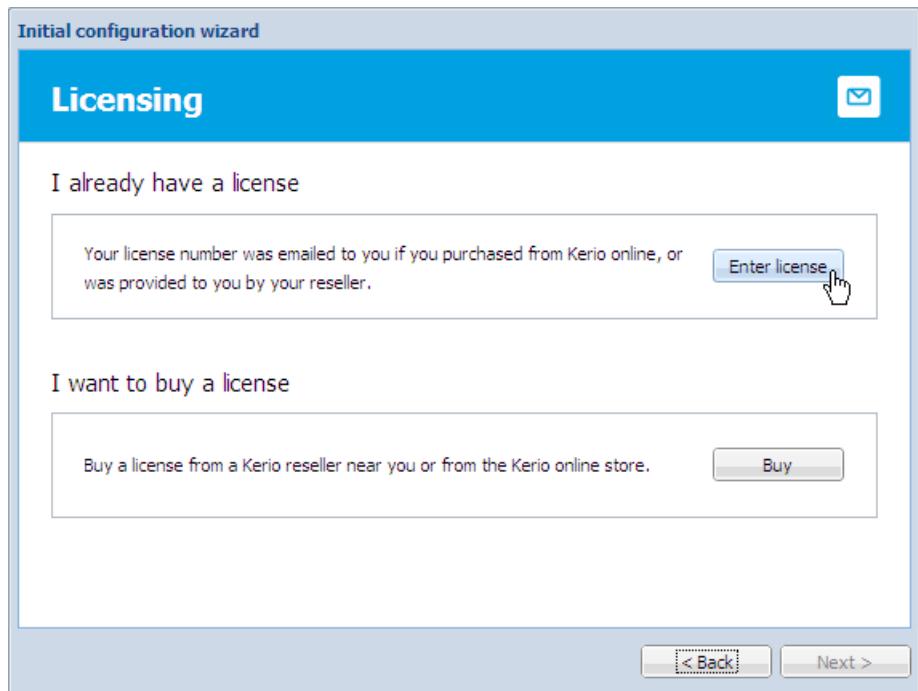
Registering Kerio Connect from the initial configuration wizard

You can register Kerio Connect while running the initial configuration wizard. For more information, refer to [Performing initial configuration in Kerio Connect](#) (page 15).

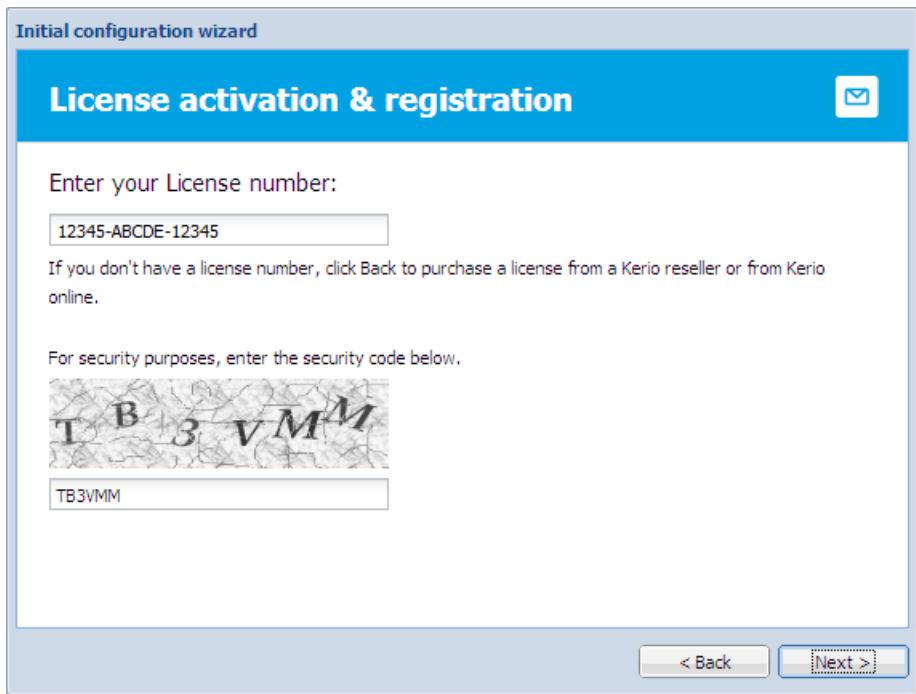


Registering a full version

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.



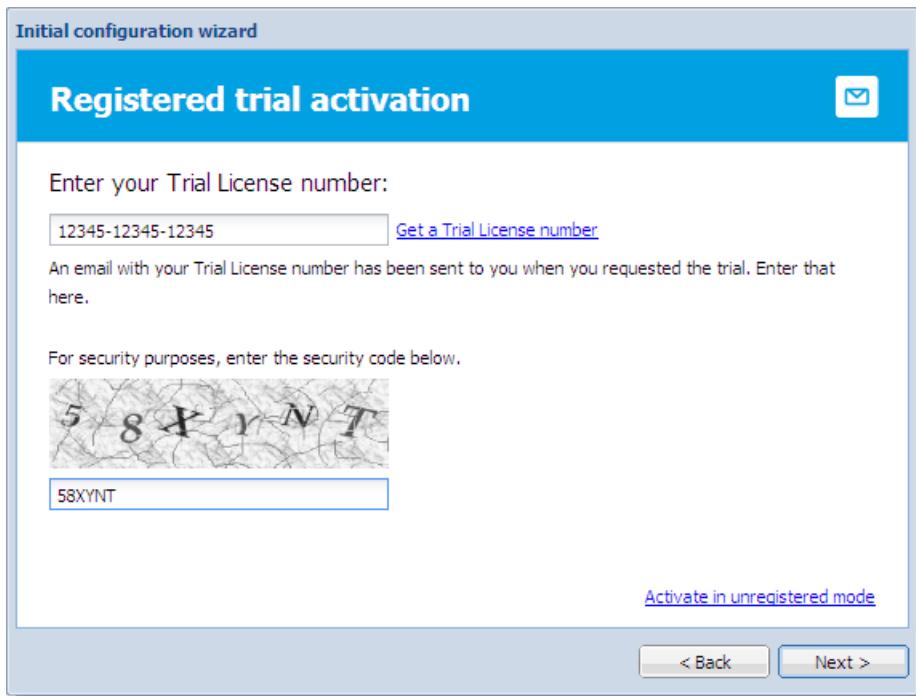
3. Key in your license number and security code, and click **Next**.



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

Registering a trial version

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



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

Using an unregistered trial version

If you want to use Kerio Connect in the unregistered mode, click **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.

NOTE

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

The screenshot shows the Kerio Connect Dashboard with the title 'Dashboard' at the top left. At the top right, there is a search bar with the placeholder 'Where is ...' and a magnifying glass icon, followed by the text 'Administrator'. Below the header is a main content area titled 'License Details'. Inside this area, there is a table of information:

Trial number:	Unregistered trial version
Product expiration date:	2016-07-07
Number of active mailboxes:	0 (1 created)
Kerio Antivirus:	Yes
Exchange ActiveSync® extensions:	Yes
Kerio Anti-spam:	No

Below the table, a pink callout box contains the text: 'Register your copy to get antivirus updates and Exchange ActiveSync®.' and a link 'Become a registered trial user...'. At the bottom of the 'License Details' box, there are two links: 'Install license...' and 'Register product with a purchased license number...'. At the very bottom of the dashboard, there are three buttons: 'Add Tile', 'Report Problem...', and 'Suggest Idea...', followed by the copyright notice 'Kerio Technologies s.r.o. All rights reserved. Legal Notices'.

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

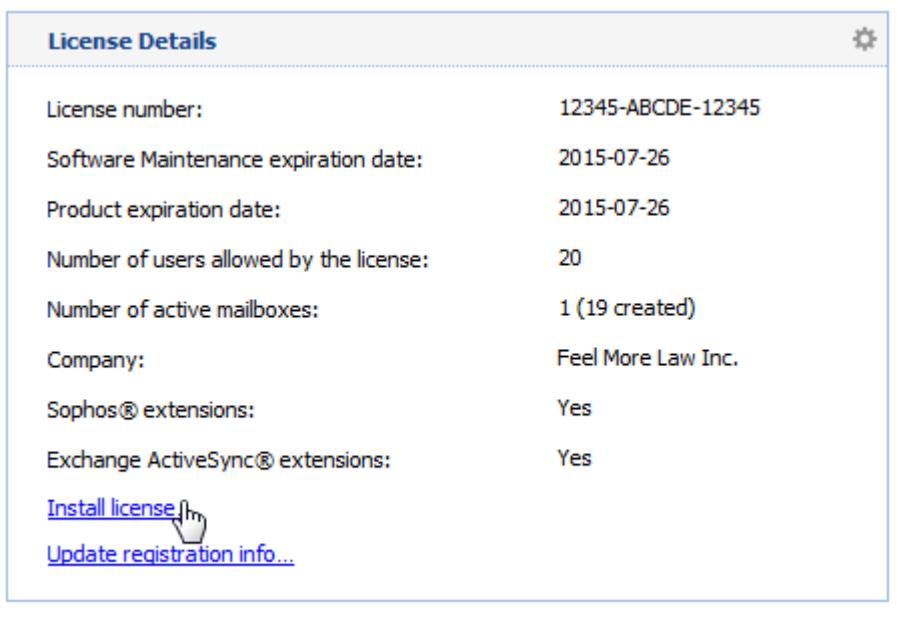
If you previously registered a trial version of Kerio Connect and have now purchased the full version, the license file gets automatically imported to your product within 24 hours of your purchase. The trial ID becomes your license number.

If you haven't registered your trial version:

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

[Install license](#) 

[Update registration info...](#)

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/

2.4.8 How do I apply renewals or add-ons to my Kerio product?

When you purchase renewals or add-ons for a Kerio Product, License changes are applied automatically by the product within 24 hours. If required, you can also force an immediate update from the administration dashboard using the **update registration info** link in the **License Details** tile.

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

Use these links to find instructions for your operating systems:

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

Microsoft Windows

The procedure of switching from a 32-bit Kerio Connect version to a 64-bit version differ on both [64-bit Windows](#) and [32-bit Windows](#). systems. In case of latter, you require a new 64-bit windows machine to run 64-bit Kerio application.

NOTE

It is recommended to keep a [full backup](#) of your current installation before proceeding.

64-bit Windows

If you have a 32-bit version of Kerio Connect installed on a 64-bit Windows system, and you want to run Kerio Connect in

64-bit, you can either:

- » Upgrade to a newer 64-bit version of Kerio Connect
- » Reinstall your same Kerio Connect version in 64-bit

Upgrade to the latest 64-bit version of Kerio Connect

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

NOTE

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

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.

2. Move the **Kerio/MailServer** directory from **Program Files (x86)** folder to **Program Files** folder.



3. Locate and open the **mailserver.cfg** file from the moved directory and change all paths from **C:\Program Files (x86)** to **C:\Program Files**.

4. Now, install a new Kerio Connect 64-bit version.

NOTE

During the process, do not change the destination folder and select the **Keep current configuration** option.

Keep current configuration

The old configuration files will be kept.

Replace old configuration

Old configuration files will be replaced by the new configuration files.

Reinstall your same Kerio Connect version in 64-bit

1. Uninstall the Kerio Connect 32-bit version.

NOTE

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

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.

2. Move the **Kerio/MailServer** directory from **Program Files (x86)** folder to **Program Files** folder (the default installation folder for 64-bit programs).

OS (C:) ▶ Program Files (x86) ▶ Kerio ▶ MailServer



OS (C:) ▶ Program Files ▶ Kerio ▶ MailServer ▶

3. Locate and open the **mailserver.cfg** file from the moved directory and change all paths from **C:\Program Files (x86)** to **C:\Program Files**.

4. Install your same Kerio Connect version in 64-bit.

NOTE

During the process, do not change the destination folder and select the **Keep current configuration** option.

Keep current configuration

The old configuration files will be kept.

Replace old configuration

Old configuration files will be replaced by the new configuration files.

32-bit Windows

If you have a 32-bit version of Kerio Connect installed on a 32-bit Windows system, and you want to run Kerio Connect in 64-bit on a 64-bit Windows machine, you need to:

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

NOTE

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

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.

2. Move the **Kerio/MailServer** directory from the **Program Files** folder on your 32-bit Windows machine to **Program Files** folder on your 64-bit system.

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

NOTE

During the process, do not change the destination folder and select the **Keep current configuration** option.

Keep current configuration

The old configuration files will be kept.

Replace old configuration

Old configuration files will be replaced by the new configuration files.

Linux

The procedure of switching from a 32-bit Kerio Connect version to a 64-bit version differ on both [32-bit Linux](#) and [64-bit Linux](#) systems. In case of latter, you require a new 64-bit linux machine to run 64-bit Kerio application.

NOTE

It is recommended to keep a [full backup](#) of your current installation before proceeding.

64-bit Linux

1. Uninstall your current 32-bit Kerio Connect version.

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

RPM — `rpm -e <package name>`

2. Install the 64-bit Kerio Connect version.

32-bit Linux

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

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

RPM — `rpm -e <package name>`

2. Move files from the **opt/kerio/mailserver** directory on your 32-bit Linux machine to the same directory on the 64-bit Linux machine.

3. Install and start running the 64-bit Kerio Connect application on the 64-bit Linux machine.

Virtual appliances

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

NOTE

It is recommended to keep a [full backup](#) of your current installation 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.
 - 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 running the 64-bit Kerio Connect appliance.

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

We recommend to perform a [full backup](#) of your current Kerio Connect installation before proceeding

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

1. Uninstall the 64-bit Kerio Connect version.

IMPORTANT

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

2. Move the folder MailServer from C:\Program Files\Kerio\MailServer\ to C:\Program Files (x86)\Kerio\MailServer\.
3. Locate and open file mailserver.cfg from the moved folder and change all paths from C:\Program Files\ to C:\Program Files (x86)\.
4. Install the 32-bit Kerio Connect application.

NOTE

During the process, do not change the destination folder and select the **Keep current configuration** option.

2.4.11 Uninstalling Kerio Connect

Windows operating system

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

IMPORTANT

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

Mac OS X operating system

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

IMPORTANT

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

Linux operating system — RPM

You can uninstall Kerio Connect using the following command:

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

IMPORTANT

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

Linux operating system — DEB

You can uninstall Kerio Connect using the following command:

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

IMPORTANT

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

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

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

2.5 Upgrade

Learn how to upgrade Kerio Connect to the latest version while retaining all settings.

2.5.1 Upgrading to the latest version	37
2.5.2 Upgrading from versions older than Kerio Connect 8.0.0	40

2.5.1 Upgrading to the latest version

Learn how to upgrade to the latest version of Kerio Connect. You are eligible for upgrade to the latest version from version 8.0.0 onwards.

Prerequisites and important notes

- » We recommend to take a full backup of Kerio Connect. For more information, refer to [Configuring backup in Kerio Connect](#) (page 165).
- » Check that the Software Maintenance is valid for the upgrade. Your Software Maintenance expiration date can be found on the splash screen of your Kerio Connect Administration console. You are entitled to upgrade to the latest version that gets released during your Software Maintenance period, even post its expiration.
- » If you are manually upgrading to Kerio Connect 9.2.7 and above on Linux then you must first install the cryptsetup package before the upgrade. If you are performing the upgrade using the administration the cryptsetup package is installed automatically.
- » Check that the server meets the latest system and hardware requirements. For more information, refer to [Kerio Connect Multi-Server System requirements and Prerequisites](#) (page 46).
- » Kerio Connect requires restart during upgrade. Perform the upgrade when there is no traffic on the server or when it is least impacting on the business operation.

Configure server update check and notifications

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.

The screenshot shows the Kerio Connect Dashboard interface. At the top, there is a green notification bar with the text "Kerio Connect 9.0.2 is available. Go to [Software Updates](#) to install the new version." Below this, there are two sections: "System" and "License Details".

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...](#)

At the bottom of the dashboard, there are buttons for "Add Tile", "Technical Support...", "Suggest Idea...", "Kerio Technologies s.r.o.", "All rights reserved.", and "Legal Notices".

The screenshot shows the "Server updates" section. It displays the last update check time ("Last update check performed before: 12 hours, 30 minutes") and two checkboxes: "Automatically check for new versions" (checked) and "Check also for beta versions". A "Check Now" button is also present. A notification message indicates "A new version is available for download: [Kerio Connect 9.0.2](#)" with an "Upgrade..." button.

You can also 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

Kerio Connect supports both auto and manual upgrading. If you're using Kerio Connect 9 and above, you can automatically upgrade your version from the **Configuration > Advanced Options > Software Updates** tab on the Administration interface.

To manually upgrade:

1. Visit the Kerio download page to download the latest version: <http://www.kerio.com/connect/download>.
2. Depending on the platform that runs Kerio Connect, follow the instructions below:

Microsoft Windows

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

Mac OS X

- a. To upgrade Kerio Connect on Mac OS X, download and run the installation package.
- b. 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 this command: # dpkg -i <installation_file_name.deb>

Kerio Connect VMware Virtual Appliance

For more information, refer to [Virtual Appliance and Linux](#) (page 93).

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 problem occurs during the upgrade, consult the [Debug log](#) — right-click the Debug log section and select **Messages > Update Checker Activity**.

2.5.2 Upgrading from versions older than Kerio Connect 8.0.0

Learn how to upgrade when your current Kerio Connect setup is older than version 8.0. In case you're already on version 8.0 or above, please refer to [Upgrading Kerio Connect](#) topic.

IMPORTANT

All changes, improvements and prerequisites for Kerio Connect are cumulative. So, if you want to skip some versions, it is highly recommended to go through this topic to make sure you meet all prerequisites of the versions being skipped.

Prerequisites and important notes

- » We recommend to take a full backup of Kerio Connect. For more information, refer to [Configuring backup in Kerio Connect](#) (page 165).
- » Check that the Software Maintenance is valid for the upgrade. Your Software Maintenance expiration date can be found on the splash screen of your Kerio Connect Administration console. You are entitled to upgrade to the latest version that gets released during your Software Maintenance period, even post its expiration.
- » Check that the server meets the latest system and hardware requirements. For more information, refer to [Kerio Connect Multi-Server System requirements and Prerequisites](#) (page 46).
- » Kerio Connect requires restart during upgrade. Perform the upgrade when there is no traffic on the server or when it is least impacting on the business operation.
- » You may also want to look at version specific notes and prerequisites before upgrading. For more information, refer to [Important notes when upgrading to specific older versions](#) (page 42).
- » When upgrading a version that is older than version 7.0.0, there are a number of milestone versions that must be installed before you can proceed with upgrading to the latest. The list below shows these milestone versions, and the order in which you must install them. You need to determine and install the version higher than the one you are currently running and so on, till the last milestone version on-the list is installed. These versions are required because of changes in the installation process, so it is not possible to skip them. After you install the last milestone version on the list, you can then directly upgrade to v7.x.x and then to v8.x.x. For more information, refer to [Upgrading to the latest version](#) (page 37).

Milestone versions

1. Kerio MailServer 5.1
2. Kerio MailServer 5.5

3. Kerio MailServer 5.7.10

4. Kerio MailServer 6.0.0

5. Kerio MailServer 6.0.10

6. Kerio MailServer 6.5.2

7. Kerio MailServer 6.7.3 Patch 1

These versions are available from our archive: <http://download.kerio.com/archive/>.

Upgrading Kerio Connect

1. Visit the Kerio download page to find and download the relevant milestone version one by one: <http://www.kerio.com/connect/download>.

2. Depending on your platform follow the instructions below and repeat for each milestone version:

Windows

a. Double-click the installer.

b. Select your language (e.g. English).

c. Select **Modify** and click **Next**.

d. Leave all of the components checked and click **Next**.

e. The installation should be completed and you can click **Finish**.

OS X

a. Double-click the ***.dmg** file.

b. Double-click the installer.

c. Read the license agreement and click **Continue**.

d. Click **Agree** to continue the installation.

e. Select **Easy Install** and then click **Install**.

f. Click **Quit** once the installation gets completed.

RHEL or CentOS

Use the following commands:

```
sudo /sbin/service kerio-connect stop
```

```
sudo rpm -Uvh package_name.rpm
```

```
sudo /sbin/service kerio-connect start
```

These commands are generic and **package_name.rpm** refers to the actual package file name that you download. A real example of the second command would be: `sudo rpm -Uvh kerio-connect-7.2.3-4971-linux.rpm`.

SUSE

Use the following commands:

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

```
sudo rpm -Uvh package_name.rpm
```

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

These commands are generic and **package_name.rpm** refers to the actual package file name that you download. A real example of the second command would be:`sudo rpm -Uvh kerio-connect-7.2.3-4971-linu.x.rpm`.

Debian or Ubuntu

Run the following commands:

```
sudo /etc/init.d/kerio-connect stop  
sudo dpkg -i package_name.deb
```

These Linux commands are valid for Kerio Connect 7.0 and newer. Installing the upgrade will leave your current settings intact.

Important notes when upgrading to specific older versions

When upgrading from versions older than 8.0.0, the appropriate milestone versions must be installed one-by-one for upgrading to the latest version. For more information, refer to [Upgrading from versions older than Kerio Connect 8.0.0](#) (page 40). Some of these versions have their specific notes and prerequisites that you must know before upgrading.

Kerio Connect 7.4

- » The Bayes database gets upgraded to a different format of database at the time of the first Kerio Connect server start-up.
- » The old database remains stored in the backup folder for instances where you may have to downgrade it. In case of downgrade to older version of Kerio Connect, Kerio Outlook Connector needs to be downgraded manually.

Kerio Connect 7.3

- » If you change platform from PowerPC Mac to Mac Intel, the SpamAssassin database is erased and starts from scratch.
- » If Out Of Office settings does not work in a Microsoft Entourage account, the user have to reconfigure the account using the new configuration tool, the Account Assistant.
- » If you are using an offline version of Kerio Outlook Connector, the local cache gets converted upon the first start of Outlook. This may take up to several minutes, depending on the size of the local cache and hardware performance (expected upgrade speed is 1GB per 5 minutes). It is not possible to use Kerio Outlook Connector (Offline Edition) during the local cache conversion. For more information go to http://go.gfi.com/?pageid=connect_help#cshid=187
- » The Kerio Updater Service is mandatory so the Kerio Outlook Connector won't be upgraded without this service. For more information go to http://go.gfi.com/?pageid=connect_help#cshid=188

Kerio Connect 7.2

- » Kerio Connect 7.2 will perform various updates in your data store. Depending on the data store size and hardware configuration these updates may affect the server performance in the first 24 hours after the server upgrade.
- » Users of Microsoft Entourage may experience troubles while moving folders.
- » Apple iCal users are advised to restart their clients after server upgrade.
- » All users must reconfigure their profiles in Microsoft Outlook 2011 for Mac after upgrading from any previous beta version of Kerio Connect 7.2.
- » If you are using an offline version of Kerio Outlook Connector, the local cache gets converted upon the first start of Outlook after the upgrade. This may take up to several minutes, depending on the size of the local cache and hardware performance (expected upgrade speed is 1GB per 5 minutes). It is not possible to use Kerio Outlook Connector (Offline

Edition) during the local cache conversion. For more information go to http://go.gfi.com/?pageid=connect_help#c-shid=187.

- » From version 7.2.0 the mechanism for automatic upgrade of Kerio Outlook Connector (Offline Edition) has been changed. The upgrade process is newly performed by the new Kerio Updater Service. The service is installed within the first full installation of Kerio Outlook Connector (Offline Edition) 7.2.0 and higher. Installation of the service requires administration privileges. To ease the transition for users without administration privileges, the old upgrade mechanism will continue working through all 7.2.X versions. During this transition period, users and/or administrators have to perform full re-installation with administration privileges. For more information go to http://go.gfi.com/?pageid=connect_help#cshid=188.
- » Once you have upgraded to a version newer than Kerio Connect 7.1.4 Patch 1 you can only roll back to Kerio Connect 7.1.4 Patch 1. This is due to changes that have been implemented in the Kerio Connect software.

Kerio Connect 7.1

- » Kerio Connect will re-create all CalDAV and CardDAV databases upon the first start. It can cause temporary inaccessibility of calendar and contact items in CalDAV and CardDAV clients.
- » The integrated McAfee antivirus is replaced by Sophos antivirus. It is not necessary to change Kerio Connect license immediately. The current license with McAfee antivirus will work in the new Kerio Connect with Sophos.
- » If the license with McAfee is updated for any reason, the license is converted to the new one with Sophos antivirus. This new license cannot be used in old Kerio Connect with McAfee antivirus. This means that it is not possible to downgrade Kerio Connect after renewal.

Kerio Connect 7.0

- » On completion, the Kerio Connect server rebuilds the Indexes for all accounts within the message store directory.
- » Users are able to access their account, but may notice some slow response times while this action is completed.

Kerio MailServer 6.2

- » Since, in version 6.2 it has been required to use the exactly same version of Kerio MailServer and Kerio Outlook Connector, the upgrade to a new version of Kerio Outlook Connector is offered automatically during the first start of Microsoft Outlook after Kerio MailServer upgrade.
- » If the automatic upgrade failed for some reason, it would be necessary to upgrade Kerio Outlook Connector manually. The Kerio Outlook Connector is available from our archive, <http://download.kerio.com/archive>.

Kerio MailServer 6.1

- » The most important step in this update is to convert the Kerio Outlook Connector user settings to a new database. This is a time consuming action and can take few hours according to the Kerio MailServer message store size.
- » It is recommended to perform this upgrade at a time when it will not affect users as Kerio MailServer can be slow during this time due to a heavy load.

Kerio MailServer 6.0.10

- » Once Kerio MailServer gets upgraded to version 6.0.10, it is necessary to manually update Kerio Outlook Connector.

Kerio MailServer 5.x to Kerio MailServer 6.x

- » When upgrading from Kerio MailServer 5.7.0 to Kerio MailServer 6.0.0, according to the upgrade process you may notice a problem with a version check. This problem happens occasionally and is caused by a missing version registry key in Windows. This problem can appear only on Windows platform and can be fixed using this [registry key file](#) (a zip archive).

2.6 Kerio Connect Multi-Server

Kerio Connect Multi-Server is a distributed architecture solution designed for easy scalability.

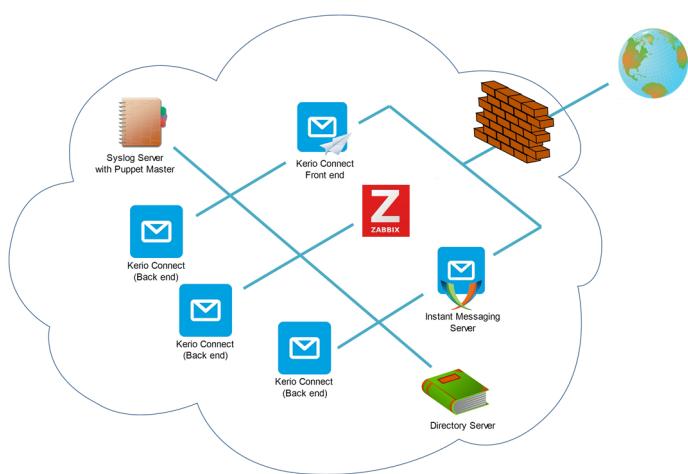
NOTE

This information is designed for Kerio Connect Multi-Server 9.

All users access their Kerio Connect account through a single server address, regardless of their home server. The connection is directed to the user's server automatically.

Use Kerio Connect Multi-Server in any of the following scenarios:

- » Large on-premise installations to reduce the load and improve the Kerio Connect performance.
- » Distributed server environments to use a single domain and a single URL to access the mailboxes.
- » Kerio Cloud Solution Partner hosting your own Kerio Connect Cloud environment to distribute users across multiple servers.



2.6.1 Current version limitations

All architectural components of Kerio Connect Multi-Server are available and ready to use. However, note the following functional limitations:

- » Users can see shared folders across all servers only in [Kerio Connect Client](#) and with [Kerio Outlook Connector \(Offline Edition\)](#). To enable sharing, set the `EnabledFolderSharing` variable of the `MultiServer` table in the configuration file to 1:

```
<variable name="EnabledFolderSharing">1</variable>
```

- » Users cannot share public folders across the servers.
- » The [Greylisting](#) service is not available.
- » IP address groups in [user access policies](#) are available only for HTTP/HTTPS.

2.6.2 Configuring Kerio Connect Multi-Server

Go through the links below to learn how to install and configure Kerio Connect Multi-Server:

- » [Installing Kerio Connect Multi-Server](#)
- » [Licensing Kerio Connect Multi-Server](#)
- » [Upgrading and downgrading Kerio Connect in Kerio Connect Multi-Server](#)
- » [Securing Kerio Connect Multi-Server](#)
- » [Migrating from current installations to Kerio Connect Multi-Server](#)
- » [Managing Kerio Connect Multi-Server](#)
- » [Creating users in Kerio Connect Multi-Server](#)
- » [Monitoring Kerio Connect Multi-Server with the Zabbix server](#)
- » [Troubleshooting Kerio Connect Multi-Server](#)

2.6.3 Installing Kerio Connect Multi-Server

NOTE

This information relates to Kerio Connect Multi-Server 9

Kerio Connect Multi-Server is available as a VMware virtual appliance with 64-bit Debian Linux. You can download using this [link](#).

The installation file is the same for all server roles. However, you must install the individual servers in the specified order:

Installation Order	Server Name	Description
1	Puppet master	Puppet master is responsible for configuring all other servers in Kerio Connect Multi-Server and server upgrades. The puppet master also contains a Syslog server which stores all logs from the Kerio Connect servers.
2	Directory server	The directory server (OpenLDAP) is the central storage location for user and group information in the multi-server deployment. All back-end servers are connected to this directory.
3	Back-end servers	Back-end servers represent individual installations of Kerio Connect. These servers work as home servers for individual users and store users' mailboxes. You can install two or more back-end servers, and you can install them now or at any later time.
4	Front-end server	The front-end server is a proxy server that routes connections to individual back-end servers with user accounts and hosts a session server.
5	Instant messaging server	(Optional). The instant messaging server also has Kerio Connect installed. All XMPP communication is routed directly to this server.
6	Zabbix monitoring server	(Optional). Zabbix monitors all servers in Kerio Connect Multi-Server. For more information, refer to Monitoring Kerio Connect Multi-Server with the Zabbix server (page 60).

NOTE

If you are upgrading from a current installation of Kerio Connect, read [Migrating from current installations to Kerio Connect Multi-Server](#) before you start the installation.

Use these links to understand the Kerio Connect Multi-Server installation and configuration process:

- » [Kerio Connect Multi-Server System requirements and Prerequisites](#)
- » [Installing the puppet master server](#)
- » [Installing the directory server](#)
- » [Installing the back-end servers](#)
- » [Installing the front-end server](#)
- » [Installing the instant messaging server](#)
- » [Installing the Zabbix server](#)

Kerio Connect Multi-Server System requirements and Prerequisites

This topic outlines the system requirements and prerequisites for installing Kerio Connect Multi-Server.

System Requirements

For better performance it is recommended to run the listed servers on multiple physical servers running VMware vSphere Hypervisor. See the Kerio Connect [Tech Specs](#) page for the supported VMware product versions.

These are the minimum system requirements for the virtual appliances:

Virtual Appliance	CPU	RAM	Disk space	LAN
Puppet master	2 CPU cores (Intel Xeon E5 recommended)	4 GB	100 GB virtual disk	1 Gbit
Directory server	2 CPU cores (Intel Xeon E5 recommended)	4 GB	Default virtual machine disk space	1 Gbit
Back-end server (200 or more users)	2 quad-core CPUs (Intel Xeon E5 recommended)	16 GB	7.2-15K RPM, SAS-SATA, 3.5", 1+ TB, RAID10 recommended 1000 IOPS read / 800 IOPS write	1 Gbit
Instant messaging server	2 CPU cores (Intel Xeon E5 recommended)	4 GB	Default virtual machine disk space	1 Gbit
Front-end server	1 quad-core CPU (Intel Xeon E5 recommended)	8 GB	Default virtual machine disk space	1 Gbit (10 Gbit recommended)
Zabbix server	1 CPU	1 GB	Default virtual machine disk space	1 Gbit

Prerequisites

Before you begin Kerio Connect Multi-Server installation, it is recommended to have the following ready:

- » Internet access
- » Correct time set on the hypervisor
- » DHCP server
- » DNS server.

Manual configuration when the DNS server is not available

If you install all servers and don't have a DNS server available in your network, you must configure the proper domain names manually on all servers except the puppet master.

On each server:

1. Run the following commands:

```
hostname -f
```

```
hostname
```

2. Open the file /etc/hosts.

3. Add the following lines to the file, and save it:

```
127.0.1.1 <result of `hostname -f`> <result of `hostname`><puppet master IP address> <fully qualified name of puppet master> <puppet master hostname>
```

4. Run the following command to finish the configuration:

```
puppet agent -t
```

Installing the puppet master server

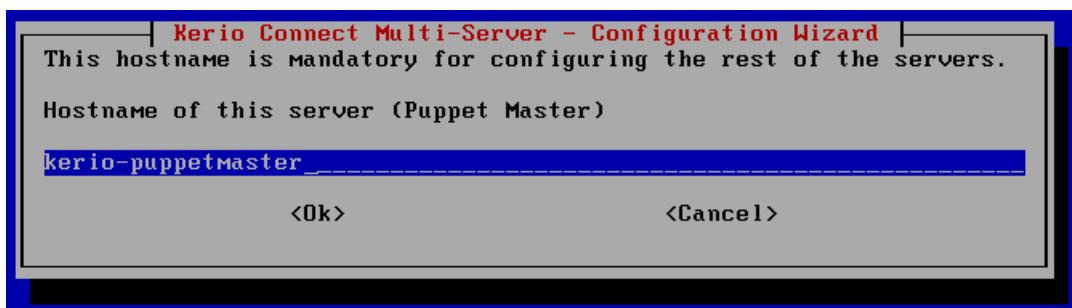
Puppet master is responsible for configuring all other servers in Kerio Connect Multi-Server and server upgrades. The puppet master also contains a Syslog server which stores all logs from the Kerio Connect servers.

To install:

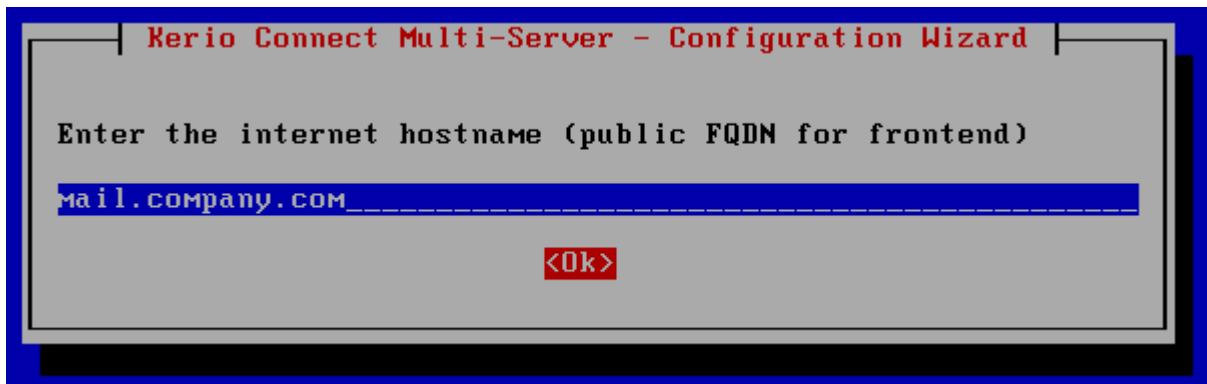
1. Run the Kerio Connect Multi-Server virtual appliance.
2. Read the **Configuration Wizard** introductory page and select **OK**
3. Select **puppetmaster** as the server's role, and select **OK**



4. Type the hostname of the puppet master server, and select **OK**. Note that you need this hostname when installing the other servers.



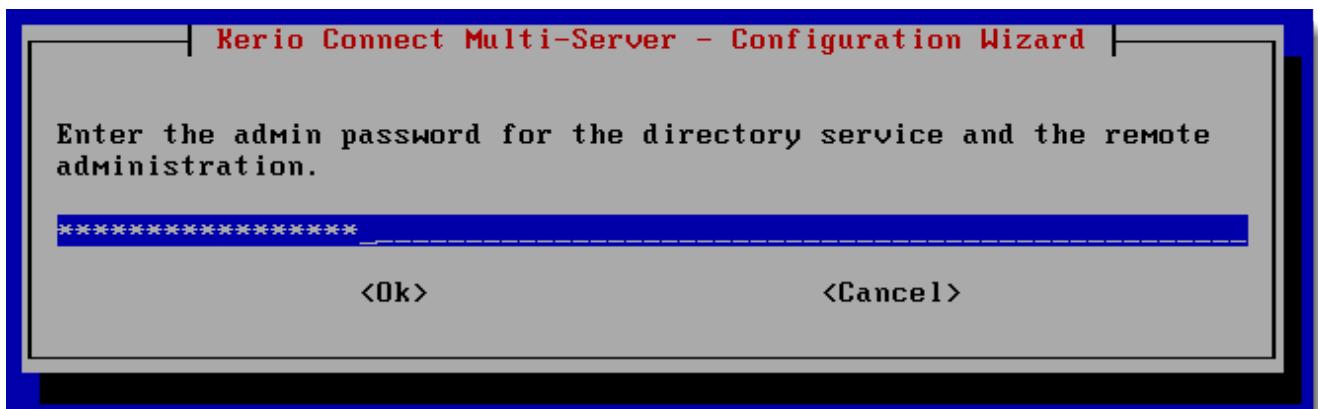
5. Type the Internet hostname of your mailserver, and select **OK**. This may be different from your domain's DNS name.



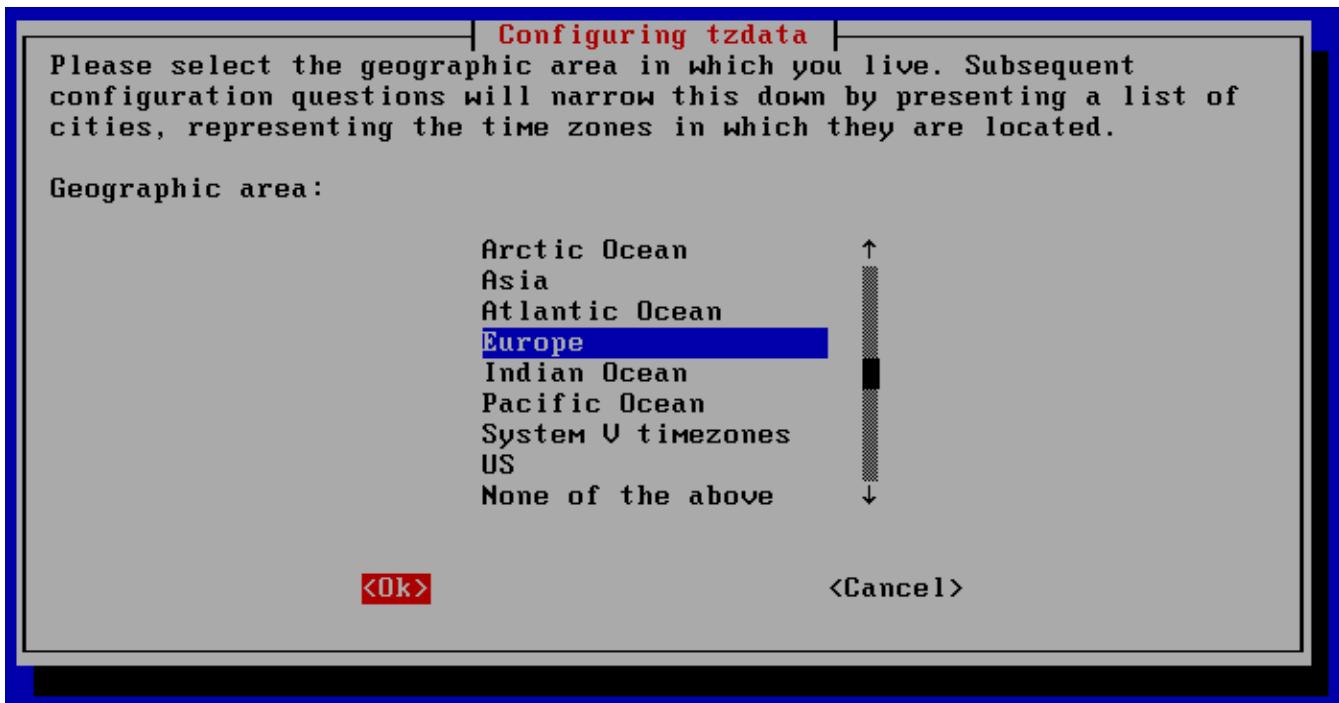
6. Type the DNS name of your domain, and select **OK**. This may be different from the Internet hostname of your mailserver.



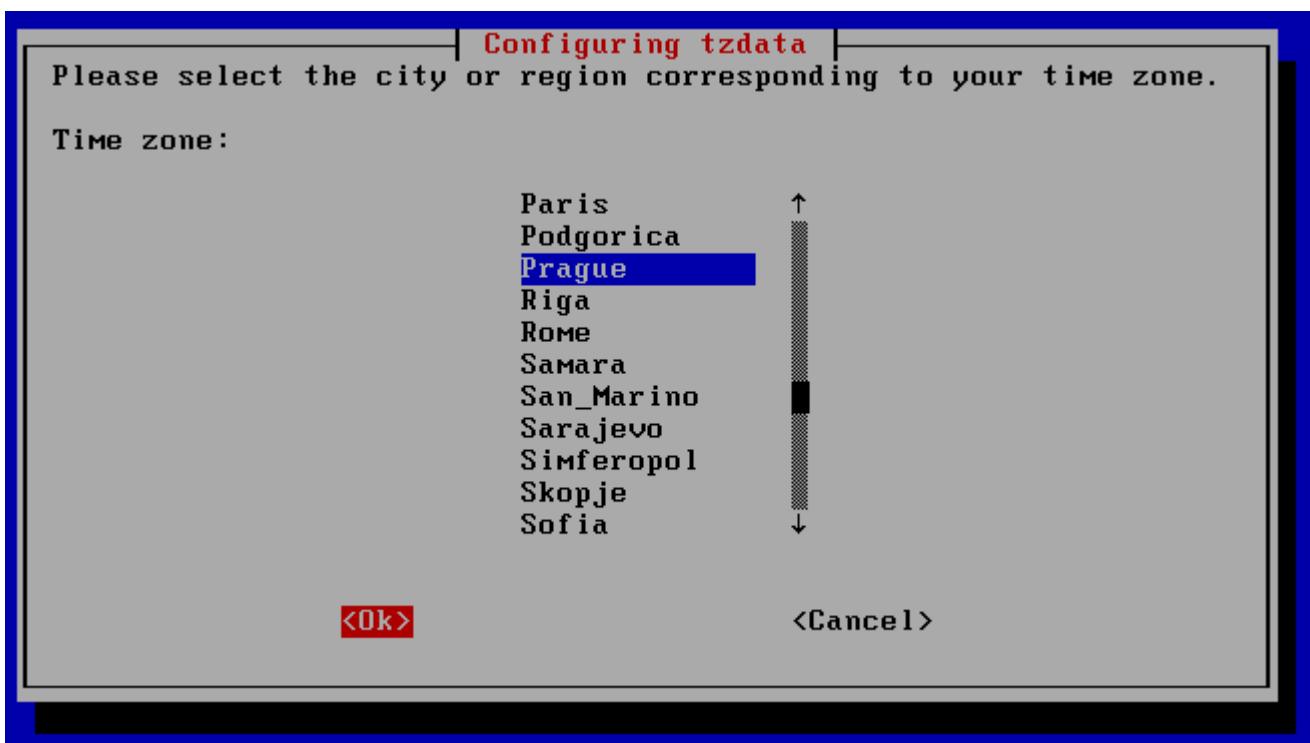
7. Type and confirm the administrator password, and select **OK**.



8. To set a correct time zone on the sever, select the your geographic area and select **OK**.



9. Select your city and select **OK**



To log in to the appliance after installation, use `root/kerio`.

If you have multiple servers and don't have a DNS server available in your network, you must configure the proper domain names manually on all servers except the puppet master.

Installing the directory server

The directory server (OpenLDAP) is the central storage location for user and group information in the multi-server deployment. All back-end servers are connected to this directory.

To install:

1. Run the Kerio Connect Multi-Server virtual appliance.
2. Read the **Configuration Wizard** introductory page and select **OK**
3. Select **directory**, and then select **OK**
4. Type the hostname of the puppet master server.
5. Type the hostname for the directory server and select **OK**

To log in to the appliance after installation, use `root/kerio`.

Installing the back-end servers

Back-end servers represent individual installations of Kerio Connect. These servers work as home servers for individual users and store users' mailboxes. You can install two or more back-end servers, and you can install them now or at any later time.

To install:

All back-end servers must have the same primary domain. If you install any back-end server later, they will be added to the distributed multi-server automatically.

The first back-end server installed is a **master server**.

1. Run the Kerio Connect Multi-Server virtual appliance.
2. Read the **Configuration Wizard** introductory page and select **OK**
3. Select **backend**, and select **OK**
4. Type the `hostname` of the puppet master server.
5. Type the `hostname` for the back-end server and select **OK**

To log in to the appliance after installation, use `root/kerio`.

Installing the front-end server

The front-end server is a proxy server that routes connections to individual back-end servers with user accounts and hosts a session server.

To install:

1. Run the Kerio Connect Multi-Server virtual appliance.
2. Read the **Configuration Wizard** introductory page and select **OK**
3. Select **frontend**, and select **OK**
4. Type the `hostname` of the puppet master server.
5. Type the `hostname` for the front-end server, and select **OK**

To log in to the appliance after installation, use `root/kerio`.

Installing the instant messaging server

The instant messaging server is an optional server, which also has Kerio Connect installed. All XMPP communication is routed directly to this server.

To install this server:

1. Run the Kerio Connect Multi-Server virtual appliance.
2. Read the **Configuration Wizard** introductory page and select **OK**
3. Select **instant-messaging**, and select **OK**
4. Type the hostname of the puppet master server.
5. Type the hostname for the instant messaging server, and select **OK**

To log in to the appliance after installation, use `root/kerio`.

Installing the Zabbix server

Zabbix monitors all servers in Kerio Connect Multi-Server.

To install Zabbix server:

1. Run the Kerio Connect Multi-Server virtual appliance.
2. Read the **Configuration Wizard** introductory page and select **OK**
3. Select **zabbix**, and select **OK**
4. Key in the `hostname` of the puppet master server.
5. Key in the `hostname` for the zabbix server, and select **OK**

To log in to the appliance after installation, use `root/kerio`.

For more information, refer to [Monitoring Kerio Connect Multi-Server with the Zabbix server](#) (page 60).

2.6.4 Upgrading and downgrading Kerio Connect Multi-Server

NOTE

This information is designed for Kerio Connect Multi-Server 9

You can use the puppet master server to upgrade or downgrade the servers in Kerio Connect Multi-Server.

Kerio Connect Multi-Server can install Kerio Connect updates automatically. You can just download the new version on the puppet master and it is automatically installed on the other servers. If you want to disable automatic updates, see section [Disabling automatic updates](#) below.

Disabling automatic updates

1. On the puppet master server, open the `site.pp` file for editing. The default location is `/etc/puppet/manifests/site.pp`
2. Add `ensure => present` to the role definitions for all server roles.

```
if $::system_role == 'backend' {
    class {'kerio_cloud::backend':
        ensure => present,
    }
}

if $::system_role == 'instant-messaging' {
    class {'kerio_cloud::backend':
        im_enabled => true,
```

```

        ensure      => present,
    }

}

if $::system_role == 'frontend' {
    class { 'kerio_cloud::proxy':
        ensure      => present,
    }
}

if $::system_role == 'directory' {
    class { 'kerio_cloud::directory':
        ensure      => present,
    }
}

```

3. Save the file.

NOTE

To enable the automatic updates again, add `ensure => latest` to the role definitions for all server roles.

Upgrading the front-end proxy server

1. Verify you have automatic updates enabled.
2. On the puppet master server, download the 64-bit Debian installation package of the front-end proxy server.

```
cd /var/packages/pool/non-free/ wget <package URL>
```

For example: `wget <http://cdn.kerio.com/dwn/connect/connect-8.5.1-4597/kerio-connect-proxy-8.5.1-4597-linux-64bit.deb>`

3. Publish the package in the repository.

```
update-archive
```

The front-end proxy server is upgraded within approximately 30 minutes.

Upgrading Kerio Connect Multi-Server

To upgrade to a newer version of Kerio Connect:

1. On the puppet master server, download the 64-bit Debian installation package of Kerio Connect.

```
cd /var/packages/pool/non-free/ wget <package URL>
```

For example, `wget <http://cdn.kerio.com/dwn/connect/connect-8.5.1-4597/kerio-connect-8.5.1-4597-linux-amd64.deb>`

2. Publish the package in the repository.

```
update-archive
```

All Kerio Connect servers are upgraded within approximately 30 minutes.

Downgrading Kerio Connect Multi-Server

To downgrade to an older version of Kerio Connect, you must disable the automatic downloads on the puppet master first and then install the version you need on other servers.

On the puppet master:

1. [Disable the automatic updates](#).
2. Place the 64-bit Debian installation package of the desired version of Kerio Connect to the `/var/packages/pool/non-free/` folder.

On each back-end, front-end, instant messaging, and directory server:

1. Log in as the `root` user.
2. Update the package definitions.

```
apt-get update
```

3. List the available version of Kerio Connect.

```
apt-cache showpkg kerio-connect
```

4. Run the `install` command with the version you want to downgrade to.

```
apt-get install kerio-connect=<version>
```

For example, `apt-get install kerio-connect=8.5.0.4190-1`

Kerio Connect downgrades to the specified version.

2.6.5 Migrating from current installations to Kerio Connect Multi-Server

NOTE

This information designed for Kerio Connect Multi-Server 9

If you are using Kerio Connect, you can easily migrate your current installation to Kerio Connect Multi-Server.

NOTE

Before you start the migration, back up your data. For more information, refer to [Configuring backup in Kerio Connect](#) (page 165).

Migrating from Kerio Connect connected to a directory service

If you are using a directory service for user management, you must install Kerio Connect Multi-Server, connect it to a directory service, and migrate users from the original server.

Connecting Kerio Connect Multi-Server to a directory service

1. Install the Kerio Connect Multi-Server [puppet master server](#).
2. Install the Kerio Connect Multi-Server [directory server](#).
3. Install one Kerio Connect Multi-Server [back-end server](#). This is the master server.
4. Log in to the back-end server administration and go to the **Configuration > Domains** section.
5. Double-click your domain and go to the **Directory Service** tab.

6. Configure the connection to your directory server. For more information, refer to [Connecting Kerio Connect to directory service](#) (page 293).

7. Continue installing the remaining servers: additional back-ends, instant messaging, front-end, and Zabbix. For more information, refer to [Installing Kerio Connect Multi-Server](#) (page 45). The directory server configuration is automatically distributed to all servers.

If you use Kerberos authentication, you must configure it on each back-end server separately. For more information, refer to [Joining Kerio Connect running on Linux to Open Directory or Active Directory](#) (page 98).

Migrating users and data from your Kerio Connect

To migrate your users and their data to the new Kerio Connect Multi-Server installation:

1. On the original Kerio Connect server, go to **Configuration > Domains**.

2. Click the **Distributed Domains** button.

3. Click **Next**.

4. Type the hostname of the first back-end server (master server) of your Kerio Connect Multi-Server, and the username and password of its admin.

5. Click **Connect**. The original server is now connected to your Kerio Connect Multi-Server.

6. On a back-end server, go to **Accounts > Users** and migrate all users from the original to the back-end server. For more information, refer to [Migrating users between the back-end servers](#) (page 59).

7. Disconnect the original server from the distributed domain in Kerio Connect Multi-Server.

Now you can start using Kerio Connect Multi-Server.

Migrating from a Kerio Connect distributed domain

If you are using a Kerio Connect distributed domain, you must install Kerio Connect Multi-Server, connect it to a directory service, and migrate users from the original servers.

To install Kerio Connect Multi-Server and connect it to a directory service, read [Connecting Kerio Connect Multi-Server to a directory service](#), above.

Migrating users and data from your distributed domain

To migrate your users and their data to the new Kerio Connect Multi-Server installation, do the following for each server in your distributed domain:

1. Disconnect the server from the distributed domain. For more information, refer to [Disconnecting server from distributed domain](#) (page 265).

2. On that server, go to **Configuration > Domains**.

3. Click the **Distributed Domains** button.

4. Click **Next**.

5. Type the hostname of the first back-end server (master server) of your Kerio Connect Multi-Server, and the username and password of its admin.

6. Click **Connect**. The server is now connected to your Kerio Connect Multi-Server.

7. On a back-end server, go to **Accounts > Users** and migrate all users from the original to the back-end server. For more information, refer to [Migrating users between the back-end servers](#) (page 59).
8. Disconnect the server from the distributed domain in Kerio Connect Multi-Server.

Now you can start using Kerio Connect Multi-Server.

Migrating from Kerio Connect with a local user database

If you have Kerio Connect with a local database of users, you must install Kerio Connect Multi-Server, connect it to a directory service, create users in the directory service and migrate the users from the original server.

Follow the instructions in [Connecting Kerio Connect Multi-Server to a directory service](#) (above), then perform the migration using the steps below.

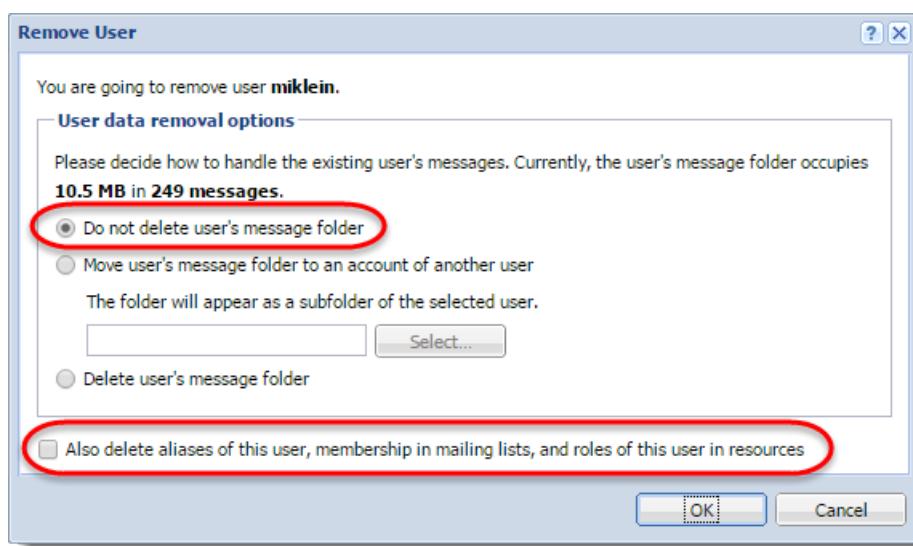
Migrating users and data from your server with a local database

To migrate your users and their data to the new Kerio Connect Multi-Server, you must remove the users from the original server, connect this server to Kerio Connect Multi-Server directory server, create the same users on the original server, and then migrate them to a back-end server.

1. On the original Kerio Connect server, go to **Accounts > Users**.

2. Remove all local users.

While removing users, in the **Remove User** dialog box, select **Do not delete user's message folder** and uncheck the **Also delete aliases of this user...** option.



3. Connect the server to the Kerio Connect Multi-Server directory server by editing the configuration file. For more information, refer to [Mapping users/groups from an OpenLDAP or Generic LDAP server](#) (page 309).
4. On the original server, create users with the same usernames as before. For more information, refer to [Creating users in Kerio Connect Multi-Server](#) (page 58).
5. On that server, go to **Configuration > Domains**.
6. Click **Distributed Domains**.
7. Click **Next**.

8. Type the hostname of the first back-end server (master server) of your Kerio Connect Multi-Server, and the username and password of its admin.

9. Click **Connect**. The original server is now connected to your Kerio Connect Multi-Server.

10. On a back-end server, go to **Accounts > Users** and migrate all users from the original to the back-end server. For more information, refer to [Migrating users between the back-end servers](#) (page 59).

11. Disconnect the original server from the distributed domain in Kerio Connect Multi-Server.

Now you can start using Kerio Connect Multi-Server.

2.6.6 Securing Kerio Connect Multi-Server

NOTE

This information is designed for Kerio Connect Multi-Server 9.

All servers in Kerio Connect Multi-Server communicate between them unsecurely. Therefore, run Kerio Connect Multi-Server in a dedicated private network protected with a firewall.

Firewall settings

This table shows the protocols and ports used in Kerio Connect Multi-Server.

IMPORTANT

Do not change these ports.

Refer to the table below and on your firewall, open the ports for the front-end server and instant messaging server.

Server	Protocol	Port
Syslog server	UDP	514
Directory server	LDAP	389
Back-end servers	IMAP	143
	POP3	110
	HTTP	80
	SMTP	25
	Kerio Connect Administration	4040
Instant messaging server	XMPP	5222
	XMPP SSL	5223
Session server	memcached	11211
Distributed domain server	Synchronization	44337
	Free/Busy HTTP	80
	Free/Busy HTTPS	443
	User migration HTTPS	443

Server	Protocol	Port
Front-end server	IMAP	143
	IMAP SSL	993
	POP3	110
	POP3 SSL	995
	SMTP	25
	SMTP SSL	465
	SMTP Submission	587
	HTTP	80, 8800
	HTTP SSL	443, 8843

2.6.7 Enforcing HTTPS in Kerio Connect Multi-Server

You can configuring the front-end server to enforce all Kerio Connect Multi-Server traffic through HTTPS:

1. Log in to the [front-end server](#).
2. Locate the `/opt/kerio/proxy/bin` directory.
3. Back up the `nginx.conf` file.
4. Open the `nginx.conf` file for editing.
5. Locate the following lines at the end of the file:

```
server {
    listen 80;
    listen [::]:80 ipv6only=on;
    listen 8800;
    listen [::]:8800 ipv6only=on;
    include http_server_settings.conf;
}
```

6. Replace the lines from step 5 with the following:

```
server {
    listen 80;
    return 301 https://$host$request_uri;
}

server {
    listen 8800;
    return 301 https://$host:8843$request_uri;
}
```

7. Save the `nginx.conf` file.
8. Restart the front-end server.

2.6.8 Licensing Kerio Connect Multi-Server

NOTE

This information is designed for Kerio Connect Multi-Server 9

Kerio Connect Multi-Server requires one standard Kerio Connect license.

However, you have to install the license on every back-end server and the instant messaging server (if you have one).

For more information, refer to [Registering Kerio Connect](#) (page 26).

2.6.9 Managing Kerio Connect Multi-Server

NOTE

This document relates to Kerio Connect Multi-Server 9

You configure Kerio Connect Multi-Server the same as any single-server installation of Kerio Connect, but take a note of the following important points:

- » Users, groups, aliases, mailing lists, and resources are distributed to all servers. Other configuration, such as domain settings, must be done on each server separately.
- » If you configure **DKIM** on the master server, Kerio Connect Multi-Server distributes the configuration to all back-end servers. For more information, refer to [Authenticating messages with DKIM](#) (page 332).
- » If you use SpamAssassin, Kerio Connect Multi-Server distributes the database to all back-end servers.
- » You must configure **backup** and **archiving** on each back-end server separately. Read [Configuring backup in Kerio Connect](#) and [Archiving in Kerio Connect](#) for additional information.
- » To use **Chat in Kerio Connect Client**, enable it per domain on the master server. For more information, refer to [Enabling chat in Kerio Connect Client](#) (page 187).

Accessing the administration interface

You can access the administration interface of the individual back-end servers only from the Kerio Connect Multi-Server internal network.

Log in to the administration interfaces of all back-end servers using these credentials:

- » username: `admin`
- » password: the password you typed when [installing the puppet master](#).

2.6.10 Creating users in Kerio Connect Multi-Server

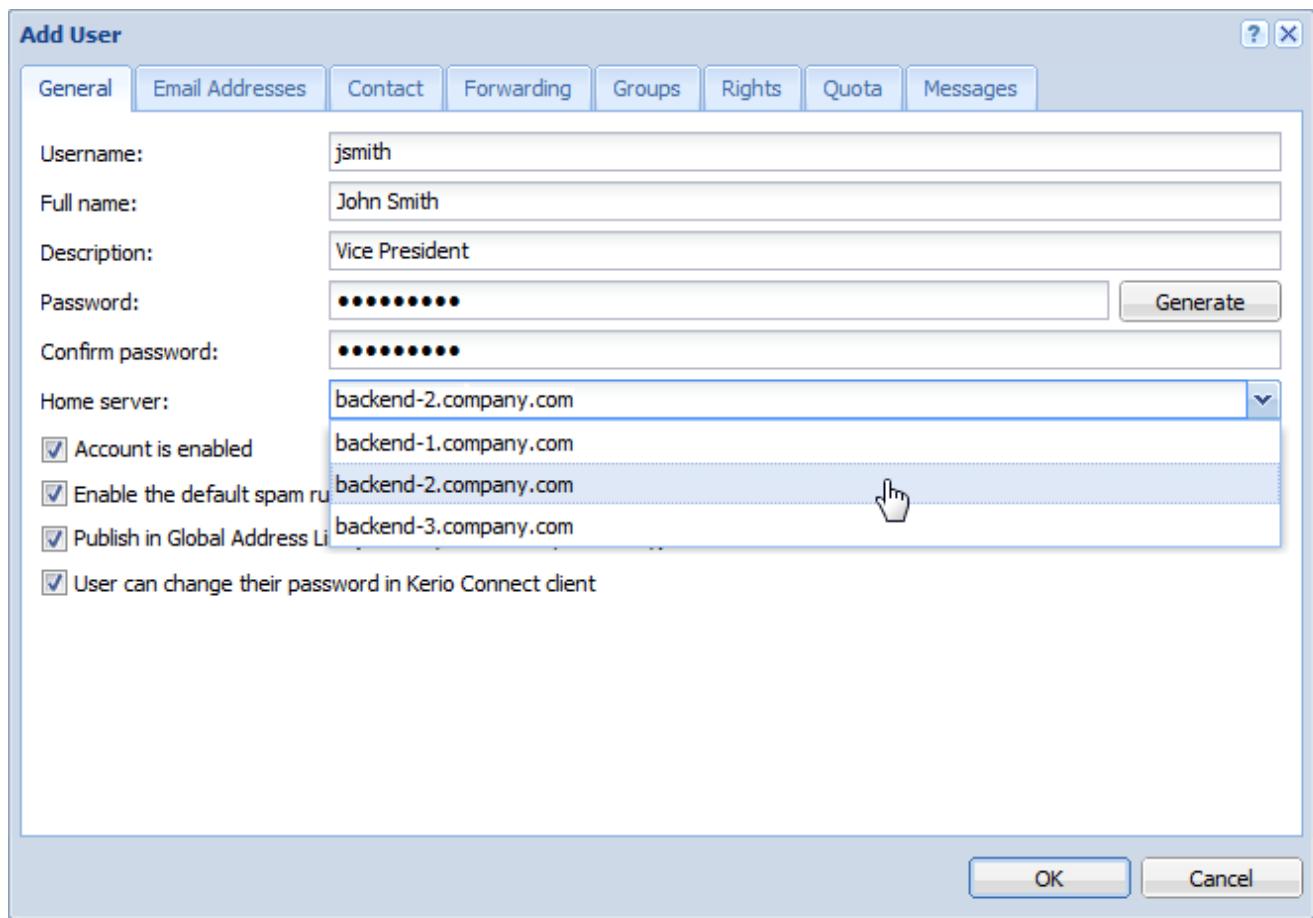
NOTE

This information is designed for Kerio Connect Multi-Server 9

You can create new users in the directory server through the Kerio Connect administration interface.

1. Log in to the **master** back-end server's administration interface. A master server is the first back-end server you installed.
2. Go to the **Configuration > Users** section.

3. Click **Add**.
4. Select **A new user in a directory service**.
5. Fill in the user information. For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).
6. Select the user's home server.
7. Click **OK**



Migrating users between the back-end servers

You can migrate any user from one back-end server to another.

1. Log in to the administration interface of the server you want to migrate users to.
2. Go to the **Accounts > Users** section.
3. Select a user and select **More Actions > Migrate Here**.
4. Confirm the migration.

The screenshot shows a user management interface for Kerio Connect. At the top, there is a search bar with the domain set to "company.com". Below the search bar is a table with columns: Username, Full Name, Home Server, and Description. Three users are listed: ajones (Adam Jones, backend-1.company.com), bthomas (Ben Thomas, backend-3.company.com), and jsmith (John Smith, backend-2.company.com, Vice President). A context menu is open over the jsmith row, with the "Migrate Here" option highlighted. Other options in the menu include "Reindex Mailbox", "Restore IM Contact List...", "User Statistics...", and "Mobile Devices...". Below the table are buttons for "Add...", "Edit...", "Remove...", "More Actions ▾", and "Import and Export ▾".

2.6.11 Accessing the Kerio Connect mailboxes

NOTE

This information is designed for Kerio Connect Multi-Server 9.

All users, regardless of their home server, access their account through the front-end server address. Kerio Connect Multi-Server directs the connection to the user's back-end server automatically.

Use the front-end server address when accessing and configuring all email clients, for example, Kerio Connect Client, Microsoft Outlook, and so on.

NOTE

Cross-server sharing is available for Kerio Connect Client users and users with Kerio Outlook Connector (Offline Edition).

2.6.12 Monitoring Kerio Connect Multi-Server with the Zabbix server

NOTE

This information is designed for Kerio Connect Multi-Server 9.

Zabbix can monitor all servers in the Kerio Connect Multi-Server deployment and display the data in one place. You can monitor CPU and memory usage and available disk space.

Puppet master automatically installs the Zabbix local agents on each server and reports the data via SNMP to the Zabbix server.

To access the Zabbix monitoring and see the data:

1. In your browser, type the Zabbix server hostname.
2. Type `admin` as the username, and use the password you typed during installation.
3. Now you can start using the Zabbix server.

Zabbix server can send notification messages. See the Zabbix documentation on [zabbix.com](#) for details.

2.6.13 Troubleshooting Kerio Connect Multi-Server

NOTE

This information is designed for Kerio Connect Multi-Server 9.

If any problem occurs in your Kerio Connect Multi-Server installation, consult the logs. Go to any back-end server's administration interface and locate the **Logs** section. For more information, refer to [Managing logs in Kerio Connect](#) (page 215).

For more information, refer to [Managing logs in Kerio Connect](#) (page 215).

2.7 Kerio Cloud

Kerio Cloud is a secure messaging and voice service provided by Kerio Technologies.

This topic provides general instructions for the initial setup and migration of your current Kerio Connect installation to Kerio Cloud.

See the sections below for additional information about each step.

Step 1: Create a Kerio Cloud account

To create a Kerio Cloud account, go to <https://secure.kerio.com/order/>.

You can select the plan type for a particular domain, the location of the data center, number of users, and optionally an additional archiving option.

For more information, refer to [Creating accounts in Kerio Cloud](#) (page 65).

NOTE

You must own the domain before creating a Kerio Cloud account.

Choose Kerio Cloud product

Kerio Cloud Messaging Business Pro - Unlimited mailbox storage, Advanced anti-spam, Kerio Operator ▼

All Business Pro mailboxes include a Kerio Operator on-premises license.

Configuration

Your domain * (To get started, tell us the domain you would like to use.) ?

feelmorelaw.com

Choose your data center

- US Data Center
 EU Data Center

How many users

Select the number of users

Email Archiving

- Not included
 Add Email Archiving

Step 2: Verify your domain

To proceed after you complete your Kerio Cloud order, you must verify you are the owner of the domain. Create a special CNAME DNS record or click the verification link sent to the domain owner.

For more information, refer to [Verifying domains for Kerio Cloud](#) (page 67).

Type	Host name	TTL	Value
CNAME ▼	keriocloud.feelmorelaw.com	3600	validation.kerio.cloud

add

Step 3: Create your first user

To create users in Kerio Cloud:

1. Go to your domain administration in Kerio Cloud. For more information, refer to [Managing Kerio Connect domain](#) (page 70).
2. Create your first user. For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).

Step 4: Create aliases

In Kerio Cloud, you can have **username aliases** and **domain aliases**.

If you have a **private cloud**, you can create **username aliases** and **domain aliases** directly in the administration interface.

If you do not have a private cloud, you can create **username aliases**. For domain aliases, contact [the technical support](#).

Step 5: Migrate data from your server to Kerio Cloud

To migrate user data from your installation of Kerio Connect to Kerio Cloud, use the online Kerio Connect Migration Service.

Before you start the migration, create a user (as described above) and assign them **full admin access** and **public folders rights**. Use this user during the migration.

For more information, refer to [Kerio Connect Migration Service](#) (page 145).

NOTE

To migrate from another service, contact [the technical support](#).

Kerio Connect Migration Service

Transfer Kerio Connect mailbox data and user accounts to a new Kerio Cloud server. [Learn more...](#)

To get started, provide your domain administrator account (Kerio Cloud) or the full administrator account of your destination server.

Hostname

host001.keriocloud.com

Administrator account

powaro@feellmorelaw.com

Password

.....

Login



Step 6: Add the necessary DNS records to your domain

To fully benefit from all the Kerio Cloud functions, you must create specific DNS records in your domain.

For more information, refer to [DNS records for Kerio Cloud](#) (page 68).

NOTE

Each provider has a different user interface and the process for adding DNS records may vary.

Here are some examples:

DNS ENTRY	TYPE	PRIORITY	TTL	DESTINATION/TARGET		
Hostname @	Type MX	Priority 10		Destination/Target host001.eu1.kerio.cloud.		
Hostname keriocloud	Type CNAME			Destination/Target validation.kerio.cloud.		
Hostname mail	Type CNAME			Destination/Target host001.eu1.kerio.cloud.		
Hostname sharecloud	Type CNAME			Destination/Target host001.eu1.kerio.cloud.		
Hostname (eg: something.pasta10.online)	Type A			Destination IPv4 address (eg: 94.136.40.129)	Add	

DNS Records

Name	Type	Priority	Weight	Port	Value	
@ feelmorelaw.com	A				93.184.216.34	
mail mail.feelmorelaw.com	CNAME				mail.feelmorelaw.com	
@ feelmorelaw.com	MX	10			mail.feelmorelaw.com	
mail_domainkey mail_domainkey.feelmorelaw.com	TXT				"v=DKIM1;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfl0chtL4siFYCrSPxw43fq4zOo3N+I220oK2Cp+NZw9Kuvg8"	
@ feelmorelaw.com	TXT				"v=spf1 mx a"	

[+ NEW RECORD](#)

Step 7: Send your first email message

Send an email message to test your Kerio Cloud and DNS settings. The message may be delayed due to antispam settings.

For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1331

NOTE

Kerio Cloud automatically deletes emails moved to Trash after 15 days.

Step 8: Configure email clients

See the following topics for details:

- » [Kerio Connect Client](#)
- » [Kerio Connect Client for Windows and Mac](#)
- » [Various mobile devices](#)

Step 9: Managing your account

See the following topics for details:

- » [Managing Kerio Connect domain](#) — Information about accessing administration and creating users, user groups, aliases, mailing lists, and resources.

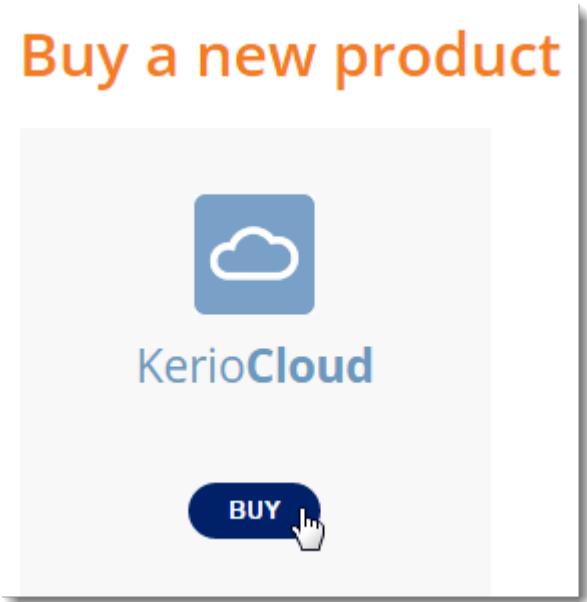
- » [Configuring domains in Kerio Cloud](#) — Information about managing domains, migrating your domains to Kerio Cloud, and upgrading your plan.
- » [Upgrading your Kerio Cloud account](#) — Information about adding users and services to your plan, and about plan upgrades.

2.7.1 Creating accounts in Kerio Cloud

You must purchase the domain in advance.

To create a Kerio Cloud account:

1. In your browser, open <https://secure.kerio.com/order>.
2. To create a new account, click **Buy** under the Kerio Cloud icon.



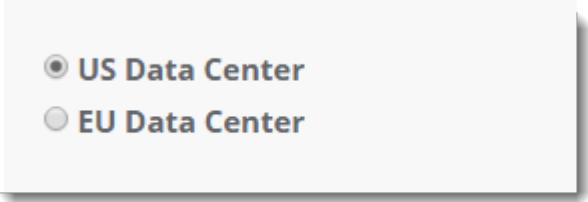
3. Select a plan.

Kerio Cloud Messaging Business - 10 GB mailbox storage, Basic anti-spam

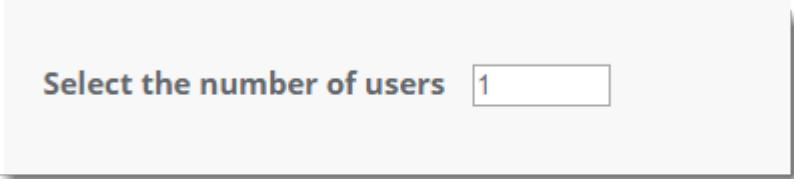
Kerio Cloud Messaging Business Pro - Unlimited mailbox storage, Advanced anti-spam, Kerio Operator

4. Type the name of your domain. You must purchase the domain in advance.

5. Select the data center location. You can have your data stored in a US based data center or in a European data center in Ireland.

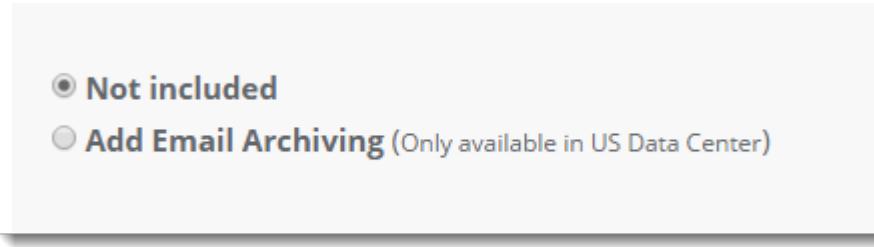
- 
- US Data Center**
 - EU Data Center**

6. Select the number of users.



Select the number of users

7. For the US based data center, you can select the email archiving feature.

- 
- Not included**
 - Add Email Archiving (Only available in US Data Center)**

8. Select the billing period.

9. Click **Add to your cart**.

10. Click **Proceed to checkout**.

To pay the subscription:

1. Select the payment method and click **Next**.
2. Fill in your contact information and click **Next**.
3. Review the details and click **Confirm**.

Now your account is set.

Kerio Cloud requires you to verify your domain. For more information, refer to [Verifying domains for Kerio Cloud](#) (page 67).

2.7.2 Configuring domains in Kerio Cloud

After you create an account for Kerio Cloud, log in to the Kerio Cloud interface where you can:

- » Upgrade your subscription.
- » Manage your domains.
- » Migrate your current domain to Kerio Cloud.

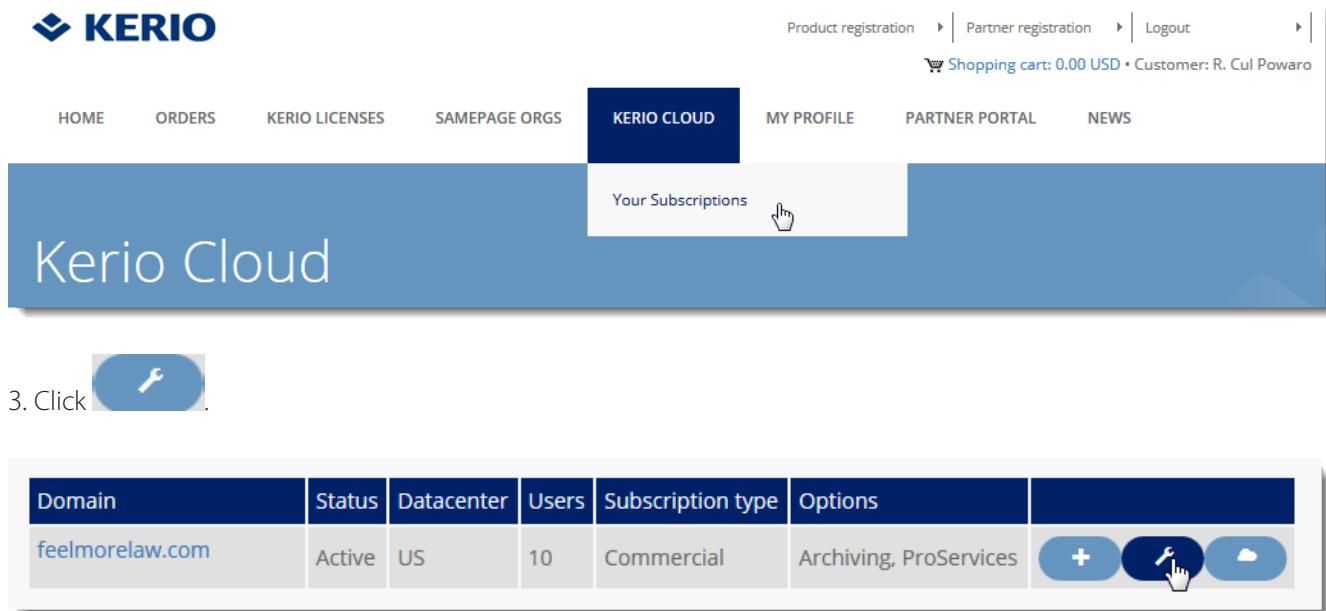
Managing domains in Kerio Cloud

1. Log in to Kerio Cloud at <https://cloud.kerio.com/>. Use the credentials you received after creating an account.

NOTE

To create a Kerio Cloud account, follow the instructions in [Creating accounts in Kerio Cloud](#)

2. Go to **Kerio Cloud > Your Subscriptions**.



The screenshot shows the Kerio Cloud dashboard. At the top, there's a navigation bar with links for Product registration, Partner registration, Logout, Shopping cart: 0.00 USD, and Customer: R. Cul Powaro. Below the navigation bar, there are several menu items: HOME, ORDERS, KERIO LICENSES, SAMEPAGE ORGS, KERIO CLOUD (which is highlighted in blue), MY PROFILE, PARTNER PORTAL, and NEWS. A large blue banner with the text "Kerio Cloud" is visible. In the center, there's a white box labeled "Your Subscriptions" with a hand cursor icon pointing at it. Below this, there's a table with a single row showing domain information:

Domain	Status	Datacenter	Users	Subscription type	Options
feelmorelaw.com	Active	US	10	Commercial	Archiving, ProServices

At the bottom right of the table, there are three icons: a plus sign, a wrench, and a cloud. The wrench icon has a hand cursor over it, indicating it's the target for the next step.

The Kerio Connect administration interface opens.

See the [Managing Kerio Connect domain](#) article for details about managing users, groups, aliases, mailing lists, and resources.

Upgrading your subscriptions

For more information, refer to [Upgrading your Kerio Cloud account](#) (page 73).

Migrating your domain to Kerio Cloud

If you create a [new domain in Kerio Cloud](#), you can migrate your data from your existing domain.

1. Log in to Kerio Cloud at <https://cloud.kerio.com/>. Use the credentials you received after creating an account.

2. Go to **Kerio Cloud > Your Subscriptions**.



3. Click

4. Follow the instructions in Kerio Connect Migration Service.

2.7.3 Verifying domains for Kerio Cloud

After you [complete the order for your Kerio Cloud account](#), Kerio sends the following verification emails:

- » An email to the owner of the domain with the verification link. Kerio finds the email address in WHOIS records.
- » An email to your email address with a request to add a CNAME record to your domain

Complete the instructions in one of the emails to verify the domain.

If the validation is pending, Kerio also sends email reminders with the same instructions 24 and 48 hours after you make the order.

Verifying domains via the verification link

Kerio sends an email with the link only to a recognized owner of the domain found in WHOIS records.

To verify the domain, open the **Kerio Cloud Domain Verification** email and click the link.

NOTE

Verify that the contact email for your domain is valid, otherwise, you will not receive the verification email.

Adding a CNAME record to your domain

To add CNAME you received in the **Domain Validation Required** email to your DNS records:

- » Ask an administrator of your DNS record to add CNAME.
- » Log into your domain registrar's admin console and add the record.

The command has the following format: `keriocloud.<domain_name> IN CNAME validation.kerio.cloud`.

NOTE

The change in your DNS records may take some time.

2.7.4 DNS records for Kerio Cloud

You must configure your domain DNS records to send/receive messages through Kerio Cloud accounts. This article describes the essential records you need to configure.

MX records

To receive email to your domain, you must configure an MX (mail exchange) record in your DNS.

The settings are different for each plan.

Business plan

Your MX record settings depend on the server your domain is hosted.

You can find the server hostname in the welcome email message you receive from Kerio Cloud.

Record Type	Hostname	Value
MX	[your domain name]	[server hostname from the welcome email] For example: host001.eu1.kerio.cloud

Business Pro plan and Private Cloud

If your server is in the **European data center**, add MX records for all of these hostnames:

Record type	Value	Priority
MX	mx1.eu1.kerio.cloud	10
MX	mx2.eu1.kerio.cloud	10

If your server is in the **US data center**, add MX records for all of these hostnames:

Record type	Value	Priority
MX	mx1.us1.kerio.cloud	10
MX	mx2.us1.kerio.cloud	10
MX	mx3.us1.kerio.cloud	10

DNS records for DKIM

To sign outgoing messages with **DKIM**, add a CNAME record to your DNS.

The CNAME record settings depend on the server your domain is hosted. You can find the server hostname in the welcome email message you receive from Kerio Cloud.

The settings are the same for both plans.

Record Type	Hostname	Value
CNAME	mail._domainkey.[your domain name]	dkim.[server hostname from the welcome email] For example: dkim.host001.eu1.kerio.cloud

DNS records for SPF

Sender Policy Framework (SPF) allows you to filter out messages with fake sender addresses.

To [use SPF](#), add a TXT record to your DNS.

The settings are the same for both plans.

If your server is in the **European data center**, add the following TXT record:

Record Type	Hostname	Value
TXT	[your domain name]	v=spf1 mx include:eu1.kerio.cloud -all

If your server is in the **US data center**, add the following TXT record:

Record Type	Hostname	Value
TXT	[your domain name]	v=spf1 mx include:us1.kerio.cloud -all

DNS for XMPP

If you want to make instant messaging in Kerio Connect accessible from other servers, you must add SRV records to your domain's DNS.

For more information, refer to [Configuring DNS for instant messaging](#) (page 184).

DNS for autodiscover

Autodiscover enables users to setup their accounts on desktop applications and mobile devices by using only their account credentials (usernames and passwords).

To enable autodiscover, you must add a SRV record to your domain's DNS.

For more information, refer to [Configuring Autodiscover in Kerio Connect](#) (page 399).

2.7.5 Managing Kerio Connect domain

The domain administrator manages accounts through Kerio Connect Administration.

They can add, edit, and remove:

- » **Users** (For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).)
- » **User groups** (For more information, refer to [Creating user groups in Kerio Connect](#) (page 272).)
- » **Aliases** (For more information, refer to [Creating aliases in Kerio Connect](#) (page 283).)
- » **Mailing lists** (For more information, refer to [Creating mailing lists in Kerio Connect](#) (page 281).)
- » **Resources** (For more information, refer to [Configuring resources in Kerio Connect](#) (page 287).)

NOTE

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

The screenshot shows the 'Users' section of the Kerio Connect Administration interface. On the left, there's a sidebar with icons for 'Users', 'Groups', 'Aliases', 'Mailing Lists', and 'Resources'. The main area has a title 'Users' with a search bar and a dropdown for 'R. Cul Powaro'. Below is a table with columns 'Username', 'Full Name', and 'Description'. The data is as follows:

Username	Full Name	Description
admin		
fan	Thomas Fan	
laboratory	Laboratory Mailbox	
maison	Pierre Maison	CFO
miklein	John Miklein	
mouse	Hector Mouse	Coroner
powaro	R. Cul Powaro	
regret	Meg Regret	
ski	Shimon Ski	
watzatko	Rada Watzatko	

At the bottom are buttons for 'Add', 'Edit...', and 'Remove...'. The overall interface is light blue and white.

Accessing the administration

To access the domain administration:

1. Log in to Kerio Cloud at <https://cloud.kerio.com/> Use the credentials you received after creating an account.

NOTE

To create a Kerio Cloud account, follow the instructions in [Creating accounts in Kerio Cloud](#)

2. Go to **Kerio Cloud > Your Subscriptions**.

Your Subscriptions



Kerio Cloud

3. Click the wrench icon  . The Kerio Connect administration interface opens.

Domain	Status	Datacenter	Users	Subscription type	Options	
feelmorelaw.com	Active	US	10	Commercial	Archiving, ProServices	  

2.7.6 Anti-spam protection in Kerio Cloud

Users of **Kerio Cloud Business Pro** and **Kerio Cloud Private Cloud** have access to an advanced anti-spam, including the ability to whitelist/blacklist email and to review messages retained by the quarantine.

Accessing the anti-spam service

1. In a web browser, type the URL that corresponds to your location:

Location	URL
Kerio Cloud EU	mx1.eu1.kerio.cloud
Kerio Cloud US	mx01.getsecuremx.com

2. Type the username and password for your Kerio Cloud account.

Reviewing the quarantine

The Kerio Cloud advanced anti-spam retains spam messages in the quarantine.

You can perform the following actions on the spam messages:

- » **Release** messages so that it delivers to your Inbox
- » **Whitelist** senders so that messages from these senders are never considered as spam
- » **Delete** messages from the quarantine

To perform these actions:

1. Select a spam message.
2. Click the button that corresponds to the actions you want to perform.

The screenshot shows the Kerio Connect web interface with the URL `mx1.us1.kerio.cloud`. At the top right, it displays "Logged In: bob@example.com | Logout", "Role: User", and "Version: 6.12 | License: STP-1-7000-896867". The main navigation tabs are "Settings", "Filter Rules" (which is selected), and "Quarantine". Below the tabs, there's a "Manage Quarantine" button. The central area is titled "Search Quarantine" with a search bar and a "SEARCH FILTERS" dropdown. It includes a "Date range: All" filter, a page number "Page: 1", and an "Entries per page: 150" dropdown. There are buttons for "Release", "Whitelist", and "Delete". A message "Showing 0 - 0 of about 0 items" is displayed. The main table header includes columns for "From", "To", "Subject", "Date", "Score", and "Flow". A message "No records found" is shown in the table body. At the bottom, there are "Release", "Whitelist", and "Delete" buttons.

©2006-2016 Copperfasten Technologies

Whitelisting and blacklisting senders

1. Switch to the **Filter Rules** tab.
2. Go to the **Users Whitelist/Blacklist** tab.
3. In the **Whitelisted/Blacklisted Email Addresses** or **Whitelisted/Blacklisted Domains**, click **Add**.
4. Type the **Sender Email** or **Sender Domain**.
5. (Optional) Type a **Comment** for better reference.
6. Click **Save**.

The screenshot shows the Kerio Connect Cloud web interface. At the top, the URL is mx1.us1.kerio.cloud, and the user is logged in as bob@example.com with a User role. The version is 6.12 and the license is STP-1-7000-896867. The navigation bar includes Settings, Filter Rules, Quarantine, User Blacklist, and User Whitelist. The User Whitelist tab is selected, showing the 'Whitelisted Email Addresses' page. The page displays a table with columns for Sender Domain, Comment, Last Modified, and Options. A modal window titled 'Add' is open, allowing the entry of a Sender Domain (microsoft.com) and a Comment (Allow all email from Microsoft). The main table below shows 'No records found.'

2.7.7 Upgrading your Kerio Cloud account

You can upgrade your Kerio Connect Cloud account anytime. You can:

- » Upgrade **Business Plan** to a **Business Pro Plan**

Kerio Cloud Messaging Business - 10 GB mailbox storage, Basic anti-spam

Kerio Cloud Messaging Business Pro - Unlimited mailbox storage, Advanced anti-spam, Kerio Operator

- » Add users
- » Add external archiving

Upgrading your plan

1. Log in to Kerio Cloud at <https://cloud.kerio.com/> Use the credentials you received after creating an account.

2. Go to **Kerio Cloud > Your Subscriptions**.



3. Click the plus icon

4. Edit your subscription plan. The options differ based on your current plan.

5. Click **Calculate the price** and then click **Add to cart**.

6. Click **Proceed to checkout**, select the payment method, and click **Next**.

7. Select a delivery address or add a new address and click **Next**.

8. Review your order and click **Confirm**.

9. Select the card type and click **Pay**.

10. Fill in the card info and click **Pay**.

2.7.8 Canceling services in the Kerio Cloud

If you need to cancel any service or domain registration, submit a ticket through the Kerio website at <http://www.kerio.com/support/technical-support>

2.7.9 Accounts created before May 10, 2016

This section applies to all Kerio Cloud accounts created before May 10, 2016.

- » Adding new domains to the Kerio Cloud accounts created prior to May 10, 2016
- » Configuring domains in the Kerio Cloud accounts created prior to May 10, 2016
- » Upgrading the Kerio Cloud accounts created prior to May 10, 2016
- » Canceling services in the Kerio Cloud accounts created prior to May 10, 2016

Adding new domains to the Kerio Cloud accounts created prior to May 10, 2016

NOTE

For accounts created prior to May 10, 2016.

To add new domains to Kerio Cloud, you can:

- » Register a new domain
- » Transfer your domain from another registrar
- » Use your existing domain and update your MX records

Registering a new domain

1. Log in to your Kerio Cloud account and click **Services > Order new service**.

2. Select **Register a new domain**.

3. Type the domain name and select the top level domain (TLD) from the drop down list.
4. Click **Check**Kerio Cloud checks the availability of the domain.

Register a new domain

www. .net ▾ **CHECK** 

Transfer your domain from another registrar

I will use my existing domain and update my nameservers

5. Select for how long you want to register the domain and click **Continue**.

You may also select additional TLD for your domain name.

Congratulations, feelmorelaw.net is available!

Register for longer and save!

 1 Year/s @ \$14.99 USD



 1 Year/s @ \$14.99 USD

 2 Year/s @ \$29.98 USD

 3 Year/s @ \$44.97 USD

 4 Year/s @ \$59.96 USD

 5 Year/s @ \$74.95 USD

Oth

 1 Y

 1 Y

terested in...

morelaw.biz





morelaw.us

NOTE

To renew your domain registration, go to **Domains > Renew domains**.

HOME E-MAILS (3) SERVICES DOMAINS BILLING SUPPORT OPEN TICKET HELLO, R. CUL!

Shopping Cart

Categories

- Kerio Cloud Messaging
- Product Addons

Actions

- Register a New Domain
- Transfer in a Domain

[MY DOMAINS](#)
[RENEW DOMAINS](#) (selected)
[REGISTER A NEW DOMAIN](#)
[TRANSFER DOMAINS TO US](#)

[BILLING](#)
[SUPPORT](#)

[OPEN TICKET](#)

[HELLO, R. CUL!](#)

Secure your domain with Kerio Cloud. Renew them. Choose how many years you want to renew for and then submit to continue.

Domain	Status	Days Until Expiry	Action
feelmorelaw.org	Active	365 Days	1 Year/s @ \$14.99 USD
powaro.com	Active	365 Days	1 Year/s @ \$14.99 USD

[Order Now](#)

For further steps, see **Setting domain parameters and ordering services** below.

Transferring your domain from another registrar

NOTE

Ask your registrar for an EPP code necessary for the transfer.

1. Log in to your Kerio Cloud account and click **Services > Order new service**.
2. Select **Transfer your domain from another registrar**.
3. Type the domain name and select the top level domain (TLD) from the drop down list.
4. Click **Transfer**.

Register a new domain

Transfer your domain from another registrar

.com ▼

TRANSFER

I will use my existing domain and update my nameservers

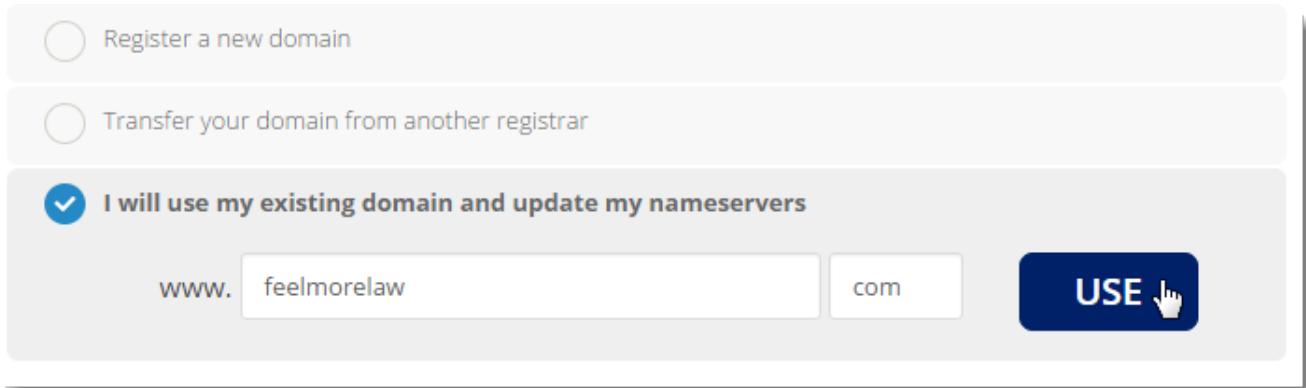
5. Click **Continue**.

For further steps, see **Setting domain parameters and ordering services** below.

Using your existing domain

1. Log in to your Kerio Cloud account and click **Services > Order new service**.
2. Select **Transfer your domain from another registrar**.

3. Click **Use**.



For further steps, see **Setting domain parameters and ordering services** below.

Setting domain parameters and ordering services

After selecting what domain type you want to use:

1. Select the number of mailboxes (users).
2. You can see the current price on the right in the **Order Summary** section.
3. Select your plan.

You can upgrade your plan later. For more information, refer to [Upgrading the Kerio Cloud accounts created prior to May 10, 2016](#) (page 88).

4. (Optional) Select **Add External email archiving** to enable external archiving. You can add archiving later. For more information, refer to [Upgrading the Kerio Cloud accounts created prior to May 10, 2016](#) (page 88).

5. Click **Continue**.

Configure your desired options and continue to checkout.

Kerio Cloud Messaging

Configurable Options

Base Kerio Connect Mailbox



Business Pro Plan Upgrade

Business Plan:

- Kerio Connect mailbox
- 10GB mailbox storage
- Basic anti-spam

Business Pro Plan:

- Kerio Connect mailbox
- **Unlimited** mailbox storage
- Advanced anti-spam
- Mobile device sync via Exchange ActiveSync

Email Archiving

Not Included

Add External email archiving

Order Summary

Kerio Cloud Messaging

Kerio Cloud Messaging

Kerio Cloud Messaging Monthly

» Base Kerio Connect Mailbox: 15

\$74.85 USD

» Business Pro Plan Upgrade: 0

\$0.00 USD

» Email Archiving: 15 \$45.00 USD

Monthly: \$119.85 USD

\$119.85 USD

Total Due Today

CONTINUE ➔

6. When **registering a new domain**, select additional options, and click **Continue**.

Please review your domain name selections and any addons that are available for them.

feelmorelaw.org

Registration Period

1 Year/s

Hosting

[Has Hosting]



DNS Management

External DNS Hosting can help speed up your website and improve availability with reduced redundancy.

FREE! / 1 Year/s

[+ Add to Cart](#)



ID Protection

Protect your personal information and reduce the amount of spam to your inbox by enabling ID Protection.

\$14.99 USD / 1 Year/s

[Added to Cart \(Remove\)](#)



Email Forwarding

Get emails forwarded to alternate email addresses of your choice so that you can monitor all from a single account.

FREE! / 1 Year/s

[Added to Cart \(Remove\)](#)

CONTINUE 

7. When **transferring your domain**, type the EPP transfer code you acquired from your registrar, select additional options, and click **Continue**.

8. Review your order and click **Checkout**.

9. If you have a **Promo Code**, type the code and click **Validate Code**.

10. To change any items, click **Edit** next to the item name.

11. To cancel the order, click **Empty Cart**.

Product/Options	Price/Cycle	
Kerio Cloud Messaging feelmorelaw.org » Base Kerio Connect Mailbox: 15 x Number of Users \$4.99 USD » Business Pro Plan Upgrade: 0 x Number of Users \$4.00 USD » Email Archiving: 15 x Number of Users \$3.00 USD	\$119.85 USD Monthly	x
Domain Registration feelmorelaw.org » Email Forwarding » ID Protection	\$29.98 USD 1 Year/s	x
Empty Cart		
Apply Promo Code		
<input type="text" value="Enter promo code if you have one"/>		
Validate Code		

Order Summary

Subtotal	\$149.83 USD
Totals	\$119.85 USD Monthly \$29.98 USD Annually
\$149.83 USD	
Total Due Today	

Checkout ➔

12. Click **Checkout**.

13. Review and update your contact information and select the payment method.

14. Agree to the **Terms of Service**.

15. Click **Complete Order**.

16. If you pay by **PayPal**, click **Complete Order**, click **PayPal Check Out**(or **Subscribe** for new PayPal account) and follow the PayPal instructions to pay your order.

Please enter your personal details and billing information to checkout.

Personal Information

R. Cul

Powaro

powaro@feelmorelaw.com

377338901

Billing Address

Feel More Law

Anglické nábrezí 1

Street Address 2

Plzen

State

30100

Czech Republic

Domain Registrant Information

You may specify alternative registered contact details for the domain registration(s) in your order when placing an order on behalf of another person or entity. If you do not require this, you can skip this section.

Use Default Contact (Details Above)

Payment Details

Total Due Today: **\$149.83 USD**

Please choose your preferred method of payment.

PayPal

Credit Card

Use Existing Card (0027)

Enter New Card Information Below

CVV Security Number

Additional Notes

You can enter any additional notes or information you want included with your order here...

I have read and agree to the Terms of Service

COMPLETE ORDER 

Once the order is complete, you receive emails with detailed information about your domains and Kerio Cloud account. See [Configuring domains in Kerio Cloud](#) for details about adding users and configuring your Kerio Connect.

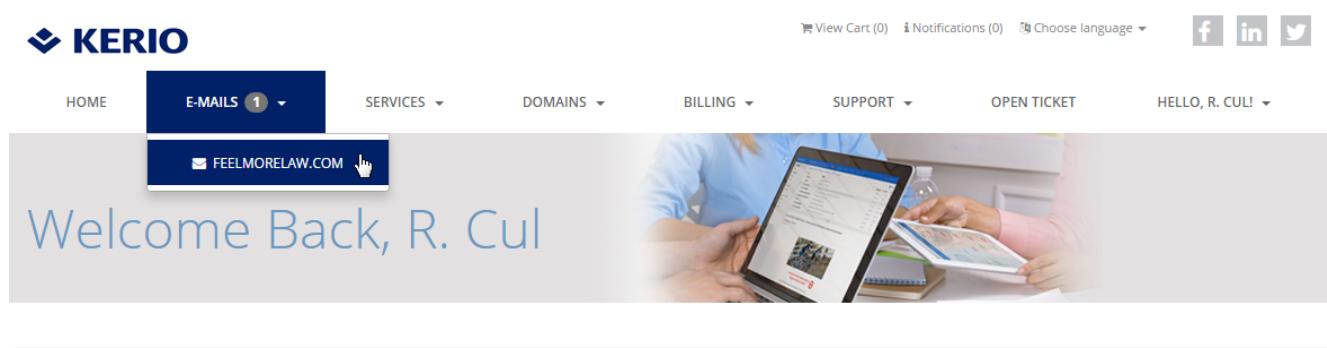
Configuring domains in the Kerio Cloud accounts created prior to May 10, 2016

NOTE

For accounts created prior to May 10, 2016.

After you create an account for Kerio Cloud, you can manage your domains in the **Email** section.

1. Login to Kerio Cloud at <http://cloud.kerio.com/>
2. Select your domain in the **Emails** drop-down list.



3. Configure your domain.

See the following sections for detailed configuration of your domain:

- » [Adding users to domains](#)
- » [Creating username/email aliases](#)
- » [Adding mailing lists](#)
- » [Adding user groups](#)
- » [Adding resources](#)
- » [Creating domain aliases](#)
- » [Enabling DKIM authentication](#)

Adding users to domains

1. Switch to your domain (see above).
2. Go to the **Email Accounts** section.
3. Click **+ Add**.

The screenshot shows the Kerio Connect dashboard. On the left, there's a sidebar with links like 'E-Mail Accounts', 'Domain Groups', 'Spam Settings', and 'Upgrade Account'. The main area has two cards: 'Users' (0 of 25 created) and 'Storage' (Unlimited). Below these are several configuration items with checkboxes: 'Unlimited Accounts' (checked), 'ActiveSync Enabled' (checked), 'Domain Aliases' (unchecked), and 'Folder Admins' (unchecked). At the bottom, there's a 'Users' section with a red circle around the '+ Add' button, followed by a message 'Users for domain: feelmorelaw.com'.

4. Type the username, password, full name and description for the user, and click **Next**.

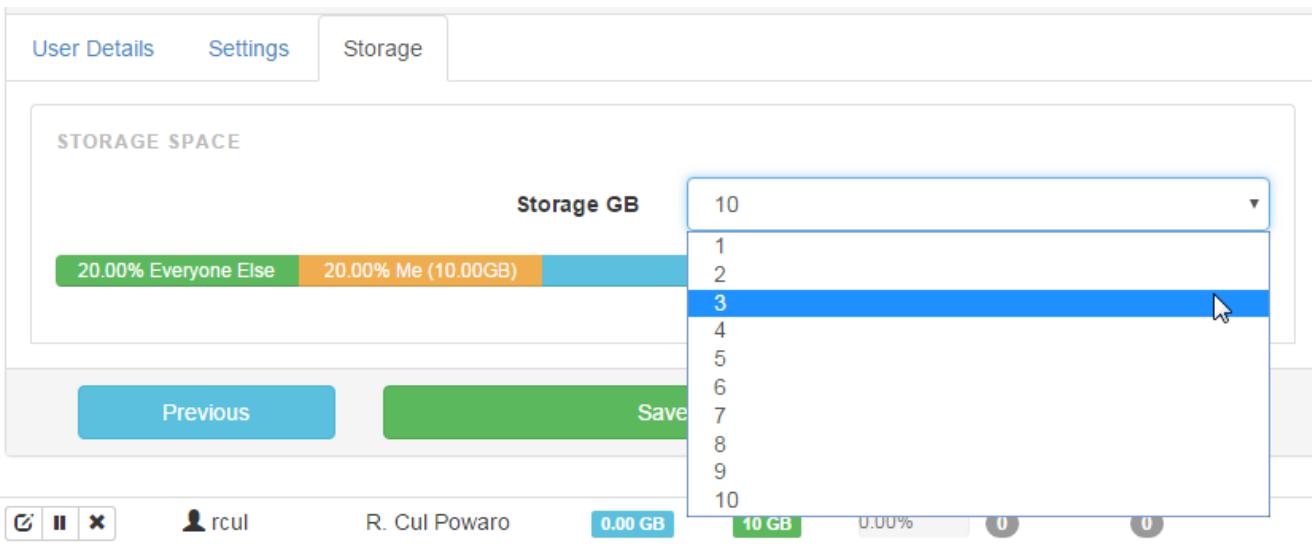
5. (Optional) You can also:

- Assign the user public folder admin access
- Publish their contact info in the global address list
- Allow the user to change their password

This screenshot shows the 'User Details' configuration page. It has tabs for 'User Details', 'Settings', and 'Storage'. Under 'PERMISSIONS', there are three checkboxes: 'Public Folder Admin' (checked), 'Allow Change Password' (checked), and 'Publish in GAL' (checked). At the bottom, there are 'Previous', 'Save' (in a green button), and 'Next' buttons.

6. Click **Next**.

7. Based on your plan, you can set the storage space in GB the user can occupy.



8. Click **Save**.

NOTE

If you use up your license (number of users) and you want to add additional users, click **Upgrade Account** in your domain settings, type the new number of users you want to have in your domain, and click **Upgrade**.

The screenshot shows the 'Upgrade Account' page. On the left, there are links for 'Upgrade Account', 'Help', and 'Webmail'. The main area is titled 'Upgrade Account' and contains a table for 'SECTION' upgrades:

	Base User Count	x \$4.99
<input checked="" type="checkbox"/> Pro Upgrade	20	x \$4.00
<input checked="" type="checkbox"/> Archiving		x \$3.00
Totals	User Cost: \$99.80 Pro Upgrade Cost: \$80.00 Archiving Cost: \$60.00	

A blue 'Upgrade' button is at the bottom.

Creating username aliases

1. Switch to your domain (see above).
2. Go to the **Email Aliases** section.
3. Type a name for the alias. The alias may contain the following characters:
 - Lower-case letters (no special characters)
 - Upper-case letters (no special characters)
 - Numbers

- . — Dot
- - — Dash
- _ — Underscore
- ? — Question mark
- * — Asterisk

4. The message can be delivered to:

- Email address — Type the email address
- Public folder — Select the public folder from the menu. This item is active only in case at least one email public folder is available.

5. Click **Add**.

ADD/EDIT DOMAIN E-MAIL ALIAS

Name	<input type="text"/> *	@...
Description	Invalid address - deliver to powaro	
Alias Type	<input checked="" type="radio"/> E-mail Address <input type="radio"/> Public Folder	
Deliver To E-mail	<input type="text"/> powaro@feelmorelaw.com	
<input type="button" value="Add"/>		

Adding mailing lists

To add a mailing list to your domain:

1. Switch to your domain (see above).
2. Go to the **Mailing Lists** section.
3. Type a name for the mailing list.
4. Type a description.
5. Select the language for the mailing list messages.
6. Click **Add**.

ADD/EDIT DOMAIN MAILING LIST

Details

Name	sales	@...
Description	Email address for the Sales dept.	
Language	English ▾	
Add		

Adding user groups

1. Switch to your domain (see above).
2. Go to the **Domain Groups** section.
3. Type a name for the group.
4. Type a description.
5. To publish the group in global address list, select **Publish in GAL**.

ADD/EDIT DOMAIN GROUP

Name	sales-team	@...
Description	Group of all sales people	
Publish in GAL	<input checked="" type="checkbox"/>	
Add		

6. Click **Add**.

Adding resources

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

To add a new resource, switch to your domain and go to the **Domain Resources** section.

ADD/EDIT DOMAIN RESOURCE

Name	<input type="text" value="alpha"/> @...
Description	<input type="text" value="Alpha meeting room"/>
Resource Type	<input checked="" type="radio"/>  Room <input type="radio"/>  Equipment
Reservation Manager	 <input type="text" value="powaro"/>
Allowed Users	 [All users of this domain]
<input type="button" value="Add"/>	

For more information, refer to [Creating new resources](#) (page 287).

Creating domain aliases

To create an alias for the entire domain, switch to your domain and go to the **Domain Aliases** section.

ADD/EDIT DOMAIN NAME ALIAS

Name	<input type="text" value="feelmorelaw.eu"/>
<input type="button" value="Add"/>	

For more information, refer to [Domain aliases](#) (page 284).

Enabling DKIM authentication

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 enable DKIM:

1. Switch to your domain (see above).
2. Go to the **Spam Settings** section.
3. Select **Enable DKIM**.
4. Click **Save**.

5. Add the displayed DKIM public key to your DNS records. For more information, refer to [Configuring DNS for DKIM](#) (page 334).

Upgrading the Kerio Cloud accounts created prior to May 10, 2016

NOTE

For accounts created prior to May 10, 2016.

You can upgrade your Kerio Connect Messaging plans anytime. You can:

- » Upgrade **Business Plan** to a **Business Pro Plan**

Business Plan:

- Kerio Connect mailbox
- 10GB mailbox storage
- Basic anti-spam

Business Pro Plan:

- Kerio Connect mailbox
- Unlimited mailbox storage
- Advanced anti-spam
- Mobile device sync via Exchange ActiveSync

- » Add users
- » Add external archiving

Upgrading your plan

1. Login to Kerio Cloud at <http://cloud.kerio.com/>
2. Select your domain in the **Emails** drop-down list.
3. Click **Upgrade Account**.
4. Type the number of total users you want have.
5. Select **Pro Upgrade** to upgrade from **Business Plan** to **Business Pro Plan**.
6. Select **Archiving** to enable external archiving.

SECTION		
Base User Count	20	x \$4.99
Pro Upgrade	<input checked="" type="checkbox"/>	x \$4.00
Archiving	<input checked="" type="checkbox"/>	x \$3.00
Totals	User Cost: \$99.80 Pro Upgrade Cost: \$80.00 Archiving Cost: \$60.00	

7. Click **Upgrade**.

8. Review your order and select the **Payment Method**. If you have a promotional code, type the code and click **Validate Code**.

9. Click the **Click to Continue** button.

Current Configuration: Kerio Cloud Messaging - Kerio Cloud Messaging (feelmorelaw.org)

Description	Price
Base Kerio Connect Mailbox: 15 => 20 x Number of Users	\$24.15 USD
Email Archiving: 15 => 20 x Number of Users	\$14.52 USD
Subtotal:	\$38.67 USD
Total Due Today:	\$38.67 USD

Promotional Code

Promotional Code

Validate Code

Payment Method

Credit Cart

CLICK TO CONTINUE >>

10. Proceed with the payment.

Canceling services in the Kerio Cloud accounts created prior to May 10, 2016

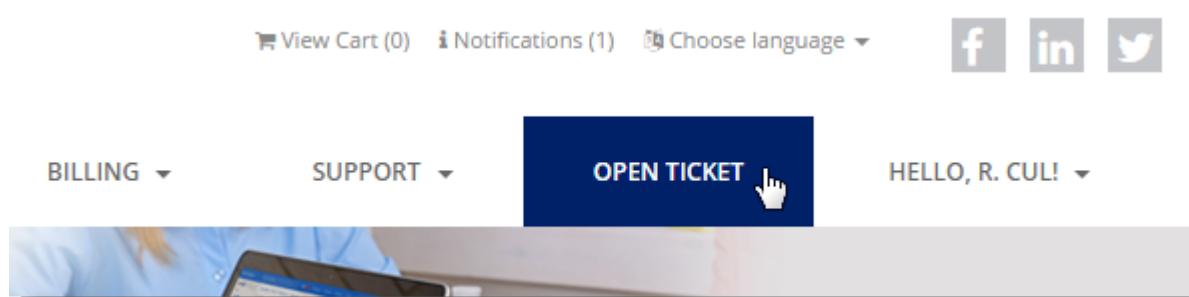
NOTE

The information here is for accounts created prior to May 10, 2016. To learn how to cancel services

If you need to cancel any service or domain registration, you must create a support ticket.

Canceling services

1. Log in to your Kerio Cloud account and click **Open ticket**.



2. Select **Billing and Account Management**

The image shows a large blue watermark-like text 'Open Ticket' overlaid on a photo of two people looking at a tablet displaying a dashboard. Below this, there are two support categories:

- Kerio Cloud Support**: Support for Kerio Cloud
- Billing and Account Management**: Account Changes and Billing Requests

A hand cursor icon is positioned over the 'Billing and Account Management' link.

3. Type a subject for the request.
4. In the **Related Services** drop-down list, select the service you want to cancel.

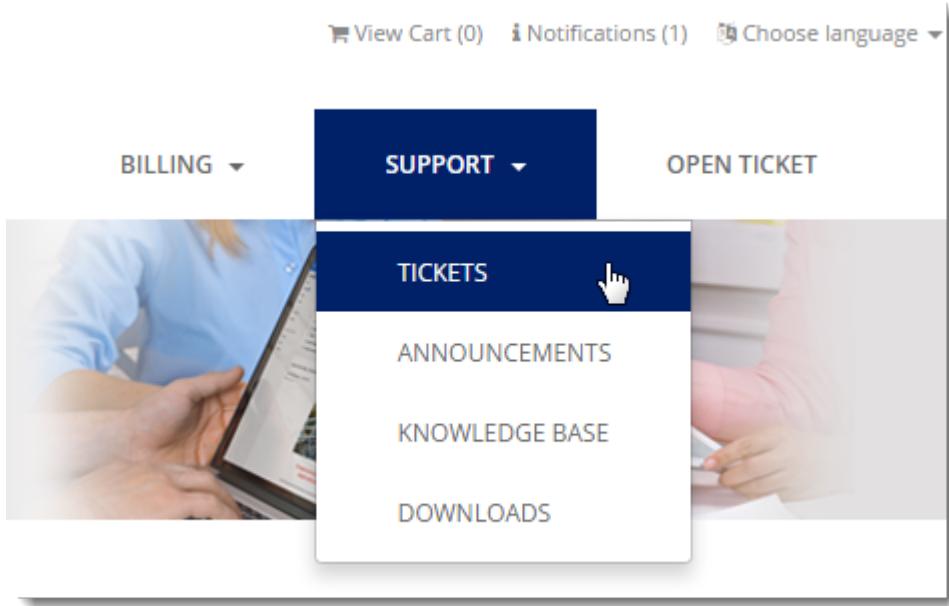
Name	Email Address	
R. Cul Powaro	powaro@feelmorelaw.com	
Subject		
Canceling		
Department	Related Service	Priority
Billing and Acc ▾	None	Medium ▾
Message	<ul style="list-style-type: none">NoneKerio Cloud Messaging - feelmorelaw.com (Active)Kerio Cloud Messaging - feelmorelaw.org (Active)Kerio Cloud Messaging - powaro.com (Active) Domain - feelmorelaw.org (Active)Domain - powaro.com (Active)	

5. (Optional) Set a priority for your request.
6. In the **Message** dialog box, specify details regarding the cancellation.
7. Type your contact telephone number.
8. Click **Submit**.

Name	Email Address	
R. Cul Powaro	powaro@feelmorelaw.com	
Subject		
Canceling		
Department	Related Service	Priority
Billing and Acc ▾	Kerio Cloud Messaging - powarc ▾	Medium ▾
Message		
<p>Hello, I'd like to cancel my subscription to Kerio Cloud with the following domain: powaro.com Thank you, R. Cul Powaro</p>		
Attachments		
<input type="button" value="Choose File"/> No file chosen	<input type="button" value="Add More"/>	
Allowed File Extensions: .jpg, .gif, .bmp, .pdf, .txt, .png, .zip, .rar, .tiff, .jpeg		
Best Contact Number		
+123456789		
<input type="button" value="SUBMIT"/> <input type="button" value="Cancel"/>		

Kerio Cloud sends a message to your email address.

To see your ticket, or add additional information and comments, click **Support > Tickets** to display the list of your tickets.



2.8 Virtual Appliance and Linux

This section describes deployment and configuration for virtual appliances and installations on Linux systems.

2.8.1 Kerio Connect VMware Virtual Appliance	93
2.8.2 Installation on CentOS 6.4 - 64-bit (both i386 and x86_64)	96
2.8.3 Installation on openSUSE 11.4 – 32-bit	97
2.8.4 Installation on openSUSE 11.4 – 64-bit (x86_64)	98
2.8.5 Joining Kerio Connect running on Linux to Open Directory or Active Directory	98
2.8.6 Kerio Connect Virtual Appliance Networking (Debian Edition - Kerio Connect 7.3.x and later)	103
2.8.7 How to make PHP's mail() command work with Kerio MailServer on Linux	104
2.8.8 Working with the Kerio Connect Virtual Appliance (CentOS Edition - Kerio Connect 7.2.x and earlier)	105
2.8.9 Working with the Kerio Connect Virtual Appliance (Debian Edition - Kerio Connect 7.3.x and later)	106
2.8.10 PAM authentication is not working in SuSE	111

2.8.1 Kerio Connect VMware Virtual Appliance

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, go to the [product pages](#).

Downloading Kerio Connect VMware Virtual Appliance

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

- » **VMware Server, Workstation** and **Fusion** — Download the VMX distribution package (*.zip), unzip and open it.
- » **VMware ESX/ESXi** — Import the virtual appliance from the OVF file's URL. VMware ESX/ESXi automatically downloads the OVF configuration file and a corresponding disk image (.vmdk). Browse to <https://www.kerio.com/connect/download/vmware-ovf-64>.

If your EXSi does not support deployment using URL. Download the required OVF files from <http://download.kerio.com/archive/>.

Then, follow these steps:

1. Select your **Product** and **Version** and click **Show Files**.
2. Download Kerio Control VMware Virtual Appliance (OVF) and Kerio Control VMware Virtual Appliance (OVF) – disk image on your local computer.
3. Browse and attach both the OVF files in the EXSi Host.
4. Wait for the deployment and the file transfer to fully complete on the EXSi Host.

NOTE

Tasks for shutdown or restart of the virtual machine are set to default values after the import. Setting these values to **hard shutdown** or **hard reset** may cause a loss of data on the virtual appliance. Kerio Connect VMware Virtual Appliance supports the so called **Soft Power Operations**. They allow you to shut down or restart the hosted operating system properly.

Working with the 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



Screenshot 4: Console — network configuration

IMPORTANT

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. View network adapters — MAC address, name and IP address of the adapter
2. Set network adapters
 - DHCP
 - static IP address (if you do not use DHCP, it is necessary to set also DNS)

NOTE

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

IMPORTANT

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 following dpkg command to upgrade Kerio Connect: # dpkg -i <installation_file_name.deb>

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

NOTE

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

2.8.2 Installation on CentOS 6.4 - 64-bit (both i386 and x86_64)

You can install Kerio Connect on 64-bit CentOS 6.4

1. Get the installation ISO images of CentOS 6.4 for i386 or x86_64 platform from www.centos.org.
2. Install CentOS 6.4 base system.
3. Disable postfix MTA in default CentOS installation: sudo /sbin/chkconfig postfix off sudo /sbin/service postfix stop
4. Download Kerio Connect 8.2 installation package in RPM format from [Kerio website](#) for the platform (i386 or x86_64).
5. Install Kerio Connect using the following command: sudo yum install kerio-connect-8.2.0-xxx-linux-x86_64.rpm or sudo yum install kerio-connect-8.2.0-xxx-linux-i386.rpm
6. Finish the initial server configuration using the CfgWizard application: sudo /opt/kerio/mailserver/cfgwizard
7. Start Kerio Connect using the following command: sudo /sbin/service kerio-connect start
8. Optionally, configure CentOS firewall to allow remote administration and Kerio Connect protocols: sudo vi /etc/sysconfig/iptables. Add line -A INPUT -p tcp --dport 4040 -j ACCEPT before the line with REJECT rule for INPUT chain.

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -p tcp --dport 4040 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

You can add same rules for other TCP ports used by services in Kerio Connect. See web administration services for the list of protocols.

To re-load the iptables firewall: `sudo /sbin/service iptables restart`

Since Kerio Connect is now installed and configured, you can access the web admin interface at <https://<servername>:4040>.

IMPORTANT

Don't forget to configure your DNS server and add proper A and MX records for the server.

NOTE

Kerio Connect users can be authenticated against PAM with `/etc/pam.d/keriomail` PAM module.

To uninstall the Kerio Connect, run `sudo yum remove kerio-connect`.

2.8.3 Installation on openSUSE 11.4 – 32-bit

You can install Kerio Connect 7.3 on openSUSE 11.4 (i386).

1. Get the installation ISO images of openSUSE 11.4 for i386 platform from www.opensuse.org.
2. Install openSUSE 11.4 base system.
3. Remove the postfix MTA running in default openSUSE installation: `sudo zipper remove postfix`
4. Download Kerio Connect 7.1 installation package in RPM format from [Kerio website](#).
5. Install Kerio Connect using the following command: `sudo rpm -i kerio-connect-7.3.0-xxxx.linux.rpm`
6. Finish the initial server configuration using the CfgWizard application: `sudo /opt/kerio/mailserver/cfgwizard`
7. Start Kerio Connect using the following command: `sudo /etc/init.d/kerio-connect start`
8. Optionally, replace sendmail with the binary from the Kerio Connect:
`sudo mv /usr/sbin/sendmail /usr/sbin/sendmail-old`
`sudo cp /opt/kerio/mailserver/sendmail /usr/sbin/sendmail`
`sudo cp /opt/kerio/mailserver/libkt* /usr/lib/`

Since, Kerio Connect is now installed and configured. You can access web administration interface at <https://localhost:4040>. Also, don't forget to configure your DNS server and add proper A and MX records for the server.

NOTE

Kerio Connect users can be authenticated against PAM with /etc/pam.d/keriomail PAM module.

2.8.4 Installation on openSUSE 11.4 – 64-bit (x86_64)

You can install Kerio Connect 7.3 on openSUSE 11.4 (amd64).

1. Get the installation ISO images of openSUSE 11.4 for x86_64 platform from www.opensuse.org.
2. Install openSUSE 11.4 base system.
3. Remove the postfix MTA running in default openSUSE installation: `sudo zipper remove postfix`
4. Download Kerio Connect 7.3 installation package in RPM format from [Kerio website](#).
5. Install Kerio Connect using the following command: `sudo rpm -i kerio-connect-7.3.0-xxxx.linux.rpm`
6. Finish the initial server configuration using the CfgWizard application: `sudo /opt/kerio/mailserver/cfgwizard`
7. Start Kerio Connect using the following command: `sudo /etc/init.d/kerio-connect start`
8. Optionally, if you want to use PAM for authenticating users in Kerio Connect, install 32-bit PAM libraries: `sudo zypper install pam-32bit`
9. Optionally, replace sendmail with the binary from the Kerio Connect:
`sudo mv /usr/sbin/sendmail /usr/sbin/sendmail-old`
`sudo cp /opt/kerio/mailserver/sendmail /usr/sbin/sendmail`
`sudo cp /opt/kerio/mailserver/libkt* /usr/lib/`

Since, Kerio Connect is now installed and configured. You can access web administration interface at <https://localhost:4040>. Also, don't forget to configure your DNS server and add proper A and MX records for the server.

NOTE

Kerio Connect users can be authenticated against PAM with /etc/pam.d/keriomail PAM module.

2.8.5 Joining Kerio Connect running on Linux to Open Directory or Active Directory

Both Active Directory and Open Directory offer directory services which can be configured to work with Kerio Connect running on Linux. This article describes how to perform this configuration.

Assumptions

Before you begin this article, the following must be true:

1. A properly configured and working Active Directory or Open Directory domain.
2. Valid DNS records for your AD or OD domain.
3. A properly configured and working Kerio MailServer installation on a supported version of Linux

Choose the appropriate setup for your network from the options below and follow the steps in the specified order:

Open Directory

1. Preparing Open Directory for Kerberos
2. Obtaining the Kerberos Realm and DNS Names in Open Directory
3. Configure the /etc krb5.conf file
4. Calibrate the time
5. Join Kerio Connect to the Open Directory Service
6. Troubleshooting
7. Linux Packages

Active Directory

1. Obtaining the Kerberos Realm and DNS Names in Active Directory
2. Configure the /etc krb5.conf file
3. Calibrate the time
4. Join Kerio Connect to the Active Directory Service
5. Troubleshooting
6. Linux Packages

Preparing Open Directory for Kerberos

Linux uses a technology called Kerberos for directory services security. Support for Kerberos in Open depends on your version of OS X.

Mac OS X 10.5.x and Mac OS X 10.6.x

On these versions, Open Directory is configured for Kerberos by default. To verify that Kerberos is working, follow these steps:

1. On the Open Directory server run Server Admin.
2. Under **Computers & Services** choose the Open Directory server.
3. The **Overview** page should show the message, "Kerberos is: Running."

If you do not see message, it must be configured and started.

- » For more information, see section, **Setting Up Open Directory Services** in [Open Directory Manual for Mac OS X 10.5](#).
- » For more information, see section, **Setting Up Open Directory Services** in [Open Directory Manual for Mac OS X 10.6](#).

Mac OS X 10.7.x and 10.8.x

Versions of Mac OS X 10.7 and 10.8 server have changed quite a bit, please see the following Apple documentation:

- » [Mac OS X 10.7: Manage Users > Open Directory Services](#)
- » [Mac OS X 10.8: Manage Users > Open Directory Services](#)

Obtaining the Kerberos Realm and DNS Names

Learn how to obtain the Kerberos Realm and DNS Names in Active Directory and Open Directory, respectively.

Obtaining the Kerberos Realm and DNS Names in Active Directory

To obtain the Kerberos Realm and DNS Names in Active Directory, perform the following steps:

1. Open **Programs- > Administrative Tools- > Active Directory Management**.
2. Choose **Active Directory Domains and Trusts**.
3. The Active Directory domain names are listed.

The Active Directory domain name is also the corresponding Kerberos realm name and DNS domain name. Pick the domain you want to join the mailserver to. Always use the Kerberos realm name in upper case letters and the DNS domain name in lower case letters.

Obtaining the Kerberos Realm and DNS Names in Open Directory

The Kerberos realm name and DNS domain name will already be known if it was necessary to setup Open Directory for Kerberos .

If Open Directory is already running Kerberos, then use the following process:

1. Open a terminal as an admin user
2. Enter the following command:

```
sudo grep -A 2 domain_realm /Library/Preferences/edu.mit.Kerberos
```

Example:

```
tiger:~ root# grep -A 2 domain_realm /Library/Preferences/edu.mit.Kerberos [domain_realm] .example.mac = TIGER.EXAMPLE.MAC example.mac = TIGER.EXAMPLE.MAC tiger:~ root#
```

In this example, The DNS domain name is on the left of the equals (=) symbol, and the Kerberos realm name is on the right.

NOTE

Always use upper case letters when referring to the Kerberos realm name even if you've seen it in lower case letters on the server. Always use lower case letters when referring to the DNS domain name. It prevents confusion since they are often the same in many networks.

Configuring krb5.conf file

NOTE

This information is specific to a mailserver on Linux. If your mailserver is on Mac OS X Server, you can achieve this by simply joining the machine properly to Open Directory. If you face any problem in joining, take a look at the [Troubleshooting](#) section for information on the `kinit` command that is used to test authentication.

The `/Library/Preferences/edu.mit.Kerberos` file on your Open Directory master is a **krb5.conf** file. You can copy this file from the Open Directory master to the Linux machine running Kerio Connect and use it as the `/etc/krb5.conf` file.

For example, in linux:
linux:~# cd /etc
linux:/etc# scp
opendirectoryserver:/Library/Preferences/edu.mit.Kerberos./krb5.conf
replace opendirectoryserver with the hostname of your Open Directory server.

Step-By-Step Configuration of the /etc/krb5.conf File on Linux

A much more detailed description of the **/etc/krb5.conf** file is available on the official Kerberos website [Kerberos: Configuration Files/krb5.conf](#).

For Active Directory or Open Directory with a more complicated network (such as multiple Kerberos realms) it is necessary to configure the existing **krb5.conf** file or create one from scratch. Linux is distributed with a **/etc/krb5.conf** file that contains references to EXAMPLE.COM as follows:

A typical default **/etc/krb5.conf** file on Linux looks something like this:

```
[libdefaults] default_realm = EXAMPLE.COM dns_lookup_realm = false dns_lookup_kdc =  
false [realms] EXAMPLE.COM = { kdc = kerberos.example.com:88 admin_server =  
kerberos.example.com:749 default_domain = example.com } [domain_realm] .example.com =  
EXAMPLE.COM example.com = EXAMPLE.COM
```

Edit the file parameters using the following instructions:

Parameter	Instructions
[libdefaults]	Set default to the Kerberos realm name for your network. For example, for realm name KERIO.COM the script would look like: <pre>[libdefaults] default_realm = KERIO.COM dns_lookup_realm = false dns_lookup_kdc = false</pre>
[realms]	Each "realm" is listed as a realm name in upper case letters equals symbol and then a small section enclosed in curly braces as shown in the example above. 1. Change the EXAMPLE.COM realm name to correct Kerberos realm name or if no example realm exists, copy the one from the example krb5.conf file shown above. 2. Each realm contains "kdc" and "admin_server" values. Set those to the fully qualified DNS hostname of the Open Directory or Active Directory server. 3. Set the default_domain to the DNS domain name bound to the realm. 4. There can be multiple realms so Kerio MailServer can have multiple mail domains joined to different Kerberos realms. Example: for realm KERIO.COM, Open Directory master master.kerio.com, and DNS domain kerio.com <pre>[realms] KERIO.COM = { kdc = master.kerio.com:88 admin_server = master.kerio.com:749 default_domain = kerio.com }</pre>
[default_realm]	This section simply contains DNS domain name, equals symbol, then Kerberos realm name then another line identical except with a preceding dot as shown in the example above. 1. Change each instance of EXAMPLE.COM to your Kerberos realm name in upper case letters. 2. Change each instance of example.com to your DNS domain name that is bound to the corresponding Kerberos realm. 3. There can be similar entries in this section for other domains and their respective realms so Kerio MailServer can have different mail domains joined to different Kerberos realms. For example, if realm is KERIO.COM and the DNS domain is kerio.com: <pre>[default_realm] .kerio.com = KERIO.COM kerio.com = KERIO.COM</pre>

Calibrating the time

The difference between the clock on the Linux server and the clock on the AD or OD directory master server ('domain controller') must not be more than 5 minutes (300 seconds).

There can be problems if the **[libdefaults]** section of the **krb5.conf** file contains an entry called **clockskew** and it is set to a very low value. The default for this value is 300.

Calibrating the clocks without a working NTP network can be difficult if this value is set too low. If the domain controller and Kerio MailServer computers are not calibrated by NTP, then remove this value if it exists. If they are calibrated by NTP but you still cannot authenticate, try increasing the value.

Joining Kerio Connect to a Directory Service

Read our knowledge-base article [Setting of Directory Services](#) to learn how to join Kerio Connect to a directory service.

NOTE

Be sure to check the domain search suffix.

For a domain such as **ad.example.com**, the search suffix should be `dc=ad, dc=example, dc=com`, but sometimes it will only show as `dc=example, dc=com`. This will prevent Active Directory authentication from working. Insure that it is correct for your domain name.

Troubleshooting authentication issues

A command called `kinit` is available in the command prompt on either Linux or Mac (any version). This command is used to issue Kerberos queries and can confirm if Kerio authentication should work. Here are the two ways you can run this command to test authentication.

Method 1

Run the following command:

```
kinit username
```

When running, replace `username` by a valid user on the directory server such as `diradmin` or `administrator`. It will prompt you for a password, and would return no errors if it works.

Method 2

It is recommended to also run this command even if the previous `kinit` command worked. As there still might be a problem with the **SMP** host. For example when testing on `mail.company.com`, the command would look like:

```
kbd>kinit -S host/mail.company.com@SERVER01.COMPANY.COM
```

Note that this will throw a Kerberos error if the mailserver machine is not properly joined. In this command, `mail.company.com` is the hostname of the mailserver, and `SERVER01.COMPANY.COM` is the kerberos realm name.

Ensure that the DNS on the Linux mailserver is pointed to the DNS server provided by the Active Directory or Open Directory server.

Many Kerberos issues are actually problems in DNS. The best policy is to always use the DNS provided by the directory service. Using 3rd party DNS is possible, but is not recommended and involves some configuration that is beyond the scope of this document. If it is not possible to use the correct DNS server, then be sure the correct DNS forwarding is configured so queries are still answered by the directory server machine.

For Kerberos problems in Open Directory that might be caused by DNS, visit the following article from Apple and go to chapter 10: [Kerberos is Stopped on an Open Directory Master or Replica](#).

Essentially, the same steps provided in the Apple document apply to DNS on Active Directory as well.

If users still cannot authenticate to Kerio MailServer, yet there are no errors except password failures, then it is possible the **keytab file** is damaged. The keytab file is a special file used by Kerberos. The keytab file is more likely to get messed up in Open Directory than with Active Directory because Open Directory does not always depend on Kerberos whereas Active Directory depends on it for everything.

Linux Packages for using Kerberos

The correct packages for using Kerberos are distributed with most modern linux systems. However, if for some reason they are somehow missing, try installing the following packages:

- » pam_krb5-1.31-1, krb5-libs-1.2.2-4
- » krb5-workstation-1.2.2-4

NOTE

These versions will change over time.

2.8.6 Kerio Connect Virtual Appliance Networking (Debian Edition - Kerio Connect 7.3.x and later)

This topic provides information on networking for the Kerio Connect VMware virtual appliance.

NOTE

This information is provided 'As Is' and that Kerio Technical Support will only be able to help with default values.

First ensure that you are running the Debian variant of Linux. There are several ways to do this, we recommend the use of the following command:

```
uname -a
```

The output from this command displays the linux type.

If you are using CentOS, refer to the following [topic](#) instead.

Prerequisites

The configuration details outlined below require terminal access with the root user.

Working in the console

At the Virtual machine Console Press Alt+F2 to switch the visible console to another terminal (tty) screen within the Virtual machine management Interface.

Where prompted, log in as "root" (without the quote marks). To start with, the default password is "kerio" (without the quote marks). You will be forced to change the password upon first login. Please keep your new password safe, as a forgotten password can NOT be recovered!

Updating the System

Log on to the system console.

First we need to make sure that the operating system is up to date, there are two commands to run to do this:

```
apt-get update  
apt-get dist-upgrade
```

Working with the Firewall

Kerio Connect Virtual Machine contains a powerful iptables firewall, this is installed on all Linux Servers.

Administrators may use the "ufw" tool to control iptables firewall

You can either set all traffic defaults to allow:

```
ufw default allow
```

Or, turn it off altogether:

```
ufw disable
```

Or you can allow traffic to a specific port:

```
ufw allow 8989
```

NOTE

For more details please see, <http://help.ubuntu.com/community/UFW>.

Checking and Editing Virtual Network Adapter Settings.

Linux virtual machines on ESX/ESXi 4.1 using the vmxnet3 virtual adapter may experience a loss of network connectivity when the virtual NIC switches between offline and online.

This may also effect networking Link Speed.

Kerio Connect Virtual Machine is based on Linux.

/var/log/messages or dmesg may contain entries similar to:

```
kernel: eth0: tq_error 0x80000000
kernel: eth0: resetting
kernel: eth0: intr type 2, mode 0, 1 vectors allocated
kernel: eth0: NIC Link is Up 10000 Mbps
```

Disable TSO if you are experiencing the above.

1. Log in as root to the terminal.

2. To determine the device name of your virtual network card, run the command: `ifconfig`

3. To determine your current TSO setting for that adapter, run the command: `ethtool -k eth1`, where **eth1** is the vmxnet3 adapter based on ifconfig output from step 3.

4. To disable TSO, run the command: `ethtool -K eth1 tso off`

NOTE

TSO is used to reduce CPU overhead on TCP/IP. Disabling TSO may cause higher CPU during high network traffic.

2.8.7 How to make PHP's mail() command work with Kerio MailServer on Linux

For Ubuntu

Look for the `sendmail_path` setting in the **/etc/php.ini** file. By default, it is set to `/usr/sbin/sendmail -t -i`.

You can replace the original sendmail with the Kerio version using the following commands:

```
sudo apt install sendmail
sudo apt install mailutils
cd /usr/sbin
mv ./sendmail ./sendmail-orig
cp /opt/kerio/mailserver/sendmail .
```

```

cp /opt/kerio/mailserver/libktssl.so.1.0.0 /usr/lib
cp /opt/kerio/mailserver/libktz.so.1 /usr/lib
cp /opt/kerio/mailserver/libktcrypto.so.1.0.0 /usr/lib

```

You can test by executing this command for Test email:

```
echo "test" | mail admin@youdomain.com
```

For RHEL or CentOS

```

# yum -y install sendmail
# yum -y install mailx
cd /usr/sbin
mv ./sendmail ./sendmail-orig
cp /opt/kerio/mailserver/sendmail .
cp /opt/kerio/mailserver/libktssl.so.1.0.0 /usr/lib
cp /opt/kerio/mailserver/libktz.so.1 /usr/lib
cp /opt/kerio/mailserver/libktcrypto.so.1.0.0 /usr/lib
/sbin/ldconfig -v

```

You can test by executing this command for Test email:

```
echo "test" | mail admin@youdomain.com
```

2.8.8 Working with the Kerio Connect Virtual Appliance (CentOS Edition - Kerio Connect 7.2.x and earlier)

IMPORTANT

This information is provided 'As Is' and Kerio Technical Support will not be able to help you further if you have any problems.

First ensure that you are running the CentOS variant of Linux. You can use the following command: `sb_release -a`. The output from this clearly displays the linux type. If you are using Debian, refer to [this topic](#) instead.

With Kerio Connect 7.2.x and earlier, the Kerio Virtual Appliance comes with CentOS as an operating system. In order to minimize the size of this Virtual Appliance, there are some helpful debugging tools that are not part of the operating system and you may need to install them manually.

You can use the Synaptics program from the graphical desktop of your server to install these tools, or you can do so from a command line as follows:

Program	Description	Installation Command
Telnet	Helpful tool for testing connectivity to a network socket and issuing commands.	<code>yum install telnet</code>
Dig	DNS tool to lookup hostnames.	<code>yum install bind-utils</code>
Nano	Simple text editor.	<code>yum install nano</code>
VNC server	Remote Desktop server, to enable remote access to the server.	<code>yum install vino</code>

In case of **VNC server**, the following additional configuration is required:

- » Accessing the preferences and enabling remote desktop.
- » Setting up a VNC password that can be different to your Kerio Connect admin password.

You can access Configuration using the following command: `vino-preferences`

You can check that the Vino server runs using the following command: `lsof -i -n -P`

Post installation, look for this line `vino-serv 1818root17uIPv4110090t0TCP *:5900 (LISTEN)` as it tells you that Vino uses port 5900 to allow access to the server desktop.

The Kerio Connect VM comes with a firewall **IPTables**. You can configure it through a terminal to allow port 5900 through using the following command: `iptables -A INPUT -p tcp --dport 5900 -j ACCEPT`.

Or, you can disable IPTables altogether, using the following command: `iptables -F`

Finally, test your connection with a program like realVNC or UltraVNC on a Windows machine, or Chicken of the VNC on a Mac. You need to enter your server address as follows: <server.name>::5900

NOTE

There are two colons :: in the address. The server name is the host name of your mailserver and the 5900 comes from the lsof output you obtained earlier.

2.8.9 Working with the Kerio Connect Virtual Appliance (Debian Edition - Kerio Connect 7.3.x and later)

Learn how to use Kerio Connect VMware virtual appliance.

IMPORTANT

Please note that this information is provided 'As Is' and that Kerio Technical Support will not be able to help further if you have any problems.

- » Run the Debian variant of Linux. If you see a blue Kerio screen after Kerio Connect is installed, this is out Debian version.
- » If you use the CentOS version, or do not see the blue Kerio screen after the installation, refer to [this topic](#).

Kerio Connect is running on this computer. To change settings, please point your browser to:

<https://192.168.64.183:4040/admin/>

<Enter> Access Console

Initial configuration

- » The Kerio Connect Virtual Appliance is pre-installed with a standard Debian Linux 32-bit distribution.
- » When you start the appliance for the first time, fill in the information regarding your Kerio setup in the configuration wizard .

Working with the console

- » You can press **Alt + F2** to switch the visible console to another terminal (tty) screen.
- » You can Log in as **root**. The default password is **kerio**. Change the password after the first login. Forgotten password cannot be retrieved.

Enabling SSH

Kerio Connect 7.4 and newer

You can enable the SSH client directly from the Kerio Connect console.

Kerio Connect 7.3 and older

SSH access is disabled by default. To enable remote SSH access, follow these steps:

1. Log in to the system console.
2. Configure the SSH daemon to start automatically on system startup using the following command:
`update-rc.d ssh defaults`
3. Start the SSH daemon using the following command:
`/etc/init.d/ssh start`

Point your SSH client to the IP address of the server (TCP port 22). Log in as user **root** and the new root password you created.

Changing the server time settings

Kerio Connect 7.4 and newer

You cannot set the time settings in the Kerio Control console.

Kerio Connect 7.3 and older

The default system timezone is UTC (GMT +0). To change it, follow these steps:

1. Log in to the system console.
2. Configure the timezone using the following command: `dpkg-reconfigure tzdata`
3. Reboot the server using the following command: `reboot`

Changing the firewall settings

1. Access the system console.
2. Edit the firewall configuration file **/etc/ufw/kerio-connect.ufw** using a text editor. For example: `vi /etc/ufw/applications.d/kerio-connect.ufw`
3. In the **ports=** section, add ports you want to open. For example: `ports=80 | 25 | 110 | 443`
4. Reload the firewall with the following command: `ufw app update kerio-connect`

NOTE

If you're changing firewall rules remotely over SSH, restart the firewall service with `/etc/init.d/ufw restart`. This will likely interrupt your current SSH session and you will need to reconnect if you have further work to do.

Using the Kerio IMAP Migration Tool

Due to the firewall built into the virtual system, you must change the firewall to allow the IMAP Migration Tool to work (see section [Changing the firewall settings](#)).

1. Change the firewall settings to allow the IMAP Migration Tool to work (see section [Changing the firewall settings](#)).
2. Access the system console.
3. Run the following command: `ufw allow 44337`

Upgrading Kerio Connect manually

For more information, refer to [Upgrading from versions older than Kerio Connect 8.0.0](#) (page 40).

You must download two packages:

- » Kerio Connect (**Kerio Connect - Linux (DEB)**), and
- » Kerio Connect virtual appliance console (**Kerio Connect VA Console - Linux (DEB)**).

1. Go to the [Kerio downloads page](#) and select the latest version of Kerio Connect.
2. Copy the URLs of the two packages.

3. Login to the system console and download the packages: `wget http://download.kerio.com/dwn/kerio-xxxxxx.deb`
4. Install both files.

Alternative method

1. Download the two files to your desktop.
2. Use SFTP (see section [Enabling SSH](#)) to upload the files directly to your Kerio Connect server.
3. Log in and place the files in the home directory.
4. Install the two files. (For more information, refer to [Upgrading from versions older than Kerio Connect 8.0.0](#) (page 40).)

Setting up Kerberos user authentication against Active Directory

1. Log in to the system console.
2. Install Kerberos 5 packages: `apt-get update apt-get install krb5-config krb5-user`

NOTE

For Kerio Connect 8.5 and older, install the following packages: `apt-get install krb5-clients krb5-config krb5-user`

3. In the Kerberos 5 configuration wizard, configure the Kerberos realm and domain server hostname.
4. Add new computer to your Active Directory. Use the same hostname as defined in the appliance (run `hostname -f` to display the hostname). If you set up a wrong hostname, change the following configuration files: `/etc/hostname` and `/etc/hosts`.
5. Add the Service Principal Name for the computer to the Kerberos database. Run the following command on your Windows Active Directory (master): `setspn.exe -R hostname`
6. Verify that Kerberos works. Run the following command on your Kerio Connect console: `kinit -s host/<hostname_domain.com>@<DOMAIN.COM>`
 - `<hostname_domain.com>` — the appliance hostname and corresponds to the computer name in the Active Directory
 - `<DOMAIN.COM>` — the Kerberos realm used in your Active Directory

For information on importing users from Active Directory, read [this article](#).

Adding a new disk to the virtual appliance

IMPORTANT

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

To increase available disk space for the message store, you can add a second virtual hard disk 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. To check whether Debian installed and picked up your new hard drive, run the following command: `fdisk -l`. The disk at `/dev/sdb` is picked up and there are no partitions.
4. Create a new partition on your new drive: `cfdisk /dev/sdb`. The cfdisk controller will load up and here you can create a new partition on your drive. From the menus at the bottom select the following:

- a. **New > Primary > Size in MB**.
- b. Select **Write**.
- c. Select **Quit**. Your new partition is created at `/dev/sdb1`.

5. Format the new disk: `mkfs.ext3 /dev/sdb1`. This command formats the partition with the ext3 filesystem which should work fine for your Debian system.

6. Mount the drive: `mkdir /store` (to create a directory for the drive), `mount -t ext3 /dev/sdb1 /store` (to mount the drive to this directory). Check the drive is mounted — `ls -la /store`.

Everything is now up and running. However, you must add the new drive to `/etc/fstab` so that it is mounted automatically when the server reboots.

1. Open the `fstab` file: `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 disk

1. Stop the Kerio Connect server by running the following command: `sudo service kerio-connect stop`
2. Copy all data from the old message store: `cp -R -p /opt/kerio/mailserver/store/* /store`
3. Change the message store directory path in the Kerio Connect configuration: `sed -i -e "s/\//opt\kerio\mailserver\store\store/" /opt/kerio/mailserver/mailserver.cfg`
4. Start Kerio Connect server with: `sudo service kerio-connect start`

Setting log rotation

Due to the limited disk size in the virtual appliance, set log rotation for log files by size with limited number of files.

For more information, refer to [Managing logs in Kerio Connect](#) (page 215).

Adding system locales

System locales are necessary for supporting WebMail clients in different languages (correct text sorting etc.).

Kerio Connect 7.4 and newer

System locales are added automatically as needed.

Kerio Connect 7.3 and older

By default, only **en_US.UTF-8** is installed. To add additional locales, follow these steps:

1. Log in to the system console.
2. Run the configuration wizard for the locales: `dpkg-reconfigure locales`
3. Select the locale you want to install.
4. Select a default system locale.
5. Confirm.

NOTE

Always use the UTF-8 version (e.g. cs_CZ.UTF-8, de_DE.UTF-8 etc)

Modifying system locales

By default, the server uses the **en_US.UTF-8** system locales for programs and services.

To change the system locales, follow these steps:

1. Log in to the system console.
2. To change the locale to, for example, German, run the following command: `sudo update-locale LANG-G=de_DE.UTF-8 LC_MESSAGES=POSIX`

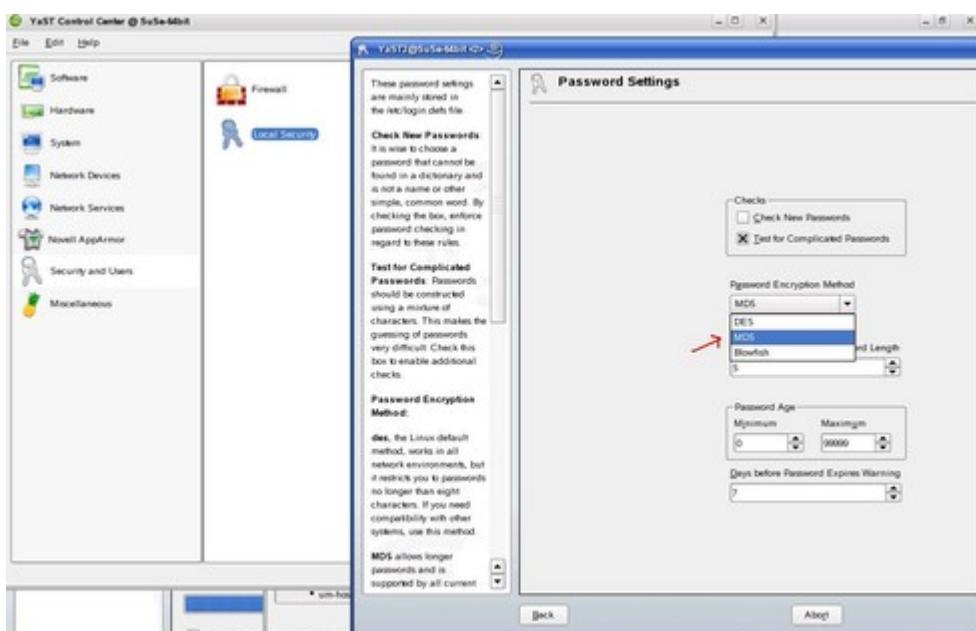
To get a list of available locales, run `locale -a` in the system console.

2.8.10 PAM authentication is not working in SuSE

In SuSE 10 it is possible to set the user's password encryption type. The supported encryption types are Blowfish and MD5. Kerio MailServer requires MD5 encryption for PAM users.

It is possible to set the encryption type during system installation or in the configuration file **/etc/default/passwd**. The encoding type is stored in line CRYPT_FILES, where Kerio MailServer needs MD5 encryption.

You can also use the graphical interface YaST for the configuration as shown on following picture:



Users created with the Blowfish password encryption need to change their password after this change. After the password change is complete the new password is saved using the MD5 encryption type.

The algorithm used for password encryption can be found in the **/etc/shadow** file:

- » DES (without prefix), ex.: abJnggxhB/yWI
- » MD5 (prefix \$1\$), ex.: \$1\$L/321sYmS\$ygf8.6wKiHfNF3rir2ca/
- » Blowfish (prefix \$2a\$), ex.: \$2a\$12\$23Yu.28Gxz8bB41WCbPXF.s5NeH5TPb-tLdtIkIQZwS1XajF5uuUnK

For reference SuSE 10 uses the Blowfish algorithm by default, while other distributions usually use MD5.

2.9 Hosting

Kerio Connect is a server application for Mac, Linux, and Windows operating systems that provides business-class email, instant messaging, scheduling, and task management via secure web access to a variety of mobile devices, web browsers, and desktop applications. As a possible deployment option you can host multiple independent organizations (tenants) on a single Kerio Connect server. This type of deployment is referred to as multitenancy.

Use these links to know general information and suggested configuration regarding the deployment of Kerio Connect in a hosting environment using multitenancy.

2.9.1 Preparing an environment for Hosting	112
2.9.2 Configuring Kerio Connect for multitenancy	113
2.9.3 Assigning domain level rights to tenant accounts	113
2.9.4 Differentiating services to tenant accounts	114
2.9.5 Branding your service	115
2.9.6 Automating configuration via Kerio Connect API	115
2.9.7 Protecting the server from mail abuse	116
2.9.8 Preparing the server for client access	116

2.9.1 Preparing an environment for Hosting

Kerio Connect is suitable for hosting approximately 300 mailbox accounts on a single system. For larger deployments, you can distribute mailboxes to multiple Kerio Connect servers. If you require more than 300 mailboxes in a single domain, consider [Kerio Connect multi-server](#). Refer to the [technical specifications](#) for information regarding the recommended system requirements and sizing information.

To maximize the efficiency and availability of your hosting environment consider the following:

- » A secure and reliable data center with redundant power and Internet.
- » Servers designed specifically for virtualization.
- » A virtualization platform.
- » An operating system optimized for your preferred virtualization platform.
- » Fast and scalable primary storage.
- » Inexpensive secondary storage for data backup and archiving.

If you find that obtaining or leasing proper hosting infrastructure is either challenging or cost prohibitive, consider alternative options such as [Kerio Private Cloud](#).

2.9.2 Configuring Kerio Connect for multitenancy

Follow the [Kerio Connect Quick Start](#) to prepare for the general installation and setup of Kerio Connect. For a multi-tenant environment you may need to set up specific types of configuration as described here:

SaaS Licensing

In a hosted multi-tenant environment it is common that the user count may frequently fluctuate. To accommodate this behavior Kerio Connect supports a SaaS license that permits the use of a non-restricted user count. Details regarding the SaaS licensing program are available to registered Kerio partners in the [Kerio Partner Portal](#).

Creating tenants

Kerio Connect separates tenants using domains. Each domain contains a unique set of users, groups, mailing lists, aliases, resources, and public folders. For more information, refer to [Domains in Kerio Connect](#) (page 248).

Personalizing tenant accounts (domains)

In the properties of each domain you can define several types of configuration that apply only to authenticated users of the domain.

Configuration Type	Description
SSL Certificates	You can personalize the connection parameters for each tenant by assigning a SSL certificate per domain. This allows users to connect securely to the server using a personalized Uniform Resource Identifier (URI). Refer to Configuring SSL certificates in Kerio Connect for information about using multiple certificates in Kerio Connect.
Custom logo	Each tenant can have a custom logo so that users can associate with their corporate brand when using Kerio Connect Client.
Email footer	Kerio Connect can append a common footer with rich formatting and images to all outbound email from a specific domain.

Refer to [Customizing Kerio Connect](#) for configuration details regarding custom logos and email footers.

2.9.3 Assigning domain level rights to tenant accounts

Domain administration enables domain level management for a designated user thus restricting full server administration.

You can designate domain level administrative rights to any user of a domain.

Username	Full Name	Description
akim	Arlene Kim	Research Analyst
bburrow	Brock Burrow	Accounting executive
cpage	Cathy Page	Legal Counsel
gtownsend	Gloria Townsend	HR Director
jdoll	Jacqueline Doll	IT Director
jmcmillian	Jolie Mcmillian	Vice President of Operations
mhess	Miles Hess	Director of advertising
npineda	Nicolas Pineda	PR Manager
wharrison	Wesley Harrison	Director of business development

Screenshot 5: Delegating domain level administration

Refer to [Assigning admin rights to individual users](#) for information about domain level administration.

2.9.4 Differentiating services to tenant accounts

As a hosting provider you may want to support varying service levels to offer a tiered pricing model that accommodates a broad range of customer preferences. Kerio Connect supports several options to enable differentiated features and functionality at the user and domain levels.

Assigning user access policies

You can associate users with access policies to limit the type of services, protocols, or applications they are allowed to use. For more information, refer to [Restricting access to some services](#) (page 405).

Setting domain limits and quotas

In the properties of each domain you can set limits and quotas to enforce usage requirements as part of your hosting services.

Domain Property	Description
User count	Set a limit on the number of users in a domain. This option prevents domain level administrators from creating more users than may be allowed. For more information, refer to Limiting the number of users per domain (page 252).
Chat	Disable chat per domain so that you can offer chatting in Kerio Connect Client as a premium option. For more information, refer to Enabling chat in Kerio Connect Client (page 187).
Disk space	Assign a cumulative storage limit to all users and public folders within a domain so that you can enforce storage limits and offer larger storage capacities as a premium option. For more information, refer to Limiting the disk space per domain (page 253).

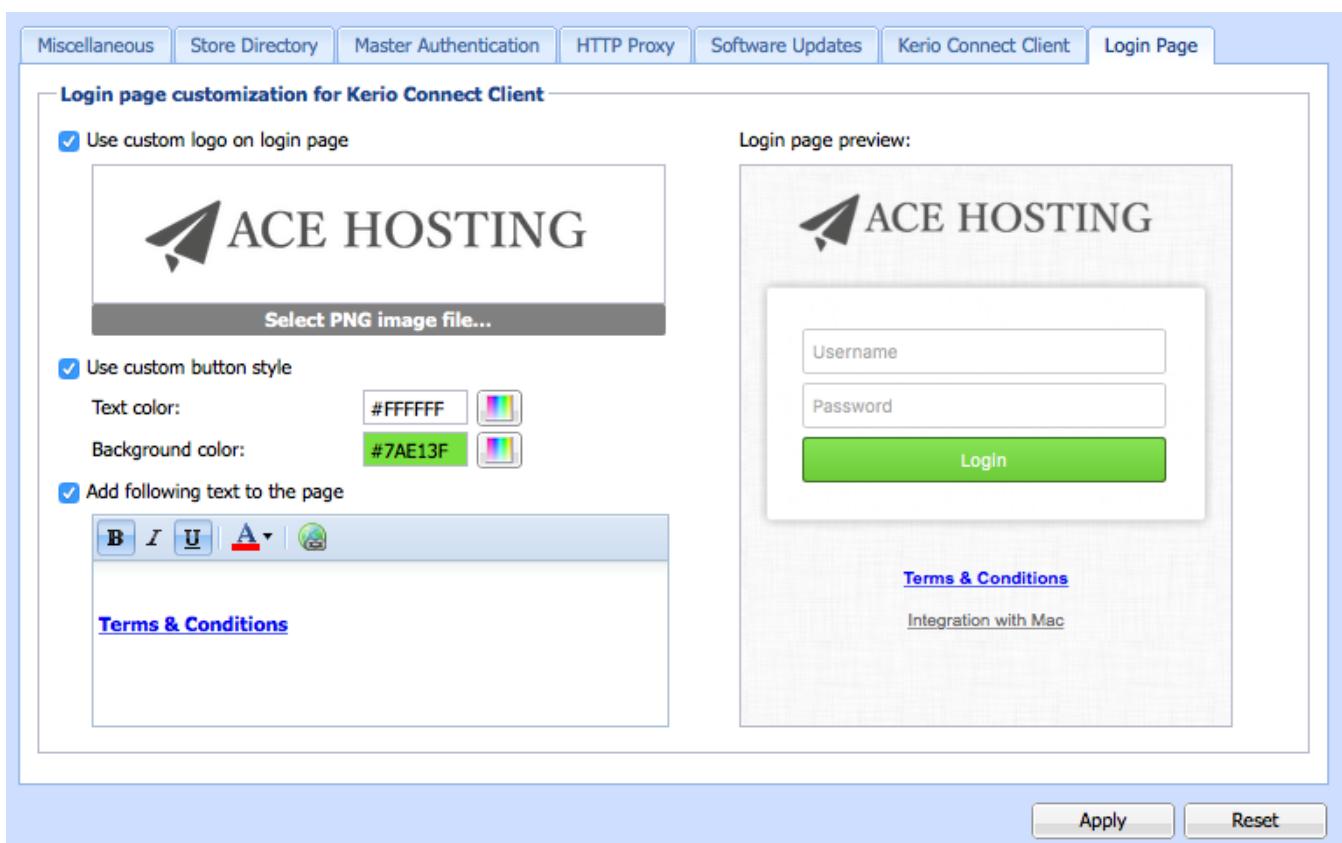
Domain Property	Description
Outgoing message size	Restrict the size of outgoing messages from a specified domain. Assign larger message sizes as a premium option. For more information, refer to Limiting the size of outgoing messages (page 278).
Deleted items recovery	You can enable retention of deleted messages for an acceptable interval such as 30 days. The process for recovering deleted messages is a faster and less disruptive option than recovering data from a backup and may be used as a premium option. For more information, refer to Recovering deleted items (page 277).

Relaying email through alternative services (smart host)

You can use alternative mail relay services for various purposes such as data loss prevention (DLP), archiving, or compliance. To achieve this, you can create conditional rules to relay outgoing messages from or to specific domains through an external server. For more information, refer to [Sending outgoing messages through multiple servers](#) (page 408).

2.9.5 Branding your service

In a hosting environment, you can customize the login page of Kerio Connect as per your identity. This enables you to match the login experience with your company brand.



Screenshot 6: Branding

For more information, refer to [Customizing the Kerio Connect Client login page](#) (page 222).

2.9.6 Automating configuration via Kerio Connect API

In a multi-tenant hosted environment, you may use additional software to manage tenant accounts for billing, accounting, and administration. You can simplify this management by automating tasks and integrating with your

management software using the Kerio Connect API. Example usage of the Kerio Connect API includes:

- » Retrieve the mailbox size of a user or the number of users in a domain.
- » Add or remove a user or domain
- » Modify user or domain properties
- » Create or modify a mailing list

Learn more about the API in the [Kerio developer zone](#).

2.9.7 Protecting the server from mail abuse

To optimize server utilization in a hosting environment you may decide to occupy your servers with the maximum number of recommended mailbox accounts. In this situation it is important to enforce storage quotas, strong passwords, and email delivery restrictions to prevent abuse and ensure uninterrupted operation.

Setting storage quotas

Set user mailbox storage quotas to prevent excessive accumulation of email. This improves the server performance and encourages users to transfer large files via alternative services. For more information, refer to [Limit the size of user mailboxes](#) (page 280).

Assigning email delivery restrictions

In a multiserver environment all tenants share the same bandwidth and server resources. To ensure fast and reliable access to these resources you can assign SMTP security options such as the maximum number of messages per hour or the maximum size of an incoming message. For more information, refer to [Securing the SMTP server](#) (page 411).

Enabling items clean-out

You can prevent users from retaining discarded or spam email by enabling items clean-out. Items clean-out preserves space and server processing by removing old messages from the trash or spam folders. For more information, refer to [Deleting old items in users' mailboxes automatically](#) (page 275).

Enforcing password complexity

Kerio Connect protects mailbox accounts by enforcing strong passwords and prohibiting password guessing. In a multi-tenant environment it is extremely important to maintain this setting as a single compromised account can be extremely disruptive to mail delivery for all users of the server. For more information, refer to [Password policy in Kerio Connect](#) (page 329).

2.9.8 Preparing the server for client access

In a hosting environment you may not have the ability to assist users with the setup of desktop and mobile applications for mailbox access. You can use various technologies and services to simplify the user experience for mailbox setup and access.

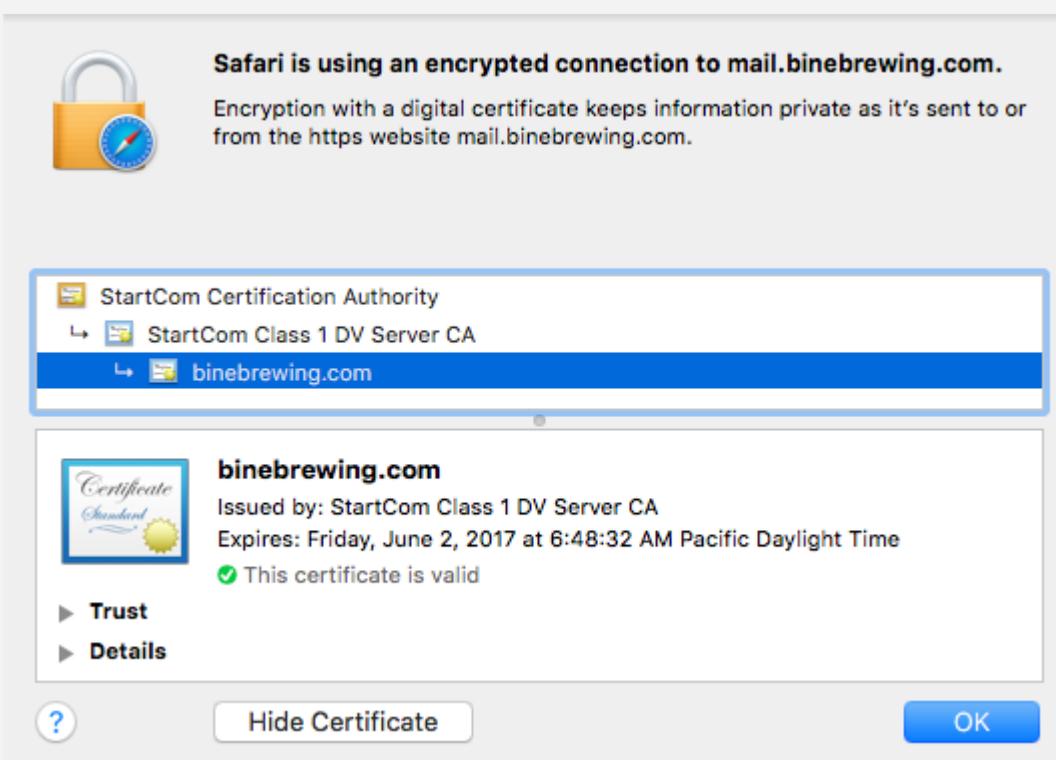
Configuring DNS for automatic account configuration

Many messaging applications use Autodiscovery to simplify the configuration of accounts. You can enable this technology in Kerio Connect through proper DNS configuration. Refer to [Configuring Autodiscover in Kerio Connect](#) and [Configuring DNS for instant messaging](#) for details.

Enabling secure remote access to services

In a hosting environment client applications can access Kerio Connect services from insecure networks. In order to maximize security you can set policies to enforce encrypted and secure methods of remote access.

Service	Description
SSL redirection and enforcement	Kerio Connect can redirect users to the secure version of the web services and prevent insecure connections. This ensures secure connectivity and prevents the possibility of eavesdropping. For more information, refer to Configuring a secure connection to Kerio Connect (page 325)..
SMTP Submission	The Simple Message Transport Protocol (SMTP) protocol is commonly filtered or blocked in residential and public Internet locations. An extension to SMTP called submission uses an alternate port (587) and enables users to authenticate and subsequently relay mail without the same layers of filtering. Make sure this service is available to your server to improve email delivery for your users..
Certificate Authority (CA) signed certificates	Kerio Connect includes a self-signed SSL certificate, however most applications prompt users with disruptive warnings when connecting to secure services that do not have a certificate signed by a trusted authority.



Screenshot 7: Prompt for a signed certificate

For more information, refer to [Creating certificates signed by a certification authority](#) (page 379).

2.10 OS X

Learn about various Kerio Connect features and configurations specific to OS X operating systems.

2.10.1 Kerio Connect Account Assistant	118
2.10.2 Configuring a Microsoft Exchange Internet account on Mac OS X	121
2.10.3 Support for Apple iCal/Calendar using the CalDAV standard	122

2.10.4 Contacts folders in Apple Addressbook/Contacts app via CardDAV	125
2.10.5 Delegation in Microsoft Outlook 2011	126
2.10.6 Enabling logging for synchronization with Outlook for Mac	128
2.10.7 Enabling PHP's mail() command to work with Kerio Connect on Mac OS X?	129
2.10.8 How to manually create a CardDAV account in Apple Address Book	131
2.10.9 Logging iCal and AddressBook communication	133
2.10.10 Kerio Connect Account Assistant handling on OS X 10.8 Mountain Lion	134
2.10.11 Viewing events in delegated Calendars when using iCal with CalDAV	134
2.10.12 Getting iCal Auto Complete to work	135
2.10.13 Moving mail to a public folder in Apple Mail deletes the mail	137

2.10.1 Kerio Connect Account Assistant

Kerio Connect Account Assistant is a single autoconfig tool which enables one-time auto-configuration of the following applications:

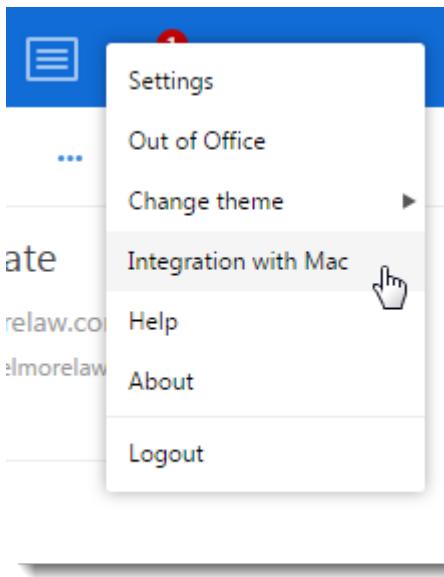
- » Apple Mail & Notes (secure IMAP, SMTP Submission)
- » Apple Calendar & Reminders (CalDAV)
- » Apple Contacts (CardDAV)
- » Apple Messages (XMPP)
- » Microsoft Outlook for Mac (Exchange Web Services)
- » Microsoft Entourage (WebDAV)

Using Kerio Connect Account Assistant

Kerio Connect Account Assistant is unique for each user. You can download it from your own integration page.

1. Open the Mac integration page (e.g. <http://mail.feelmorelaw.com/integration>).

You can also click your name in Kerio Connect Client and select **Integration with Mac**.



2. Click on **Set up my Mac** and download Kerio Connect Account Assistant to your computer.

Integration with Mac

Windows Linux Mobile Devices

Connect your Mac to Kerio Connect:

The page has a blue header bar with the text "Set up my Mac". Below the header are five small icons representing different applications: Mail (envelope), Calendar (calendar with date 17), Contacts (person icon), Messages (speech bubble), and Microsoft Outlook (envelope with '0').

Kerio Connect Account Assistant will be downloaded. It will allow you to configure your Mail, Calendar, Contacts, Messages or Microsoft Outlook.

(Mac OS X 10.6 and later)

[See other options](#)

3. Once the download finishes, the installation program gets started —confirm installation and run it.
4. Select which products installed on your computer to configure (you can configure any of them later) and click **Continue**.



5. Enter your Kerio Connect Client password and click **Continue**. Now the configuration application verifies your identity and server connection.

6. Click **Configure** to run the configuration of the selected applications.

Now the configured applications are available and ready.

NOTE

All previous configuration modules are available at the integration page, upon clicking on See other options.

Troubleshooting

Public contacts lost after upgrading to OS X 10.11 El Capitan

Due to the changes in the Contacts application in OS X 10.11 El Capitan, users lose their public contacts after upgrading their system to El Capitan. To get their public contacts back, they must download and install Kerio Connect Account Assistant version 8.5.3 or newer.

Kerio Connect accounts deleted on OS X 10.11 El Capitan

Due to the changes in the Contacts application in OS X 10.11 El Capitan, all CardDAV accounts created by Kerio Connect Account Assistant are deleted if you synchronize your Keychain with iCloud.

Switch off the synchronization of Keychain and run the Kerio Connect Account Assistant to configure the applications again.

2.10.2 Configuring a Microsoft Exchange Internet account on Mac OS X

With Kerio Connect 8.3 and later, you can configure the Exchange (EWS) type of Internet Accounts on Mac OS X 10.9 and later. The support for EWS Internet Account includes Apple Mail & Notes, Calendar & Reminders, and Contacts.

NOTE

You can also use [Kerio Connect Account Assistant](#) to configure these applications using alternative account types that offer additional functionality.

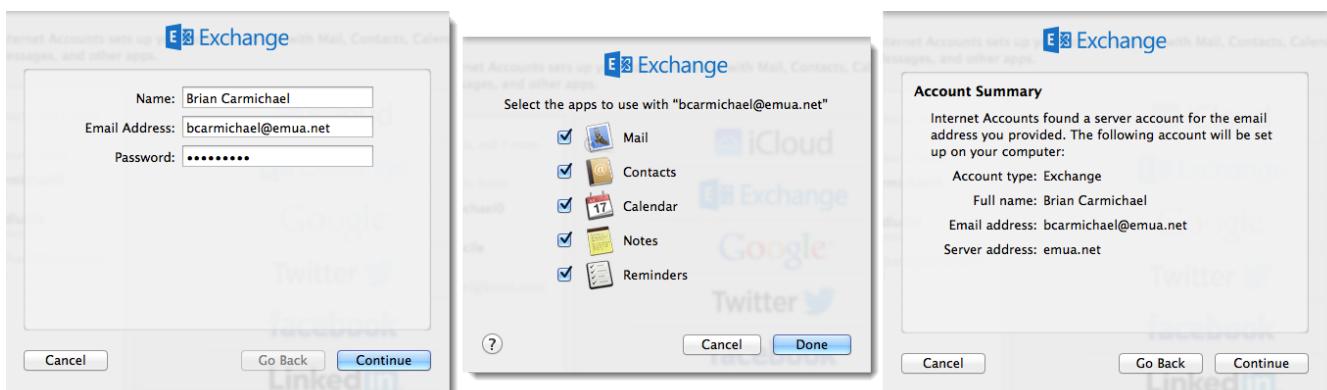
Enabling automatic discovery

You can configure your DNS to support the Autodiscover feature. With autodiscovery, users can use only their username and password to create an account.

For more information, refer to [Configuring Autodiscover in Kerio Connect](#) (page 399).

Adding an Exchange Internet account

1. In **System Preferences**, select **Internet Accounts**.
2. In the right window pane, select **Exchange**.
3. Type your email address and password.
4. Verify the information and click **Continue**.
5. Select the applications you want to configure and click **Done**.



Exchange account limitations

- » Public and shared folders are not synchronized in Mail. You can use [IMAP](#) or [Kerio Connect Client](#).
- » Public and shared calendars (without Delegation) are not synchronized in Calendar. You can use [CalDAV](#) or [Kerio Connect Client](#).
- » Public and shared contacts are not synchronized in Contacts. The Global Address List can be queried. You can use [CardDAV](#) or [Kerio Connect Client](#).
- » You cannot move or create folders within specially designated folders (e.g. Inbox, Drafts, Sent, Trash, Junk)
- » Only one reminder can be synchronized with an event.

2.10.3 Support for Apple iCal/Calendar using the CalDAV standard

CalDAV is an Internet standard which allows applications such as Apple iCal and Apple Calendar to manage calendaring information on a remote server (Kerio Connect).

Kerio Connect supports the following CalDAV features:

- » Calendar availability (free/busy information)
- » Events with privacy tag
- » Travel time for events
- » Scheduling (invitation requests)
- » Per-folder sharing (without delegation)
- » Older sharing notifications
- » Full delegation support
- » Custom labels for shared calendars

NOTE

The CalDAV standard does not support synchronization of nested calendars. To synchronize all your calendars, they must be at the same level.



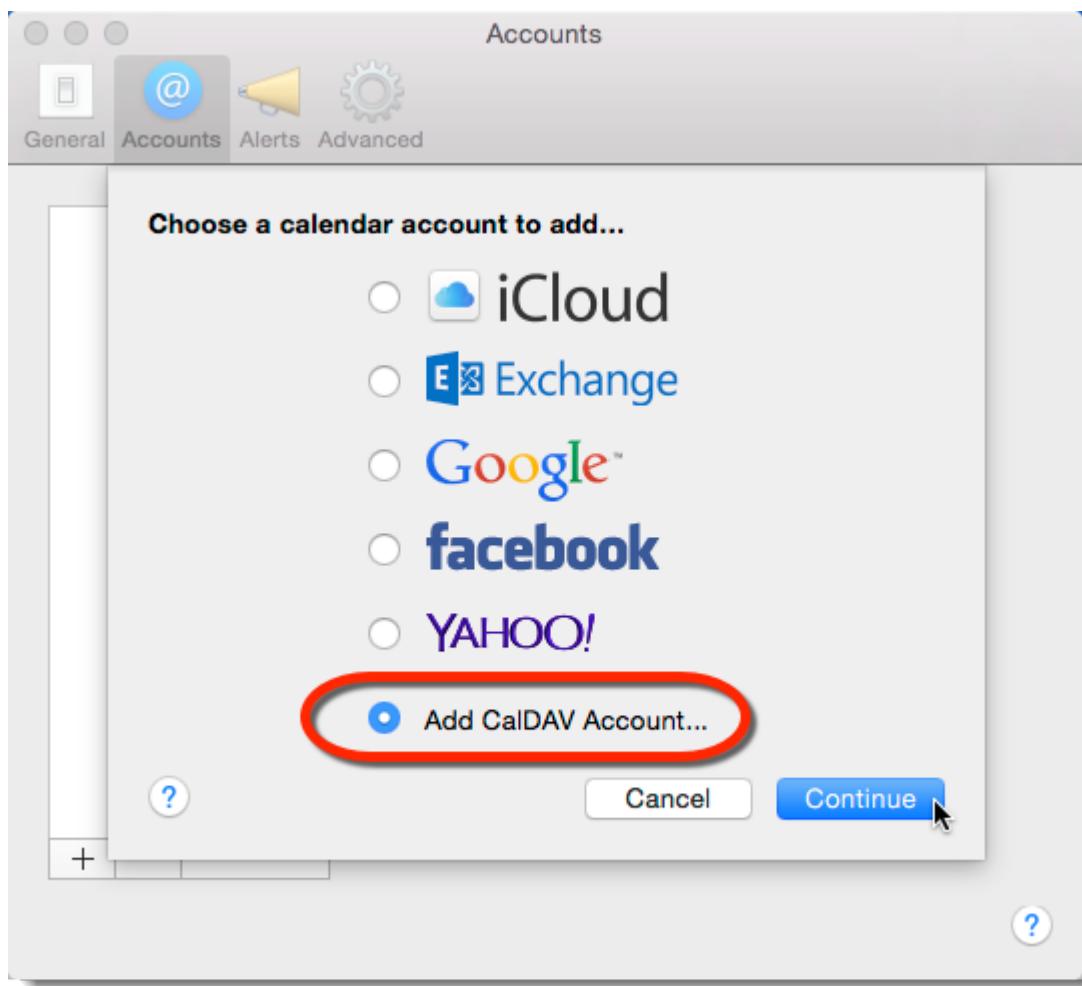
Configuring CalDAV account

Automatic configuration

Use [Kerio Connect Account Assistant](#) to automatically configure Apple iCal/Calendar accounts on Mac OS X 10.6 or later.

Manual configuration

1. Run the **Apple iCal/Calendar** application.
2. In the menu, select **iCal/Calendar > Preferences** and go to the **Accounts** tab.
3. Click the **+** button to create a new account.
4. Select **Add CalDAV Account** and click **Continue**.



5. Select **Manual**, and type your credentials and the location of your Kerio Connect server.

Add a CalDAV Account

To get started, provide the following information:

Account Type:	Manual
User Name:	powaro
Password:	*****
Server Address:	mail.feelmorelaw.com

Cancel Create

A screenshot of a "Add a CalDAV Account" dialog box. It contains fields for Account Type (set to Manual), User Name (powaro), Password (represented by a series of asterisks), and Server Address (mail.feelmorelaw.com). The "Server Address" field is highlighted with a blue selection bar. At the bottom are "Cancel" and "Create" buttons, with a cursor pointing at the "Create" button.

6. Click **Create**.

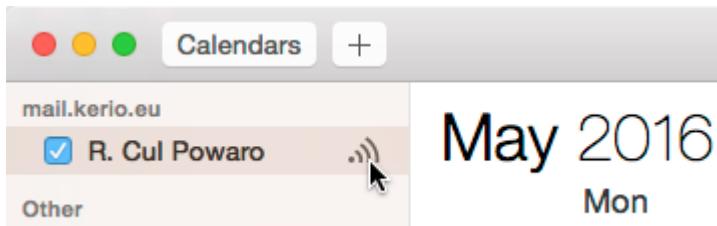
Sharing calendars

If you configure Apple iCal/Calendar with CalDAV, you can share individual calendars with other users.

You can also use an advanced type of sharing — [delegation](#). A delegate has full control over your calendar and can also create and accept meeting invitations on your behalf.

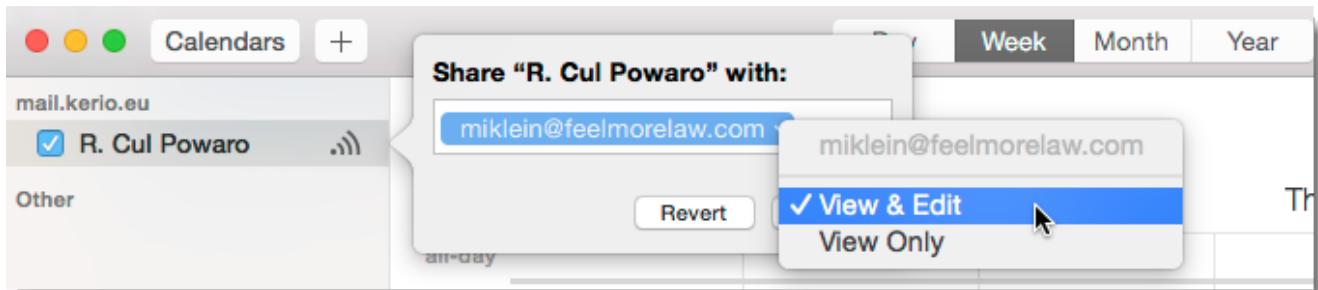
To share a calendar:

1. Select the calendar you want to share from the list of your calendars.
2. Click the share icon next to the calendar name.



3. Type the email address of the user, you want to share the calendar with.
4. To assign rights to the calendar, click the arrow next to the email address and select the level of rights.

You can set sharing to **View only** or **View & Edit**.



5. Click **Done**.

Adding shared, public or resource calendar

Users assigned sharing rights receive a notification which invites them to join the shared calendar.

Accept the invitation and the calendar is added to your calendar list.



If you decline the invitation (or do not receive one), [subscribe to the calendar](#) in your Kerio Connect Client and [select it for synchronization](#).

CalDAV/CardDAV

Select folders to synchronize with your iCal and CalDAV/CardDAV client:

[Check all](#) | [Uncheck all](#)

<input checked="" type="checkbox"/>	Calendar
<input checked="" type="checkbox"/>	Calls tasks
<input checked="" type="checkbox"/>	Cases tasks
<input checked="" type="checkbox"/>	My contacts
<input checked="" type="checkbox"/>	Personal tasks
<input checked="" type="checkbox"/>	Powaro's calendar - lab
<input checked="" type="checkbox"/>	My tasks
<input type="checkbox"/>	Calendar - branch2-meetingroom (resource)
<input checked="" type="checkbox"/>	Contacts (public folder)
<input type="checkbox"/>	Launch dates (public folder)

NOTE

When user adds a shared calendar, they can apply custom properties (for example, colors, names, description) which does not affect the properties of the calendar owner. This behavior is contrary to Delegation, where any calendar property changes performed by the delegate directly affects the owner's calendar.

Assigning delegates

You can also use an advanced type of sharing — delegation. A delegate has full control over your calendar and can also create and accept meeting invitations on your behalf.

Delegates are assigned in the account settings, under the **Delegation** tab. Select the **Edit** button to add a delegate.

Receiving immediate updates

In Kerio Connect 8.5 and newer, you receive updates immediately through the push notification service.

NOTE

If a secure connection to the notification server is unavailable, users receive updates later.

2.10.4 Contacts folders in Apple Addressbook/Contacts app via CardDAV

When you create several contacts folders via Webmail (Sales, Customer etc.) and then sync your Apple Addressbook/Contacts with the Kerio Connect server, these different contacts folders appear as groups.

If they do not appear as groups, then this might be due to the limitation of the used CardDAV protocol in Apple Addressbook/Contacts, with which the account is configured by the Account Assistant tool of Kerio Connect. To fix this, you need to add a category to the addresses in the contacts folders with the same name, as in the contacts folder itself.

For example; let's assume, you have a contacts folder in Webmail called **Sales**. When you open every single address in this folder and assign a category **Sales** to it, this category will reflect in Apple Addressbook/Contacts as a group after the next sync with your Kerio Connect server.

To create a new category in Webmail, just click **Categories**, key in the name of the new category and click **Add to list**.

IMPORTANT

Assigning categories only works via old Webmail. The new Kerio Connect Client has no category functionality.

NOTE

When you create groups in Apple Addressbook/Contacts, these groups do not appear as a contacts folder in your Webmail.

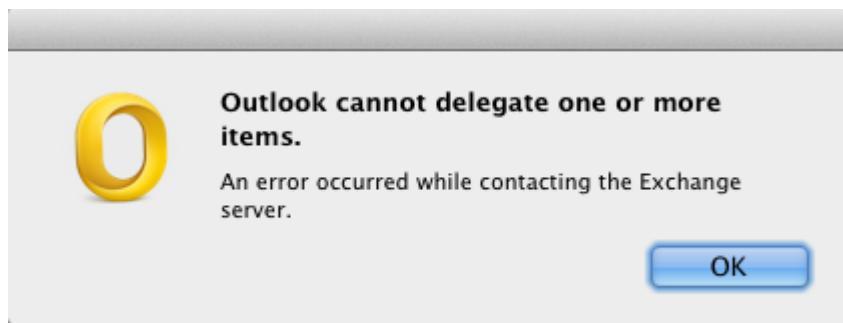
2.10.5 Delegation in Microsoft Outlook 2011

Delegation is an advanced type of sharing. A **delegate** can act on your behalf. A **delegate** can act on your behalf — they can send/confirm your event invitations, and/or send/receive your messages.

Delegating users

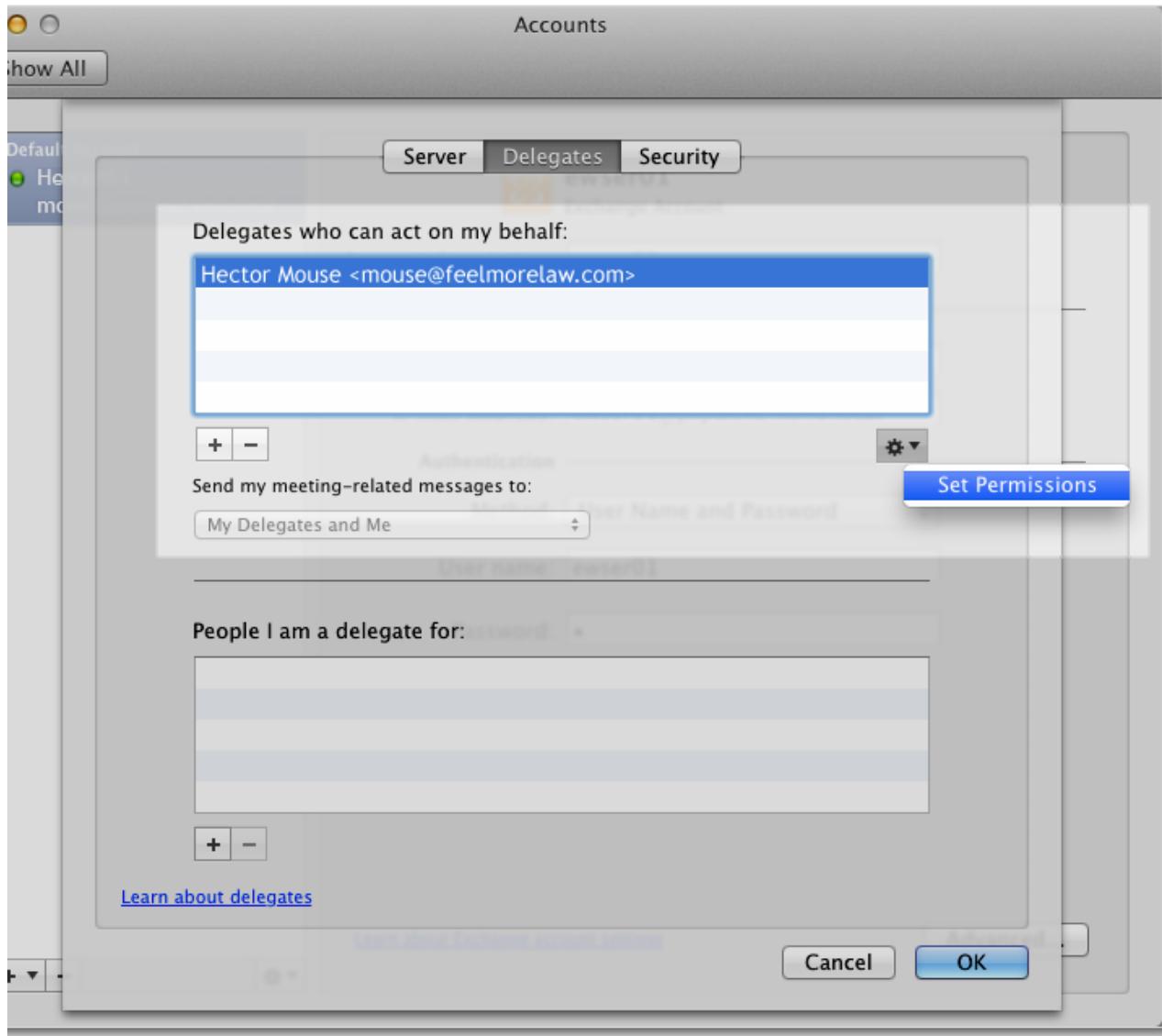
In Outlook 2011, delegates must have at least **Editor** rights to act on your behalf.

With a lower level of rights, you receive the following error message:

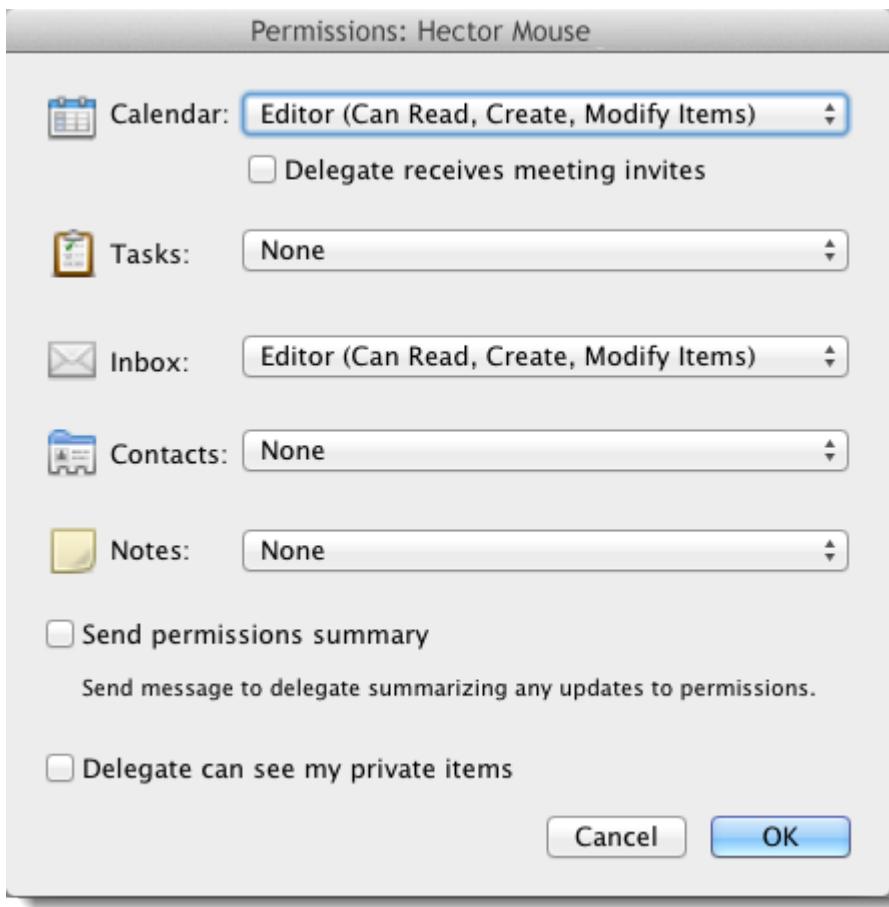


Assigning rights to delegates

1. In your account settings, go to section **Delegates**.
2. Select a delegate and click **Set Permissions**.



- In Kerio Connect 8.3.2 and newer — assign the delegate at least the **Editor** rights to **Inbox** and/or **Calendar**.
- In Kerio Connect 8.2.0-8.3.1 — assign the delegate at least the **Editor** rights to both **Inbox** and **Calendar**.



5. Click **OK** to confirm.

2.10.6 Enabling logging for synchronization with Outlook for Mac

Microsoft Outlook for Mac uses the Exchange Web Services protocol (EWS) which runs over HTTP(S).

EWS heavily depends on the server journal, therefore, it is helpful to enable specific message types logging in:

- » Kerio Connect
- » Microsoft Outlook for Mac

Enable specific logging in Kerio Connect

In the Kerio Connect Debug log, enable the following message types:

- » Services > HTTP Server
- » Message Store > Journal Database
- » HTTP Server Modules > EWS
- » HTTP Server Modules > WebDAV Server Requests (if you use Free/Busy)

Error log and Warning log also help.

Journal log

EWS intensively uses the server journal and is affected by its performance. Kerio Connect saves the `.journal.db` file in the root of each mailbox folder.

By default, Kerio Connect saves the journal events for 60 days. To improve the journal performance, you can decrease the period:

1. Stop Kerio Connect.
2. Locate the configuration file of Kerio Connect.

The default location is:

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

3. Open the `mailserver.cfg` file for editing.
4. Locate the `JournalLogExpiration` value in the `MessageStore` table.

```
<variable name="JournalLogExpiration">60</variable>
```

5. Change the number of days the journal log is saved.

NOTE

EWS requires the minimum of 30 days.

6. Save the file.
7. Start Kerio Connect.

NOTE

Deleting the `.journal.db` file may corrupt the synchronization of all dependent clients ((EWS, Exchange ActiveSync clients, KOFF) and users must create new profiles.

Enabling Error log in Outlook for Mac

For detailed information about logging in Outlook for Mac, see [How to enable logging in Outlook for Mac](#) on the Microsoft website.

2.10.7 Enabling PHP's mail() command to work with Kerio Connect on Mac OS X?

Using the PHP's `mail()` command with Kerio MailServer requires:

- » creating a symbolic link
- » changing the `php.ini` file
- » setting the permissions on the `SendMail` binary
- » disabling Postfix, and
- » configuring the Relay Control settings

Creating the symbolic link

1. In Terminal, navigate to the directory `/usr/sbin` using: `cd /usr/sbin`
2. Disable OS X's `Sendmail` binary using: `sudo mv ./sendmail ./sendmail-orig`
3. Create the symlink using: `ln -s /usr/local/kerio/mailserver/sendmail`

Changing the php.ini file

1. Using Terminal, navigate to the directory /etc using this command: cd /etc
2. Rename php.ini.default to php.ini using: sudo mv php.ini.default php.ini
3. Edit the **php.ini** file with the VI editor using: vi php.ini
4. Used /sendmail, to quickly find the sendmail section of the **php.ini** file.

NOTES

Press **J** and **K** to move up and down and **H** and **L** to move to left and right in the VI editor.

5. Press **X** to remove the semi-colon in front of sendmail_path.
6. Press **I** to enter Insert mode.
7. Change sendmail_path to sendmail_path = /usr/local/kerio/mailserver/sendmail -i -t
8. Press **ESC** to exit Insert mode.
9. Use **w !** in the terminal to save the changes.
10. Use **q !** in the terminal to exit the VI editor.

Setting the permissions on the SendMail binary

1. Using Terminal, navigate to the directory /usr/local/kerio/mailserver using this command: sudo cd /usr/local/kerio/mailserver
2. Run this command to change the permissions on the SendMail binary: sudo chmod 755 sendmail
3. Verify the permissions are correct using the command: ls -l sendmail

We are expecting this result: -rwxr-xr-x@ 1 root wheel 4252344 Dec 11 18:38 sendmail

NOTE

As of version 7.2.0 of Kerio Connect you will also need to make the following changes.

4. Using Terminal, navigate to the directory /usr/local/kerio/mailserver using this command: sudo cd /usr/local/kerio/mailserver
5. Run this command to change the permissions on the first file, sudo chmod 755 ktcrypto.0.9.8.dylib
6. Run this command to change the permissions on the second file, sudo chmod 755 ktssl.0.9.8.dylib
7. Verify the permissions are correct using the command: ls -l kt*
8. Run this command to change the permissions of the mailserver directory, so the PHP can access the sendmail file located in this directory, sudo chmod 755 /usr/local/kerio/mailserver

The result should be:

```
-rwxr-xr-x 1 root wheel 3395124 Jul 18 15:44 ktcrypto.0.9.8.dylib  
-rwxr-xr-x 1 root wheel 740656 Jul 18 15:44 ktssl.0.9.8.dylib
```

IMPORTANT

Please note that the permissions on these files are reset after upgrading Kerio Connect.

Disabling Postfix (for OSX 10.4-10.6)

Using Terminal, type this command: `sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/org.postfix.master.plist`

That single command should stop Postfix from trying to start on port 25.

Configuring the Relay Control settings

1. While logged into the Kerio MailServer Admin Console, go to Configuration > SMTP Server > Relay Control.
2. Enable **Users from IP address group** and click **Edit**.
3. Click **Add**.
4. Name the Address Group Localhost.
5. Select **Host** and key in `127.0.0.1` in the IP address field.
6. Click **OK**.
7. Click **Apply** and **Close**.
8. Select the IP address group named Localhost.
9. Click **Apply**.

You should now be able to use PHP's mail() command with Kerio MailServer.

Using Terminal, type this command to send a test email: `echo test | mail -F admin@yourdomain.com`

NOTE

The webserver application must run as root when executing the PHP script.

2.10.8 How to manually create a CardDAV account in Apple Address Book

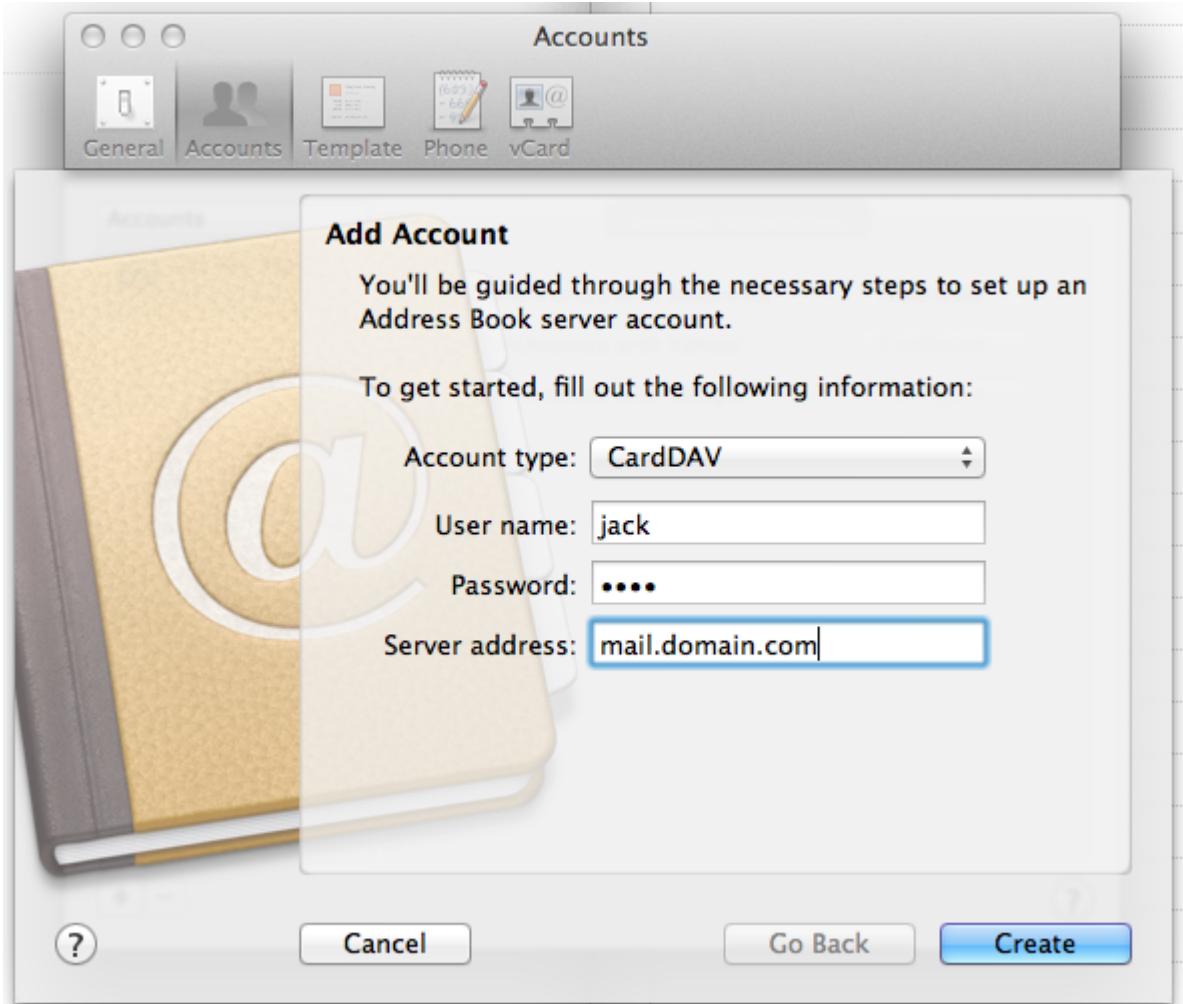
Use the information present in this topic to learn how to manually create a CardDAV account for personal and public contacts in Apple Address Book.

NOTE

A manual setup of the public folders does not work if Kerio Connect is installed on a 10.6.8 Mac Server. Every other version of the Mac software allows your users to configure a manual public CardDAV account.

Personal Contacts

To create a CardDAV connection to your personal contacts, you need to go to **Address Book > Preferences > Accounts**, add an account, select **CardDAV** as the account type, and key in your server address and credentials. Refer to the screen shot below for an example.



Screenshot 8: Adding personal contacts

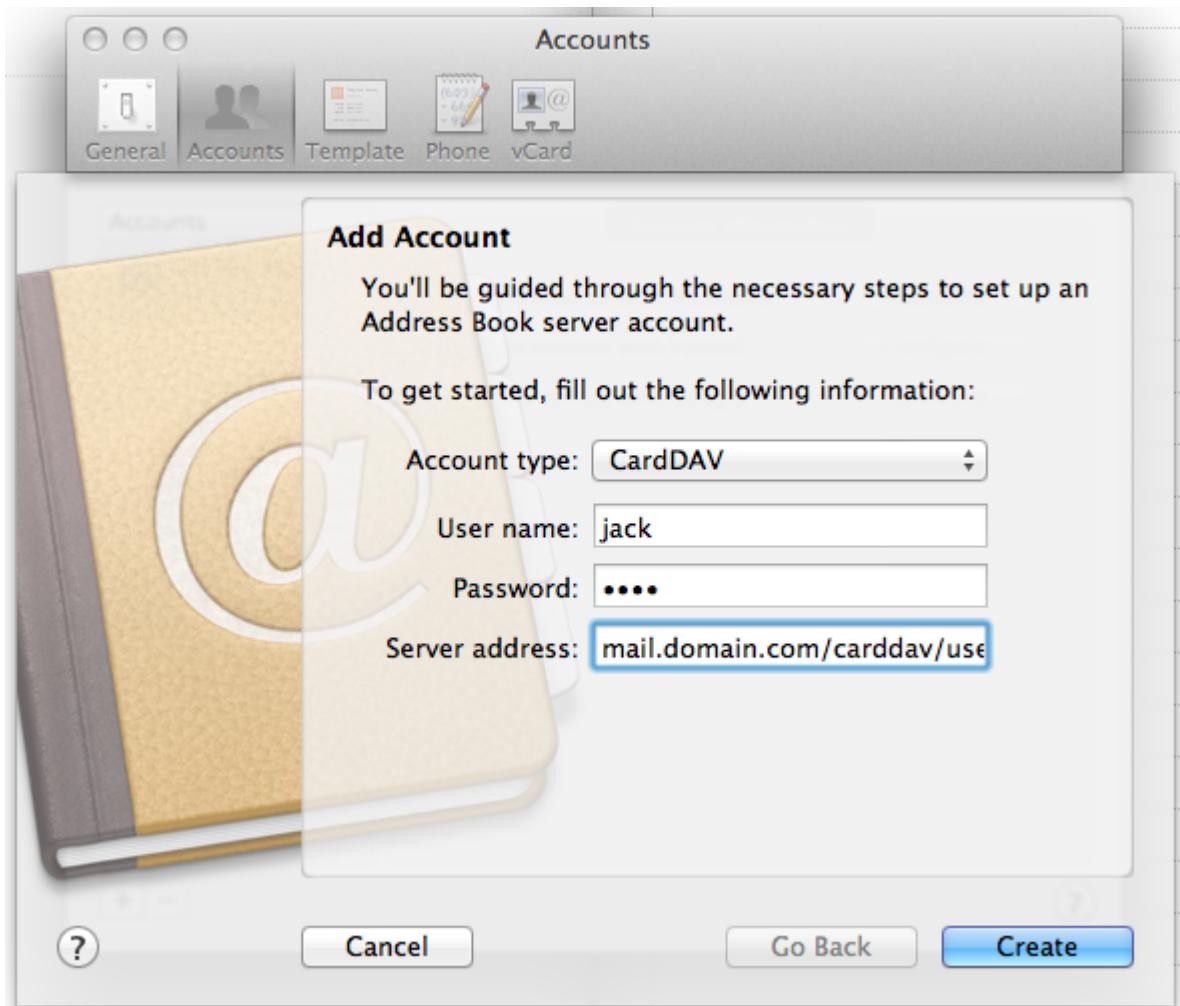
Public Contacts

To create a CardDAV connection to your public contacts, will need to go to **Address Book > Preferences > Accounts**, add an account, select 'CardDAV' as the account type, and key in your server address and credentials. However the server address needs to be a URL for the public folder. It needs to follow the following format:

[server address]/carddav/users/[domain]/.public/

For example, mail.server.com/carddav/users/domain.com/.public/.

Refer to the screen shot below for an example.



Screenshot 9: Adding public contacts

2.10.9 Logging iCal and AddressBook communication

Learn how to gather client side logs for the iCal and Address Book applications communicating with Kerio Connect.

Calendar (iCal) with CalDAV account

In the Terminal, use the following command:

```
defaults write com.apple.iCal LogHTTPActivity yes
```

The logs are stored in **System Console**.

Contacts (Address Book) with CardDAV account

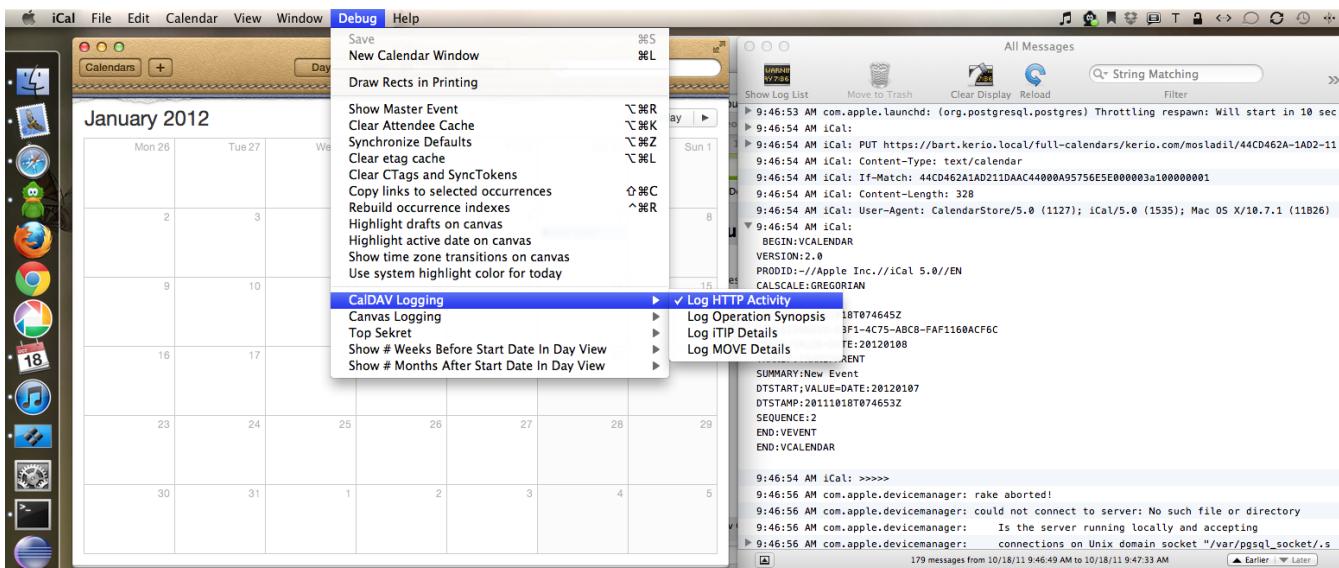
Mac OS X 10.7 & Mac OS X 10.8

In the Terminal, use the following command:

```
defaults write com.apple.AddressBook.CardDAVPlugin EnableDebug -bool YES
```

```
defaults write com.apple.AddressBook.CardDAVPlugin LogConnectionDetails -bool YES
```

The logs are stored in **System Console** and **~/Library/Logs/CardDAVPlugin/**.



2.10.10 Kerio Connect Account Assistant handling on OS X 10.8 Mountain Lion

Apple has added an important new feature called GateKeeper in OS X 10.8 which is designed to protect the end user from running malicious software from unknown developers. This depends on developer signing which becomes complicated with the way the Kerio Connect Account Assistant is built *on-the-fly* for the end user.

The GateKeeper feature in OS X 10.8 is designed to allow developers to sign their applications in a secure way so that you can be assured of any threat that a malicious attacker might pose. This works well for most applications which never change.

However, the Kerio Connect Account Assistant is actually modified for you by Kerio Connect when you choose to download it. It is created with your settings - username, special server settings, etc., so that you will not have to bother yourself with those things to configure your programs. And, since the Kerio Connect Account Assistant is modified by its very nature, it cannot be signed using the GateKeeper protection provided by Apple.

It is easy to get around this by holding down the **Control** key when you click the program to run it. This works when you download and run the Kerio Connect Account Assistant from within the Kerio Connect webmail interface.

Apple describes this **Control-Click** process as running **Apps from anywhere** in their **Core Technologies Overview** document available on their website.

2.10.11 Viewing events in delegated Calendars when using iCal with CalDAV

When iCal is connected to Kerio MailServer via CalDAV protocol, users can manage shared access to their Calendars through the iCal delegation feature.

In specific situations, after selecting the delegated Calendar of another user, you may not see any of the shared events. This can happen through a variety of known circumstances, specifically when Calendar data has been imported from other Calendaring systems, or there has been some type of corruption to the file system (e.g. restored from a broken RAID).

Kerio MailServer 6.7.2 significantly reduces the possibility of this circumstance by incorporating sanity checks on synchronized Calendar data, and stripping invalid data. If you are experiencing this issue, make sure to update to the current version of Kerio MailServer.

It is important to note that the upgrade will not correct any existing Calendar events that have already been synchronized to Kerio MailServer. It is therefore necessary to manually identify and delete these events, which are causing a break in the synchronization.

The following steps describe the process of using webmail to move all events from the affected Calendar to a temporary Calendar, then moving back only the properly formatted events.

1. Log in to the webmail account of the user who owns the affected Calendar. If their Calendar folder contains many items, it is recommended to set the number of displayed messages (located in **Settings > General**) to 200.
2. Right click **Inbox** and create a new sub-folder `calendar_temp` and assign it as a Calendar type folder.
3. Right click Calendar folder and choose **Move or copy all**.
4. Select the new `calendar_temp` folder as the destination and choose **Move**. This will move everything to the new calendar, including events with invalid data.
5. Now select the `calendar_temp` folder and enable the list view from the menu at the top of the calendar window.
6. Select the first event, then hold the **Shift** key and select the bottom event. This should select all events in the window.
7. Drag these items into the original Calendar folder. Repeat this process until all calendar items have been manually moved back into the original Calendar folder.
8. Make sure to include recurring events as well, as the list view of recurring events is selected as a separate menu item.
9. At this point you may delete the `calendar_temp` folder.

NOTE

Although you won't see any information remaining inside the `calendar_temp` folder, it might actually contain the improperly formatted events. The action of **Move or copy all** transfers all of the data, including the broken events, while the action of manually selecting the visible events and moving them back preserves only the properly formatted events.

2.10.12 Getting iCal Auto Complete to work

If iCal does not Auto-Complete the email addresses of invitees for events. Try following these steps to resolve the problem:

1. Remove the iCal CalDAV account and run the **Auto-configure iCal** tool. This tool can be found in your WebMail, go to **Settings > Integration with Mac**.
2. Go to the Directory Utility and check that the LDAP entry for Kerio MailServer is at the top. You can find the Directory Utility in Leopard in **Finder > Applications > Utilities > Directory Utility** and, in Snow Leopard at **OSX drive name > System > Library > CoreServices > Directory Utility**.
3. Clear the local LDAP caches:
`~/Library/Calendars`
`~/Library/Preferences`
`~/Library/Caches/com.apple.ical`
4. Check that the LDAP port is not blocked or being port forwarded to another machine in the network, such as the Open Directory machine.
5. Check that the SSL certificate is not out of date

If the problem still persists, please follow the next steps carefully as the problem may be with your PTR records:

1. Check that the Kerio MailServer LDAP service can be accessed from any computer by using the following command in Mac OSX Terminal:

```
ldapsearch -v -x -H ldap(s)://kms-server-address:LDAP port number
```

For example, `ldapsearch -v -x -H ldaps://mail.company.com:636`

If the search is successful, then you should see the following response:

```
# search result
```

```
Search:2
```

```
Result: 0 Success
```

2. If OpenLDAP answers successfully, then you need to check whether the PTR record is correct. You need to get the IP address of the MailServer hostname using nslookup:

```
nslookup [KMS hostname]
```

For example, `nslookup mail.kerio.com`

You should get this reponse in return:

```
Server: 192.168.10.10
```

```
Address: 192.168.10.10#53
```

```
Non-authoritative answer:
```

```
Name: mail.kerio.com
```

```
Address 63.197.252.130
```

NOTE

The IP addresses above are examples. In real-time these IP addresses for your KMS hostname will be different.

Once you have this information, take a note of the IP address (in the example, it is 63.197.252.130). You can now perform a dig on this address to check the PTR record.

```
dig -x [IP Address]
```

For example, `dig -x 63.197.252.130`

You should get this reponse in return:

```
; <>> DiG 9.4.1-P1 <>> -x 63.197.252.130
;; QUESTION SECTION: ;130.252.197.63.in-addr.arpa. IN PTR
;; ANSWER SECTION: 130.252.197.63.in-addr. IN PTR 63-197-252-130.ded.pacbell.net.
;; SERVER: 192.168.10.10#53(192.168.10.10)
;; MSG SIZE rcvd: 89
```

You will now need to perform an nslookup on the PTR record to see if the record is pointing to a name for which there is no A record:

```
nslookup 63-197-252-130.ded.pacbell.net
```

You should get this reponse in return:

```
Server: 192.168.10.10
```

```
Address: 192.168.10.10#53
```

```
Non-authoritative answer:
```

Name: 63-197-252-130.ded.pacbell.net

Address: 195.39.55.2

You should get this response in return:

Server: 192.168.10.10

Address: 192.168.10.10#5

** server can't find 63-197-252-130.ded.pacbell.net.kerio.local:
NXDOMAIN

If your PTR record has an incorrect response, then your local administrator will need to point the records to the correct location.

However after doing these tests (the test of the KMS LDAP Service is fine, the OpenLDAP works and the PTR records are correct) and running the Auto-Config tool still does not work, then please follow the steps below to enable logging, open a new ticket with the Kerio Technical Support Team and send us the logs in the ticket you create.

In Terminal application, type the following commands:

```
touch /Library/Preferences/DirectoryService/.DSLogDebugAtStart
```

```
sudo killall DirectoryService
```

1. Inspect Directory Service extended debug log:

```
/Library/Logs/DirectoryService/DirectoryService.debug.log
```

2. Inspect Directory Service standard debug log:

```
/Library/Logs/DirectoryService/DirectoryService.server.log
```

3. Rule out the problem from Directory Service logs and Kerio MailServer logs.

4. To disable Directory Service extended logging, run:

```
rm /Library/Preferences/DirectoryService/.DSLogDebugAtStart
```

```
sudo killall DirectoryService
```

2.10.13 Moving mail to a public folder in Apple Mail deletes the mail

In Apple Mail, if you try to move a message to a public folder for which you only have read-only ("reader") rights. You do not receive an error as would be expected and the operation appears to work correctly. However, the message does not appear in the public folder and is lost.

This is caused by an bug in Apple Mail - it is not caused by Kerio MailServer. In technical terms, Apple Mail doesn't check the response to the IMAP COPY request because it behaves as it succeeded even when it fails. The problem occurs with all read-only folders. This problem also happens with other mailservers, e.g. MS Exchange.

A bug has been filed with Apple. Until this is fixed in Apple Mail, you should educate your users to avoid this bug.

2.11 Kerio Connect API

The Kerio Connect API enables you to programmatically access your Kerio Connect server to integrate with third-party solutions or write scripts to automate specific tasks. The API provides all actions available in the client and administration interfaces of the product. For example, you can add/remove users, update IP address groups, read logs, manage time ranges, and much more.

For more information about Kerio Connect API, go to http://go.gfi.com/?pageid=connect_help#cshid=api

3 Using

This section contains information about:

3.1 Monitoring Kerio Connect	138
3.2 Export and Migration	142
3.3 Archiving	159
3.4 Backup	165
3.5 Data store	176
3.6 Instant Messaging	180

3.1 Monitoring Kerio Connect

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

3.1.1 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 messages in queue

Go to **Status > Message Queue > Messages in Queue** tab to view 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.

NOTE

The **Queue ID** displayed in **Status > Message Queue > Messages in Queue** refers to the filename in `store/queue`.

The screenshot shows the 'Message Queue' screen in the Kerio Connect administration interface. At the top, there are tabs for 'Messages in Queue' (selected) and 'Message Queue Processing'. Below the tabs, it displays 'Message count: 2' and 'Message volume: 1.2 MB'. A table lists two messages with columns: Queue ID, Created, Next Try, Size, From, and To. The first message is from dpeterson@company.com to archive@fr.company.com, and the second is from dpeterson@company.com to archive@fr.company.com. Both messages were created on 11 Aug 2009 at different times, with their next try set for 11 Aug 2009 at later times. The sizes are 900 kB and 300 kB respectively. At the bottom, there are buttons for 'Remove Messages', 'Try to Send Now', 'Run Queue', and an 'Auto-refresh' checkbox.

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.

Go to **Status > Message Queue > Messages Processing** to view the status of messages that are currently being processed.

The screenshot shows the 'Message Queue Processing' screen in the Kerio Connect administration interface. It has tabs for 'Messages in Queue' (selected) and 'Message Queue Processing'. Below the tabs, a table lists messages with columns: ID, Size, From, To, and Status. There are two entries: one for message ID 4a81394f-00000000 (size 1.3 kB, From: dpeterson@company.com, To: ablack@company.com, Status: SMTP delivery) and another for message ID 4a8139a0-00000001 (size 1.8 kB, From: dpeterson@company.com, To: sales@company.com, Status: SMTP delivery). At the bottom right, there is an 'Auto-refresh' checkbox.

Configuring message queue parameters

In the administration interface, go to **Configuration > SMTP Server > Queue Options** tab.

Here you can specify:

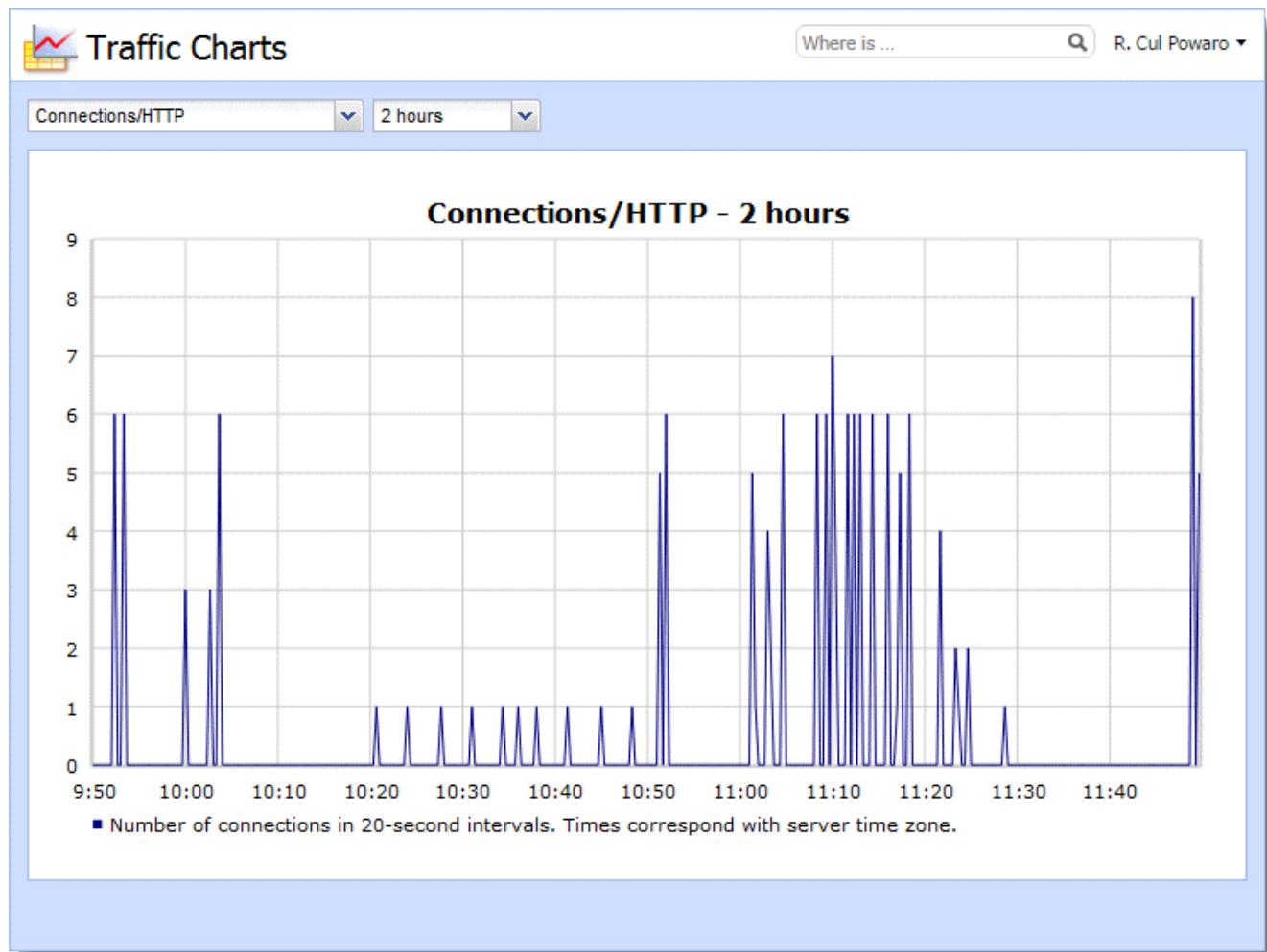
- » The maximum number of messages being delivered at a time.
- » The interval in which Kerio Connect retries to deliver messages.
- » The interval in which Kerio Connect sends the undelivered messages to senders.
- » The interval in which senders are notified that their messages have not been delivered.

NOTE

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

3.1.2 Traffic charts

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



3.1.3 Viewing statistics

In the Kerio Connect administration interface, go to **Status > Statistics** to 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.

The screenshot shows the 'Statistics' page of the Kerio Connect web interface. At the top, there's a search bar and a user dropdown for 'R. Cul Powaro'. Below the header, there are several sections with data:

- Server status**: Server uptime is 3 hours, 5 minutes.
- Storage occupied**: Total storage is 102.5 GB, Storage occupied is 39.0 GB, and Percent is 37 %.
- Antivirus statistics**: Attachments checked: 206, Viruses found: 0, Prohibited filenames / MIME types found: 0.
- Spam filter statistics** (partially visible).

At the bottom, there are buttons for Refresh, Reset, Save as..., and To Advanced Mode. A note says 'The statistics are counted since 2011-04-06 10:35'.

3.1.4 Displaying users currently connected to Kerio Connect

Go to **Status > Active Connections** to view all network connections established with the server.

The screenshot shows the 'Active Connections' page. At the top, there's a search bar and a user dropdown for 'R. Cul Powaro'. Below the header, there are two tabs: 'Active Connections' (selected) and 'Active Web Sessions'. A table lists the active connections:

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

At the bottom right, there's a checkbox for 'Auto-refresh'.

To display connections established to Kerio Connect's web interfaces and session expiry times, go 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

Auto-refresh

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

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

3.1.5 Monitoring CPU and RAM usage

Go to **Status > System Health** to view the current usage of CPU, RAM and the disk space on the machine where Kerio Connect is installed.

Details	Description
CPU usage	Timeline of the computer's CPU load. Short time peak load rates can be caused, for example, by the network activity.
RAM usage	RAM usage timeline.
Storage Usage	Currently used space and free space on the disk or a memory card.

You can also choose a **Time Interval** and view the CPU and RAM usage details according to it.

Additionally, lack of system resources may seriously affect the functionality of Kerio Connect. If these resources are permanently overloaded, click **Tasks > Restart** and then check storage usage again.

3.2 Export and Migration

This section contains information about export/import and migration from/to other servers.

3.2.1 Importing users in Kerio Connect	143
3.2.2 Exporting users in Kerio Connect	145
3.2.3 Kerio Connect Migration Service	145
3.2.4 Kerio Exchange Migration Tool	150
3.2.5 KerioIMAP Migration Tool	153
3.2.6 Transferring an installation of Kerio Connect to another server or Operating System	156

3.2.7 Migrating users from directory service to local database	158
--	-----

3.2.1 Importing users in Kerio Connect

In Kerio Connect you can import users from:

- » CSV files
- » Directory service

On Importing, the users are assigned [local user accounts](#) automatically.

NOTE

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. The columns' headings in the file must correspond with the Kerio Connect categories.

Individual fields can be separated in two ways:

- » Using semicolons (;). In this case, you can separate multiple values of a field with commas (,).

```
Name;Password;FullName;Description;MailAddress;Groups  
abird;VbD66op1;Alexandra Bird;Development;abird;read,all  
abird;Ahdppu4;Edward Wood;Sales;ewood,wood;sales,all  
mtaylor;SpoiuS158;Michael Taylor;Assist-  
ant;mtaylor,michael.taylor;all
```

- » Using commas (,). In this case, you can enclose multiple values of a field in quotations marks (" ") and separate them with comma (,).

```
Name;Password;FullName;Description;MailAddress;Groups  
abird,VbD66op1,Alexandra Bird,Development,abird,"read,all"  
ewood,Ahdppu4,Edward Wood,Sales,"awood,wood","sales,all"  
mtaylor,SpoiuS158,Michael Taylor,Assist-  
ant,"mtaylor,michael.taylor",all
```

NOTE

There is no rule about the order of the columns. Only the **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

IMPORTANT

If you want to import users from a Windows 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. This displays a list of users.

NOTE

During the import, sensitive data is transmitted (such as user passwords). You must secure the communication using SSL encryption.

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

Microsoft Active Directory

1. Go to **Accounts > Users** and select a domain to which you want to import users.
2. Click **Import and Export > Import from a Directory Service**.
3. Type the name of the Microsoft Active Directory domain, the name of the server with Active Directory, and the user-name and password of an Active Directory user who has at least *read* rights. Then confirm. This displays a list of users.

NOTE

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

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. This displays a list of users.

NOTE

During the import, sensitive data is transmitted (such as user passwords). You must secure the communication using SSL encryption.

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.

3.2.2 Exporting users in Kerio Connect

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. In the export file, individual fields 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 name uses `users_<DomainName>_<date>.csv` format.

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 name uses `users_<DomainName>_<GroupName>_<date>.csv` format.

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 name uses `users_<DomainName>_<MailingListName>_<date>.csv` format.

3.2.3 Kerio Connect Migration Service

Kerio Connect Migration Service is a web-based application that allows you to transfer mailbox data and user accounts from your machine containing Kerio Connect installation to [Kerio Cloud](#).

NOTE

To transfer data and configuration from one Kerio Connect server to another, use backup and restore. See [Configuring backup in Kerio Connect](#) and [Data recovery in Kerio Connect](#).

Prerequisites

On the **Source server**, you need a Kerio Connect installation with:

- » The domain you want to migrate.
- » The account with full admin access and admin access to public folders. Do not use the **built-in administrator** account.
- » IMAPS access to the server on port 993.
- » Access to the administration interface on port 4040.
- » Port 44337 open for internal communication during migration.

On the **Destination server**, you need a Kerio Cloud account with:

- » The same domain used on the source server
- » An admin account for the domain you want to migrate with admin rights to public folders

NOTE

From one server, you can migrate only one domain at a time. To migrate multiple domains from a single server, migrate the domains one by one.

What data is migrated

Kerio Connect Migration Tool transfers the following items:

- » All mailboxes created in Kerio Connect.
- » All emails, calendars, contacts, tasks, and notes.
- » All users email filters in Kerio Connect Client.
- » Public folders (calendars, contacts, tasks, and notes).

What data is not migrated

- » Passwords
- » Aliases
- » Resources
- » Mailing lists
- » Server settings

Changes to user accounts

Kerio Cloud has only domain admin accounts (no full admin access). Therefore, Kerio Connect Migration Service adjusts the access rights to Kerio Connect Administration as follows:

- » Full admin becomes a domain admin.
- » Read-only admin becomes a standard user.

See [Assigning admin rights to individual users](#) for more information about admin access.

Users must also re-configure their clients to use the Kerio Cloud server hostname. See **step 12** below.

Migrating data

NOTE

Kerio Connect Migration Service migrates your data from your Kerio Connect to Kerio Cloud periodically. Before you end the migration process, you must download the new user passwords, change your DNS MX records, and the users must re-configure their email clients.

1. In your browser, go to the Kerio Connect Migration tool page:

- To migrate to a **US based** data center, go to <https://migration.kerio.cloud/>.
- To migrate to a **European** data center, go to <https://migration.eu1.kerio.cloud/>.

2. To connect to the cloud server, key in:

- The hostname of the cloud server you received after [registering for an account](#).
- The Kerio Cloud domain admin email address and password.

The screenshot shows the 'Kerio Connect Migration Service' login page. At the top, it says 'Transfer Kerio Connect mailbox data and user accounts to a new Kerio Cloud server. [Learn more...](#)' Below that, it says 'To get started, provide your domain administrator account (Kerio Cloud) or the full administrator account of your destination server.' There are three input fields: 'Hostname' containing 'host001.keriocloud.com', 'Administrator account' containing 'powaro@feelmorelaw.com', and 'Password' containing '.....'. A blue 'Login' button is at the bottom right, with a cursor pointing to it.

3. Click **Login**.

4. To connect to your source server, key in:

- The hostname of your Kerio Connect server.
- The email address and password of a user with full admin access rights and public folder admin access.

Kerio Connect Migration Service

Source	Destination
	Hostname: host0001.keriocloud.com Domain: feelmorelaw.com

Connect to source server

To continue, provide your full administrator account of your Kerio Connect server with data you want to migrate.

Hostname

Administrator account

Password

Connect

5. Click **Connect**. Kerio Connect Migration Service verifies the access to both servers and that both servers have the same domain.

6. Click **Run migration** to start the migration process.

Kerio Connect Migration Service

Source Hostname: mail.feelmorelaw.com Domain: feelmorelaw.com	Destination Hostname: host0001.keriocloud.com Domain: feelmorelaw.com
--	--

Ready

0%

7 user account(s) will be created.
0 users of 7 migrated.
0 items of 183 migrated.
0 MB of 27 MB migrated.

[Run migration](#)  [End migration](#)

[Show details](#) [Download log](#)

7. Optionally, you can temporarily interrupt the migration process whenever you want by clicking **Pause migration** and then **Resume migration**.

[Resume migration](#) [End migration](#)

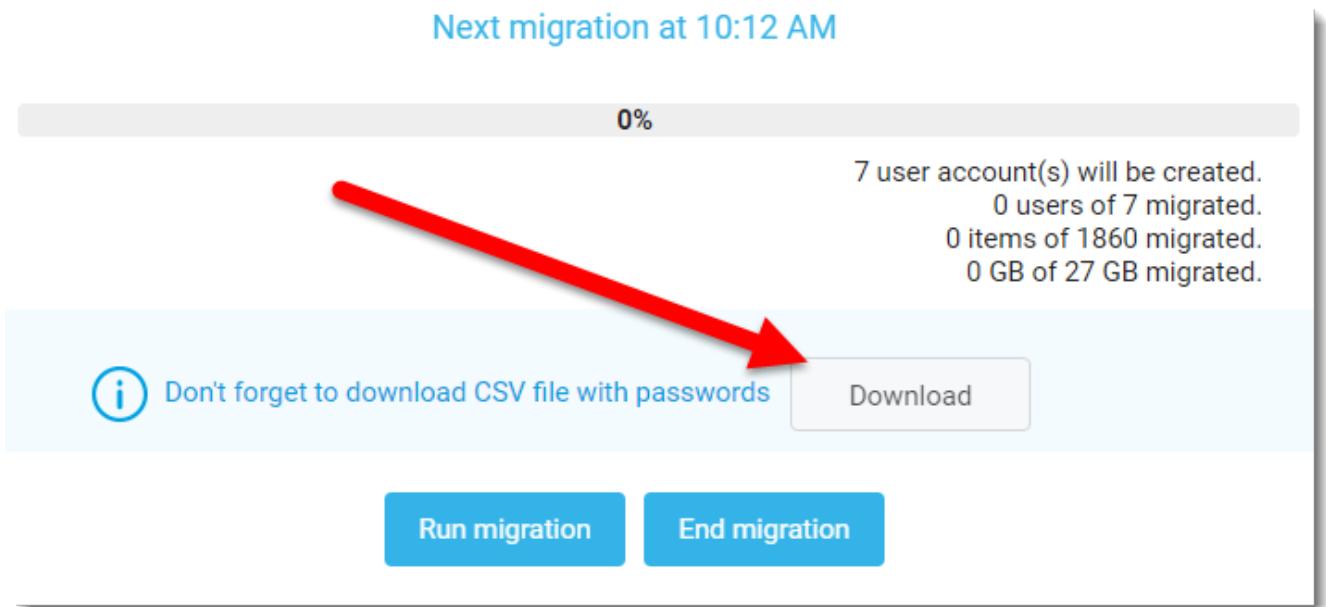
► Last migration finished at 10:02 AM

[Show details](#)   [Download log](#)

8. Click **Download** to save a CSV file with usernames and new user passwords for the migrated accounts.

IMPORTANT

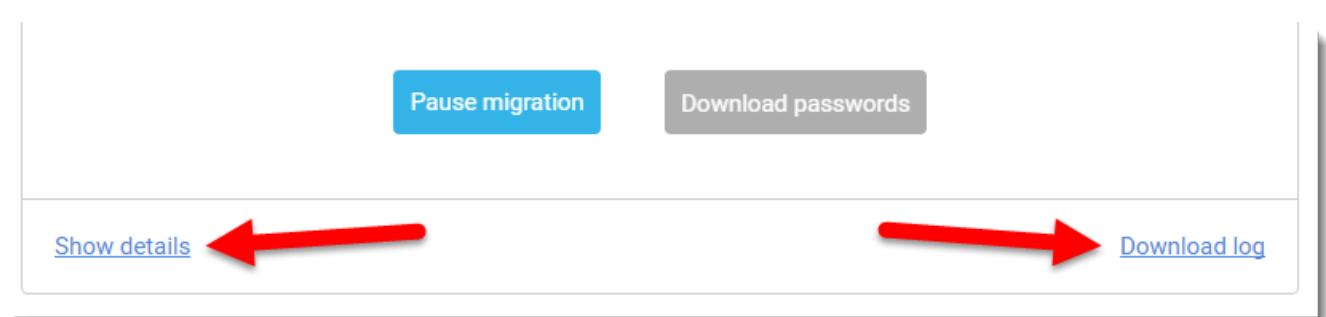
You must download the passwords before you end the migration. Otherwise, all user passwords will be lost.



9. Change your DNS MX records so that they point to the Kerio Cloud server. For more information, refer to [What is an MX record, and how is it created?](#) (page 401).
10. Verify that messages for your domain are properly routed to the Kerio Cloud server.
11. Users must re-configure their clients to use the Kerio Cloud server hostname. They must also use the passwords from the CSV file you downloaded in **step 9**. It is recommended to change the passwords immediately after their first login.
12. Click **End Migration** to finish the migration process.

NOTE

Click **Show details** during the migration to display the last 2000 lines of the migration log. To see the full log, click [Download log](#).



13. If necessary, re-configure your [DNS](#) for autodiscovery and [DKIM](#), and adjust any domain settings in Kerio Cloud.
14. Stop using your old Kerio Connect server.

3.2.4 Kerio Exchange Migration Tool

The **Kerio Exchange Migration Tool** (KEMT) is a free application for migrating public folders, accounts, and user data (Email, Contacts, Calendars, Tasks, Notes) from your Microsoft Exchange Server to Kerio Connect.



Screenshot 10: The migration process

Preparing for the migration

See the Kerio Connect [product page](#) for supported versions of Microsoft Exchange server and Microsoft Outlook.

The duration of the migration depends on many factors, and may take some time. If possible, perform the migration during light usage hours.

The migration tool does not overwrite or remove the existing data in the destination Kerio Connect mailboxes. You can therefore run the migration tool on active Kerio Connect mailboxes, and the data will be merged.

Ensure that data on Microsoft Exchange does not change during or after the migration process. To prevent this from happening, ensure that users and new email are directed to Kerio Connect server before starting the migration.

Before you start

1. [Install Kerio Connect](#) and run it.
2. Verify that the [IMAP service in Kerio Connect](#) runs on port 143.
3. On a machine which can access both Kerio Connect and the source Exchange server, install Microsoft Outlook and the Kerio Exchange Migration Tool

NOTE

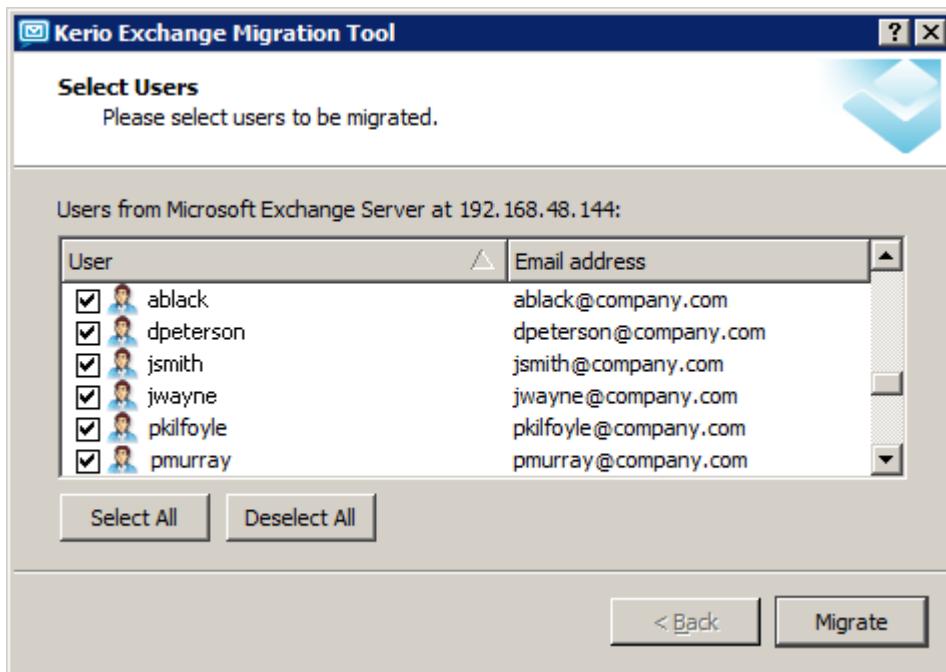
Do not install the KEMT tool on a computer that has both Exchange server and the Kerio Connect server. This results in migration failure.

4. Disable receiving new emails on the source Exchange server temporarily (otherwise migrated data will be inconsistent).
5. Verify that MAPI is enabled on the Exchange server. See [Enable or disable MAPI for a mailbox](#) for details.
6. If connection between the Exchange server and Kerio Connect goes through a firewall, open the following firewall ports:
 - TCP protocol on port 143
 - TCP/UDP protocol on port 44337

Migrating the data

1. Verify that both the source Exchange server and Kerio Connect are running.
2. Run the Kerio Exchange Migration Tool (KEMT) and follow the wizard.
3. Key-in the hostname of the source Exchange server and its administrator.
4. Key-in the hostname and admin credentials of Kerio Connect.

5. Select the accounts for migration. The migration process may be time-consuming. We recommend to migrate data in parts (groups of users).

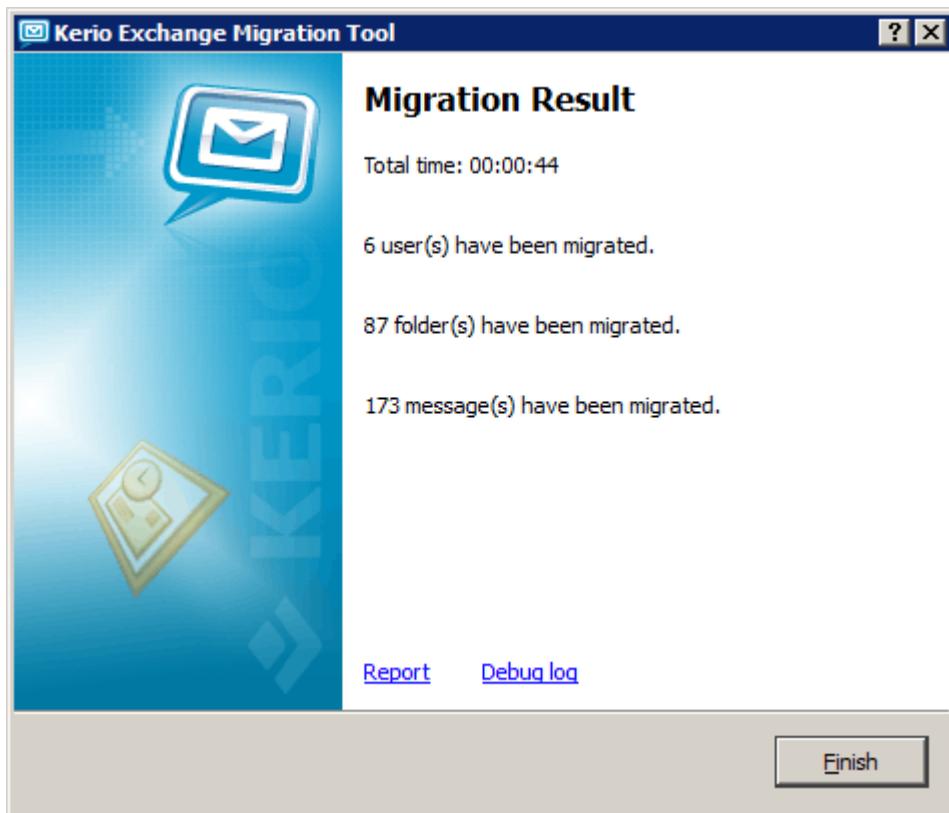


6. Click **Migrate**.

NOTE

If you interrupt the migration process, the tool only saves the completely migrated data of the user currently being migrated. Before you resume, delete the partially migrated user in Kerio Connect to prevent data duplication. See the [Report log](#) section for details.

7. When the migration is finished, click the [Report](#) or [Debug log](#) links to see the migration result.



Users should create new accounts/profiles in users' email clients to avoid data inconsistency.

Migration process logs

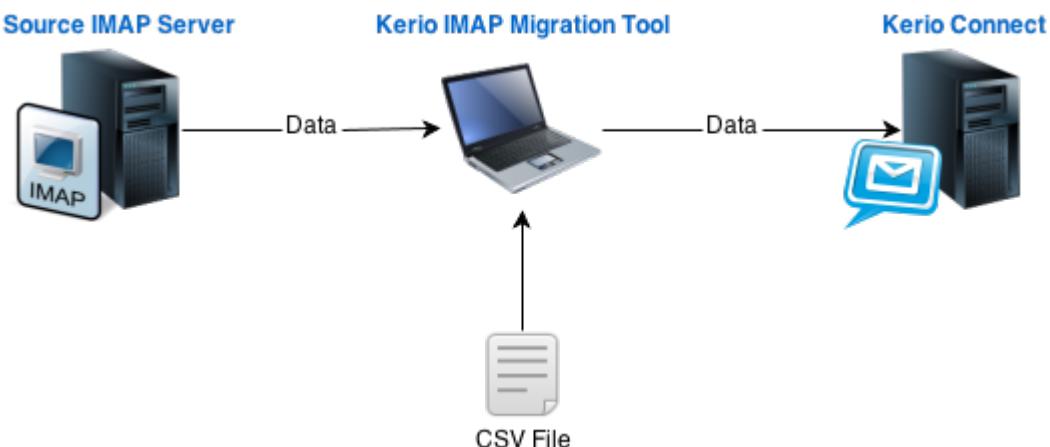
The Kerio Exchange Migration Tool (KEMT) generates various logs during the migration process. They are stored within the KEMT installation folder in `\logs\MMDDYYYY_HHMMSS`.

Every time you start the migration tool, it generates a new log.

Log file	Description
Report log	After completion of each migration, it is recommended to go through this file to make sure that no errors occurred and that all user accounts have been migrated correctly. If users had not been mapped to Kerio Connect before the migration, the Report log includes new user passwords generated by the migration tool.
Debug Log	Information in this log is useful especially for the developers. If you have any issues during the migration process, this log can help the Kerio technical support to find the solution.

3.2.5 KerioIMAP Migration Tool

The **Kerio IMAP Migration Tool** (KIMT) is a free application for migrating user accounts, email messages and folders from your IMAP server to Kerio Connect.



Screenshot 11: The migration process

Preparing for the migration

The duration of the migration depends on many factors, and may take some time. If possible, perform the migration during light usage hours.

The migration tool does not overwrite or remove the existing data in the destination Kerio Connect mailboxes. You can therefore run the migration tool on active Kerio Connect mailboxes, and the data will be merged.

Ensure that data on the source IMAP server does not change during or after the migration process. To prevent this from happening, ensure that users and new email are directed to Kerio Connect server before starting the migration.

CSV file with user accounts

Before the migration, prepare a CSV file with the list of users and their passwords. This information is crucial for access to the source IMAP server. The CSV file must follow this pattern: `user@domain.com;password;Full Name`.

Public and archive folders

Public and archive folders cannot be migrated by the standard procedure. If you need to migrate these folders, move them to the mailbox of any user to migrate them as private folders.

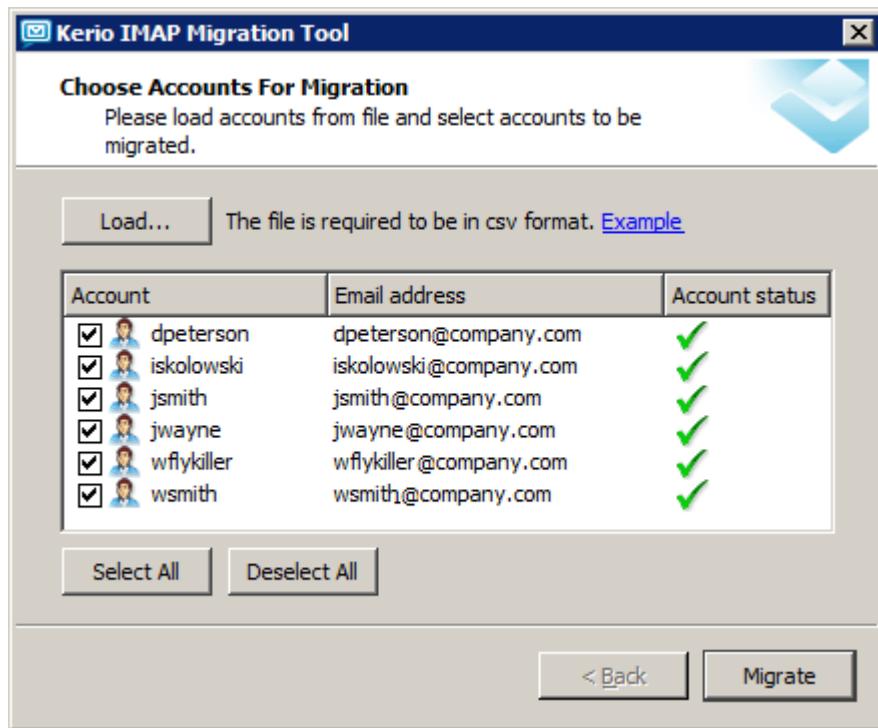
Before you start

1. [Install Kerio Connect](#) and run it.
2. Make sure the [IMAP service in Kerio Connect](#) runs on port 143.
3. On a machine which can access both Kerio Connect and the source IMAP server, [download](#) and install the KIMT tool.
4. We recommend you to make sure the source IMAP server cannot accept new emails. Otherwise migrated data will be inconsistent.
5. If the connection between the IMAP server and Kerio Connect goes through a firewall, open the following firewall ports:
 - TCP protocol on port 143
 - TCP/UDP protocol on port 44337

Migrating the data

The migration requires that both the source IMAP server and Kerio Connect are running.

1. Run the KIMT tool and follow the wizard.
2. Key-in the hostname of the source IMAP server. We recommend to **Use SSL connection** for security reasons.
3. Key-in the hostname and admin credentials of Kerio Connect.
4. In **Choose Accounts For Migration**, load the CSV file and select users to migrate. The migration process may be time-consuming. We recommend to migrate data in parts (groups of users).

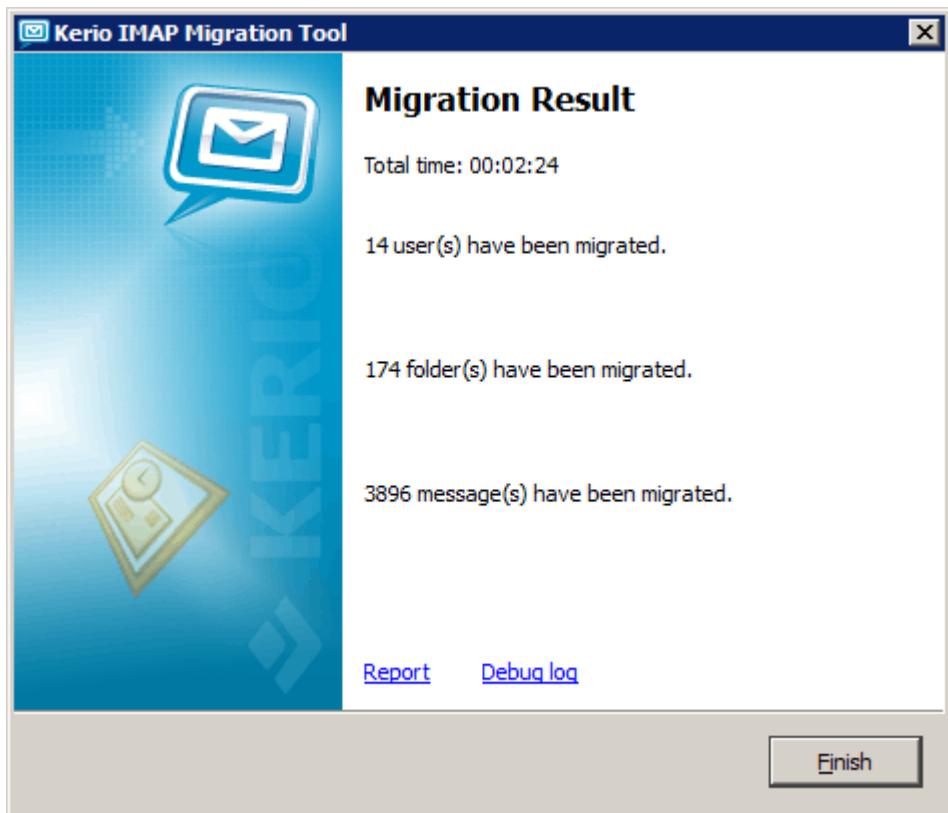


5. Click **Migrate**.

NOTE

If you interrupt the migration process, the tool only saves the completely migrated data of the user currently being migrated. Before you resume, delete the partially migrated user in Kerio Connect to prevent data duplication. See the [Report log](#) section for details.

6. When the migration is finished, click the [Report](#) or [Debug log](#) links to see the migration result.



Once the migration is completed successfully, we recommend you to create new accounts/profiles in users' email clients. This will help them avoid data inconsistency.

Migration process logs

Kerio IMAP Migration Tool generates various logs addressing the migration process. They are stored in the following locations:

- » MS Windows — %TEMP%\KimtLogs\MMDDYYYY_HHMMSS
- » Linux — ~/KimtLogs/MMDDYYYY_HHMMSS
- » Mac OS X — ~/Library/Logs/KimtLogs/MMDDYYYY_HHMMSS

Every time you start the migration tool, it generates a new log.

Log file	Description
Report log	After completion of each migration, it is recommended to go through this file to make sure that no errors occurred and that all user accounts have been migrated correctly. If users had not been mapped to Kerio Connect before the migration, the Report log includes new user passwords generated by the migration tool.
Debug Log	Information in this log is useful especially for the developers. If you have any issues during the migration process, this log can help the Kerio technical support to find the solution.

3.2.6 Transferring an installation of Kerio Connect to another server or Operating System

Kerio Connect supports two methods for moving the data and configuration of Kerio Connect to another installation of Kerio Connect running on a different server or operating system.

The first method involves using the backup and recovery feature, while the other method involves transferring the files and folders.

NOTE

In both of these methods, the two servers running Kerio Connect must be taken offline before starting the migration process in order to prevent data inconsistency.

IMPORTANT

If you are moving from the 32-bit version of Kerio Connect to the 64-bit version, refer to [Switching from a 32-bit installation of Kerio Connect to 64-bit](#)

Prerequisites

Before you begin either process make sure you have:

- » Your server license (this is located in the license section of the [dashboard](#)).
- » Full operating system access to both servers.
- » A matching version of Kerio Connect is installed on both servers (old versions can be obtained from [download.kerio.com](#)).
- » A means of transferring data, either using a portable storage device or some form of network file transfer such as FTP or SCP.

Method 1: Restoring from a backup (Recommended)

1. On the source server, perform a backup. For more information, refer to [Configuring backup in Kerio Connect](#) (page 165).
2. Copy the backup files to the target server,
3. On the target server, perform data recovery. For more information, refer to [Data recovery in Kerio Connect](#) (page 168).
4. After the recovery is complete, modify the mailserver.cfg file to use the appropriate paths on the target operating system. For more information, refer to [Editing the configuration to use the correct system paths](#) (page 158).

Method 2: Transferring the configuration and mail store directory

Kerio Connect is installed in the following location:

Operating System	Location
Mac OSX	/usr/local/kerio/mailserver/
Red Hat/SuSE	/opt/kerio/mailserver/
Windows	C:\Program Files\Kerio\MailServer\

1. In the Kerio Connect installation directory, locate the following files and folders:

- » `mailserver.cfg` - Stores Kerio Connect configuration
- » `users.cfg` - Stores users, groups, and aliases
- » `sslcert` - Directory containing the private key used in SSL connections
- » `settings` - Directory containing specific settings such as SMTP rules and images for domain footers

2. On the target server, stop Kerio Connect, then copy and replace these items from the source server.

3. Locate your mail store on the file system of the source server. This directory is defined in the administration under the **Configuration > Advanced Options > Store Directory** tab.
4. Copy the mail store directory to the desired location of the target server.
5. After copying the configuration and mail store data, modify the mailserver.cfg file to use the appropriate paths on the target operating system. For more information, refer to [Editing the configuration to use the correct system paths](#) (page 158).

[Editing the configuration to use the correct system paths](#)

If the target system is based on a different operating system or has a different directory structure, you must edit the mailserver.cfg configuration file in a text editor to define the correct system paths.

The following variables contain a system path:

Table	Variable	Description
Directories	StoreDir	Path to store directory
Directories	ArchiveDir	Path to archive directory
Directories	Backup Dir	Path to backup directory
Update	DownloadedFile	Path to recent update file by web administration upgrade feature.
FullTextSearch	Path	Path to full-text search
InstantMessaging	StorePath	Path to Instant Messaging configuration data
WebIM	StorePath	Path to XMPP configuration data
LogGlobal	RelativePathsRoot	Path to log files

On the target server, start the service, and log in using the administrator account used to access the source server. If the service fails to start, it may be caused by incorrect definition of the store directory. In that case, verify that the location of the store directory is accurately configured in the mailserver.cfg file, as described above.

Final Steps and Other Considerations

- » Register your license on the new server
- » If you are authenticating users to a directory service, make sure to [join the server to the domain](#).
- » If your server's IP address has changed, make sure to update all relevant DNS records
- » If you are moving from Mac OS X to a different OS, you must rebuild accounts that use Exchange Web Services (EWS). This means you need to remove and re-create the account that is set up as an Exchange Account in the email client application (e.g Outlook, Apple Mail). This does not apply to iOS and Android devices as they only use IMAP or ActiveSync.

3.2.7 Migrating users from directory service to local database

If you are currently using Microsoft® Active Directory®, Windows NT® domain or Novell® eDirectory™

1. Go to the Kerio Webadmin console
2. Highlight all the directory users (use *Ctrl+A*) and choose **Remove**.
3. Select **Do not delete user's message folder**.

4. Click **Import and Export > Import from a Directory Service** to import users from the directory service. For more information, refer to [Importing users in Kerio Connect](#) (page 143).
5. Select all the users within the console, choose **Edit...** and change the **Authentication** to the Internal user database.

IMPORTANT

You will need to update each user's password field manually as passwords are not transferred from AD to Kerio.

After migration, all users are assigned user accounts automatically.

If you are currently using Apple® Open Directory:

1. Go to the Kerio Webadmin console
2. Select **Import and Export > Export to a CSV File** and save the file to your hard drive.
3. Open the exported CSV file (`users_domain_YYYY-MM-DD.csv`) in Microsoft® Excel.
4. Change the **Authentication** to Internal and save the CSV file
5. Highlight all the directory users (use `Ctrl+A`) and choose **Remove**.
6. Select **Do not delete user's message folder**.
7. Click **Import and Export > Import from a CSV file** to import users from the CSV file.

IMPORTANT

You will need to update each user's password field manually as passwords are not transferred from OD to Kerio.

After migration, all users are assigned user accounts automatically.

3.3 Archiving

This section provides information about archiving data on the Kerio Connect server.

3.3.1 Archiving in Kerio Connect	159
3.3.2 Archiving chat in Kerio Connect Client	163
3.3.3 Archiving emails using GFI Archiver	164

3.3.1 Archiving in Kerio Connect

Kerio Connect can archive messages on a local hard drive or to a remote email address.

You can archive:

Message type	Description
Local messages	Messages sent by a local sender to local recipient
Incoming messages	Messages sent by a remote sender to local recipient
Outgoing messages	Messages sent by a local sender to remote recipient
Relayed messages	Messages sent by a remote sender to remote recipient

If you later need an old or deleted message, you can recover it by using [email recovery](#).

Archiving saves messages sent and received by a user 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.

NOTE

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. Check **Enable email archiving**.
3. To send the archive files to an email address, check **Archive to the remote email address** and key-in the address.
4. To save the archive files to a local hard drive, check **Archive to the local subfolder**, select the archiving interval, and specify the folder at the **Target archive directory** at the top.
5. Check the types of messages you want to archive- *local, incoming, outgoing, or relayed*.
6. To avoid the antispam and antivirus checks before archiving, check **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: C:\Program Files\Kerio\MailServer\store\archive

Select Folder...

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@feelmorelaw.eu

Archive to the local subfolder

Interval used for creating of new archive folders:

day

Compress old archive folders at:

14:20 (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

NOTE

This information is designed for Kerio Connect 9.1

1. In the administration interface, go to **Configuration > Archiving and Backup > Archiving**.

2. Select **Enable additional archiving to a remote email address for domains**.

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

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 key-in the email address.

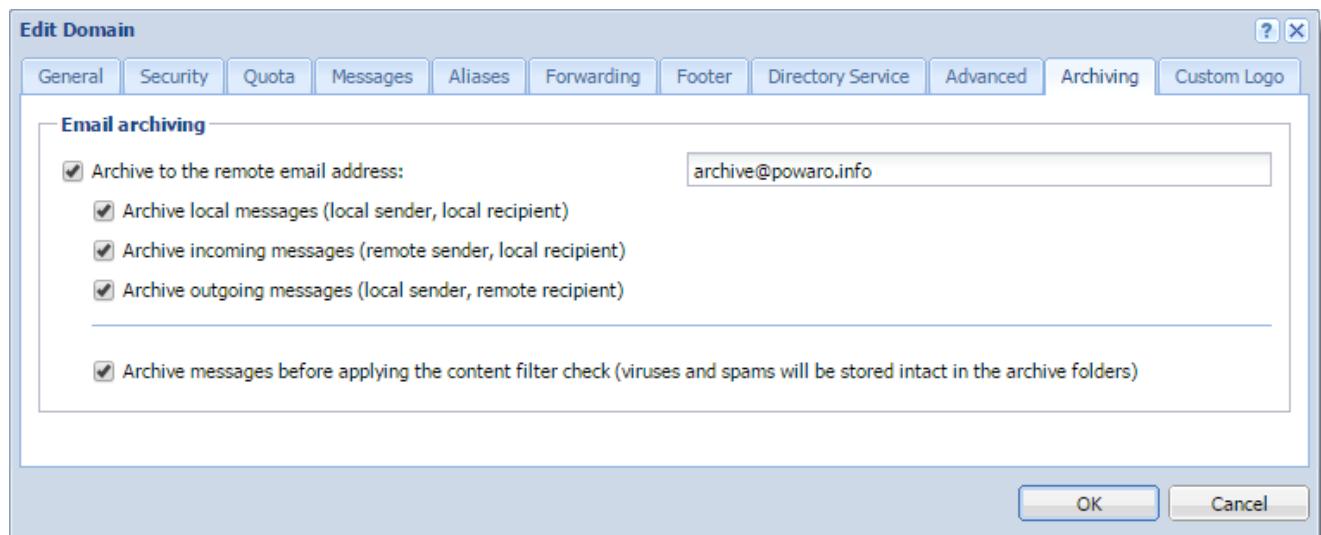
7. Select the types of messages you want to archive - incoming, outgoing, or both.

NOTE

You cannot archive relayed messages.

8. To avoid the antispam and antivirus checks before archiving, check **Archive messages before applying the content filter check**

9. Click **OK**



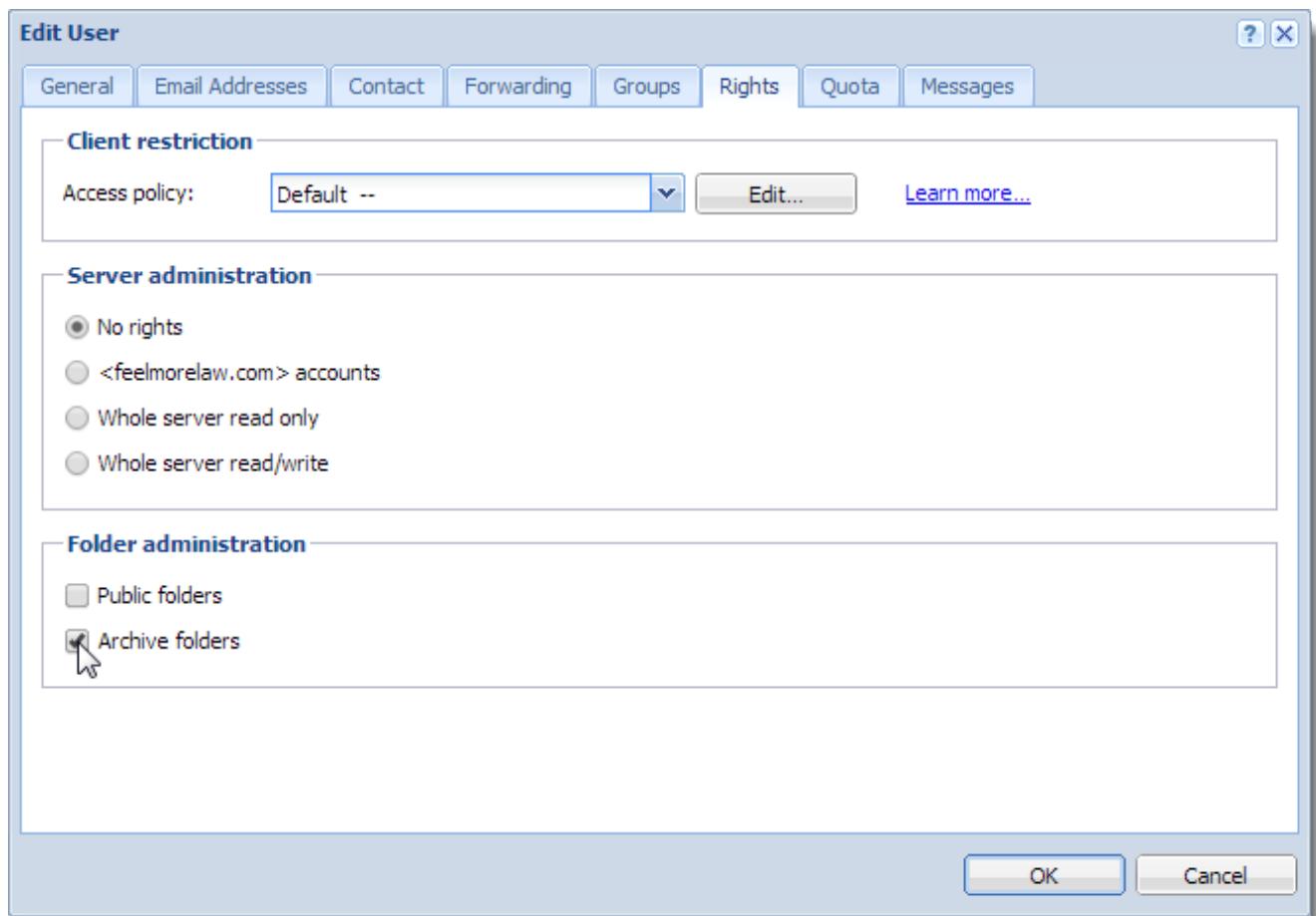
Assigning administrator rights to view archive folders

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

NOTE

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 to be viewed, it is automatically displayed in the Kerio Connect Client of users with appropriate access rights.

3.3.2 Archiving chat in Kerio Connect Client

NOTE

This information is designed for Kerio Connect 9.1

Kerio Connect automatically archives all users' chat messages sent through Kerio Connect Client.

NOTE

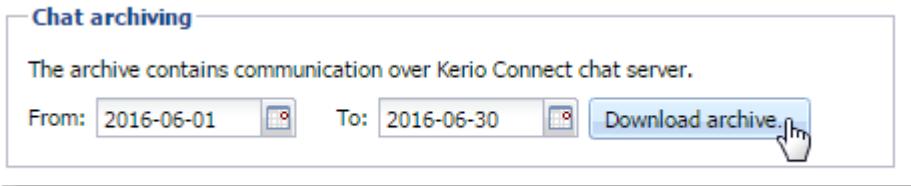
To archive only messages sent via other clients (XMPP), see [Archiving instant messaging](#).

Accessing chat archives

To download the chat archive files from the administration interface:

1. Go to **Configuration > Archiving and Backup > Archiving**.
2. In **Chat archiving**, select the time interval for the messages you want to see.

3. Click **Download archive**.
4. Save the file to your computer.



3.3.3 Archiving emails using GFI Archiver

Learn how to integrate Kerio Connect and GFI Archiver, so that emails processed by Kerio Connect are automatically archived by GFI Archiver.

GFI Archiver connects to the archive mailbox in Kerio Connect and downloads all the inbound and outbound emails from it. The emails in the archive mailbox get deleted automatically once downloaded by GFI Archiver. This way, you never lose emails, and searching emails becomes fast and easy.

Step 1: Enable Archiving in Kerio Connect

1. Log in to Kerio Connect administration interface and create a new mailbox dedicated for archiving. For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).
2. Go to **Configuration > Archiving and Backup > Archiving** and under **Email Archiving**, check **Enable email archiving** option.
3. Check **Archive to the remote email address** option and enter the email address of the journal mailbox created previously.
4. Check or uncheck the different email-types for archiving and click **Apply** to save settings.

Step 2: Connect GFI Archiver to the Kerio Connect archive mailbox

NOTE

If installing GFI Archiver on the same machine as Kerio Connect, ensure that IIS is configured to use a different port than the default port 80 since this is used by Kerio Connect.

1. Log in to GFI Archiver.
2. Go to the **Configurations** page and click **Mail Servers to Archive**.
3. Click **Add**.
4. On the **Mail Server to Archive Wizard**, select **Manual enter journal mailbox details** and click **Next**.
5. Enter the following details:

Option	Description
Mail Server	Key-in the IP address or fully-qualified domain name of the Kerio Connect mail server.
Connect using	Select IMAP .
IMAP Port	By default this is set to 143, or 993 when using SSL.

Option	Description
Use SSL	Select this option if Kerio Connect uses SSL.
Login/Password	Key in the email address and password of the Journal mailbox.
Folder	Select the mailbox folder from where to pick up emails to archive. By default this is set to Inbox and requires no change.

6. Click **Finish** to finalize setup.

Once you complete this procedure, you can test the integration by sending a test email to any Kerio Connect mail account and check if it is getting displayed under [Archived Items](#) in GFI Archiver.

3.4 Backup

This section provides information about server backup and data recovery.

3.4.1 Configuring backup in Kerio Connect	165
3.4.2 Data recovery in Kerio Connect	168
3.4.3 Examples of data recovery in Kerio Connect	170

3.4.1 Configuring backup in Kerio Connect

You can backup the following items in Kerio Connect:

- » User mailboxes
- » Public folders
- » Mailing lists
- » Configuration files
- » Licenses
- » SSL certificates
- » SpamAssassin database

You can use any removable or network disk for storing backups.

Configure backups in section **Configuration > Archiving and Backup**.

NOTE

[Temporarily disabled users](#) are not included in the backups.

Types of backups

Kerio Connect supports **Full backup** that stores all files and items, and it also supports **Differential backup** that stores files that have been added or changed since the last full backup.

You can schedule any number of full and differential backups by considering 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.

 Archiving and Backup

[Logout](#)

[Archiving](#) [Backup](#)

Enable message store and configuration recovery backup

Backup scheduling

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

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

[Add...](#) [Edit...](#) [Remove](#) [Advanced...](#)

Target backup directory

Backup directory: [Select Folder...](#)

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

! If the backup directory is on the network drive, you may need to specify username and password. [Specify...](#)

Notification

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

Current status

[Start Now](#)  Last backup finished successfully.

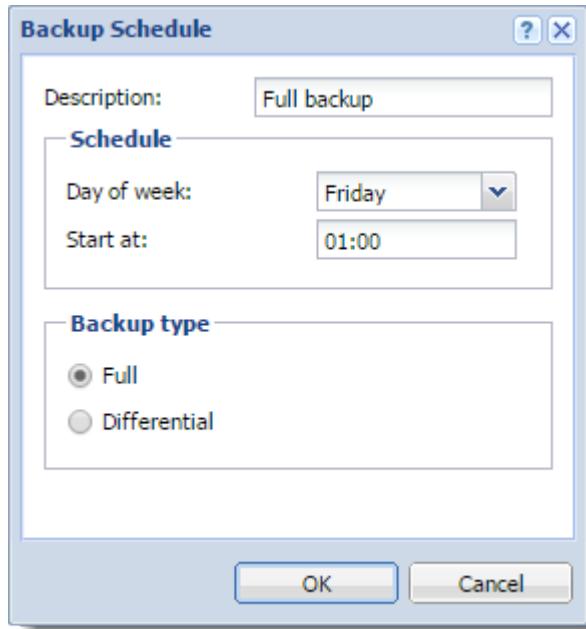
[Apply](#) [Reset](#)

Configuring backups

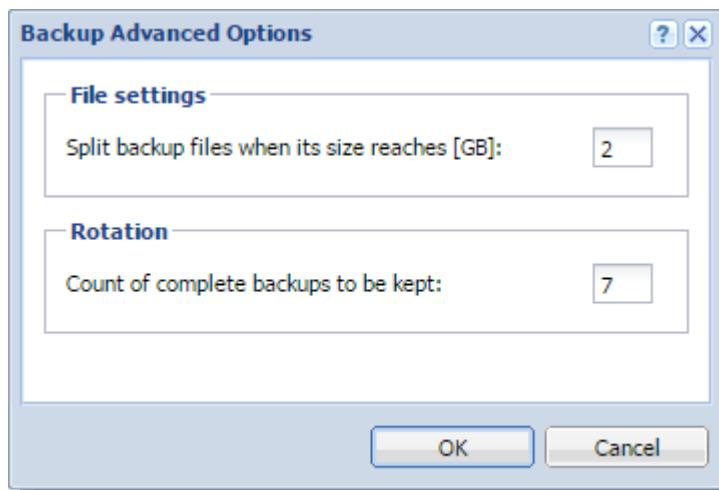
You must have full access rights to administration or you can use the built-in administrator account. For more information, refer to [Setting access rights in Kerio Connect](#) (page 209).

To configure the backup schedule:

1. In the administration interface, go to **Configuration > Archiving and Backup > Backup**.
2. Check **Enable message store and configuration recovery backup**.
3. Click **Add**.
4. Type a description for the backup.
5. Select the time and the type of the backup and click **OK**



6. Repeat steps 3-5 for additional backups.
7. Click **Advanced** 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 key-in the username and password (Microsoft Windows only).

NOTE

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

For more information, refer to [Data recovery in Kerio Connect](#) (page 168).

Data recovery examples

For more information, refer to [Examples of data recovery in Kerio Connect](#) (page 170).

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).

3.4.2 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 the Kerio Connect Recover tool:

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, if the path to the Kerio Connect installation directory is included in the path variable, use:

```
./kmsrecover [advanced options] <directory_name>|<file_name>
```

NOTE

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).

Abbreviation	Full option	Mask	Description
-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 <value></code> or <code>--mask=<value></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> .
	mail		Recover only the <code>\store\mail</code> directory.
	lists		Recover only the configuration of mailing lists, the <code>\store\lists</code> directory.
	spamassassin		Recover only the SpamAssassin database.
	license		Recover the Kerio Connect license.
	sslca		Recover SSL certificates issued by certification authorities.
	sslcert		Recover the Kerio Connect certificates.
	public		Recover public folders.
-b	--backup		Performs an additional back-up before the recovery starts. The original directory will have the <code>BAK</code> 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	--noprogress		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 <code>-d</code> and <code>-u</code> , 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:

Backup type	Abbreviation	Backup File name example
Full backup	F	<code>F20120118T220007Z.zip</code> The file name is interpreted as follows: » F — full backup » 2012 — year » 01 — month » 18 — day » T220007Z — GMT timestamp (22:00:07); always starts with T and ends with Z.

Backup type	Abbreviation	Backup File name example
Differential backup	D	D20120106T220006Z.zip The file name is interpreted as follows: » 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 The file name is interpreted as follows: » C - Backup copy or Manual backup » 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:

File/Directory name	Description
.version.txt	This file 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	This 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	This file stores Kerio Connect configuration that includes all settings done in the administration interface.
users.cfg	This file contains all users and their parameters as set in the Kerio Connect's administration interface.
.summary.txt	This file 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).

For more information, refer to [Examples of data recovery in Kerio Connect](#) (page 170).

If any problem with backups occurs, consult the **Debug log** (Right-click the Debug log area, click **Messages**, and select the **Store Backup** option).

3.4.3 Examples of data recovery in Kerio Connect

The following sections contain examples of recovery of backed-up data in Kerio Connect.

- » [Data recovery on Windows](#)
- » [Data recovery on Mac OS X](#)

- » Data recovery on Linux

Data Recovery on Microsoft Windows

This topic contains a few general examples of data recovery on 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.

NOTE

If the 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.

NOTE

If the 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 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.zip`
3. The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers the `Sent Items` folder.

NOTE

If the 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`

The `kmsrecover` detects the path to the store automatically in the Kerio Connect's configuration file and recovers the public folders.

NOTE

If the parameter contains a space in the directory name, enclose it in quotes: `kmsrecover "E:\backup 2"`

Data Recovery on Mac OS X

This topic contains a few general examples of data recovery on Mac OS X.

Full backup recovery

Conditions

- » The configuration data is stored 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: `./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/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: `/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/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 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.

Data Recovery on Linux

This topic contains a few general examples of data recovery on Linux.

Full backup recovery

Conditions

- » The configuration data is stored at the default location: /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/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 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.

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.

3.5 Data store

This section provides information about data store configuration.

3.5.1 Configuring data store in Kerio Connect	176
3.5.2 Automatic data consistency check and fix in Kerio Connect	179

3.5.1 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.

NOTE

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

2. In the Kerio Connect administration interface, go to **Configuration > Advanced Options > Store Directory**.
3. Select the new folder in the new location. Do not use a UNC path. Click **Apply**.
4. Stop Kerio Connect.
5. Copy all files from the old store directory to the new directory.
6. Run Kerio Connect.

The screenshot shows the 'Advanced Options' window in the Kerio Connect administration interface. The 'Store Directory' tab is active. The 'Directory location' section shows the path 'C:\Program Files\Kerio\MailServer\store' and a note about stopping the server if the path is changed. The 'Full text search' section has 'Enable full text search' checked, with an index location of 'C:\Program Files\Kerio\MailServer\store\fulltext'. It shows an index status of 'Rebuilding (26 users remaining)' and an index size of '0 MB, 145697 MB of disk space available', with a 'Rebuild Index...' button. The 'Storage space watchdog (minimum of free disk space required)' section sets a soft limit of 1 GB and a hard limit of 65 MB. The 'User quota' section sets a warning limit of 90% and sends messages to 'admin@company.com' every day. At the bottom are 'Apply' and 'Reset' buttons.

Configuring the full text search

In Kerio Connect, users can search their items using the full text search feature.

NOTE

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 Directory**.
2. Select the **Enable full text search** option.
3. Specify a folder for storing the fulltext search index.

NOTE

Do not use a UNC path.

Full text search

Enable full text search

Index location:

! Network storage is not recommended. [Learn more...](#)

Index status: Up-to-date

Index size: 4260 MB

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



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.

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.

Screenshot 12: Setting the data store notification limits

Limit type	Description
Watchdog Soft Limit	If the free space on the data store disk drops below this value, Kerio Connect displays a warning message in the administration interface.
Watchdog Hard Limit	If the free space on data store disk 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](#).

3.5.2 Automatic data consistency check and fix in Kerio Connect

This topic describes possible options and steps available in **Kerio Connect** to do message store consistency check.

IMPORTANT

The information present in this topic is valid for Kerio Connect 7.3.0 and newer.

Kerio Connect automatically walks through data storage on background and performs check of auxiliary files and fix in case of detected corruption. It is possible to run fix of corrupted data directly from web administration for specific users or for public folders.

For the user folder

1. Log into the Kerio Connect Administration with a user account that has read/write rights within the Administration.
2. Within the Administration, go to **Accounts > Users**
3. Select one or more users and right-click. Select **More Actions... > Reindex Mailbox**

For Public folders

1. Log into the Kerio Connect Administration.
2. Within the Administration, go to **Configuration > Domains**
3. Click on the **Public Folders...** button and press **Reindex Folders**

NOTE

All detected errors, are logged into Error or Warning logs.

Schedule of automatic storage check

- » Complete check of all folders on the server
 - Immediately after startup (starts in first 30 seconds)
 - Every 6 hours
- » Fix of corrupted **properties.fld** files, which contains extended messages attributes.
 - 1 hour after startup
 - Every 7 days

Beside of periodic check, corruption can be also detected during user's access to folder, in that case is folder added to automatic check queue and almost immediately is checked and fixed. Corrupted calendar and contact folders are processed with higher priority.

Check on each folder consists of the following steps:

- » Check the file with information about folder **status.fld**, and in case of file corruption, default values of missing attributes are used.
 - If **status.fld** doesn't exist and folder is not one of standard folders (Inbox, Calendar, Contacts, etc.), folder is not valid and is not listed in client applications.
- » Check the file with information about messages **index.fld**

- If any corruption is detected or if file is not found, index is reconstructed from messages physically stored in folder **#msgs**.
 - If the index is valid, but its records doesn't correspond to physical messages on the disk (in folder **#msgs**), redundant records are removed from index and missing messages are supplemented.
- » Check consistency of file **search.fld**, which is used to search in messages.

- If corruption is detected, the file is removed and completely reconstructed.

» Detection of invalid name of messages, used by WebDAV protocol (called DAV-names) and fix of the names.

As part of automatic control following additional actions are performed:

» Old messages are deleted, according to appropriate server settings – i.e. feature **Items Clean-out** and **Deleted Items Recovery** in domain settings.

» Check and fix of folder **#deleted**, in which are archived deleted messages, which can be restored by feature **Recover Deleted Items**.

» Check database of shared folders, which is used in CalDAV protocol, i.e. file .caldav.db.

» If more folders with the same GUID identification are detected, identification of one folder is automatically changed by newly generated.

» Fix of corrupted UIDs of calendar events.

3.6 Instant Messaging

Kerio instant messaging service is based on XMPP, an open technology for real-time communication.

3.6.1 Configuring instant messaging in Kerio Connect	180
3.6.2 Configuring DNS for instant messaging	184
3.6.3 Archiving instant messaging	186
3.6.4 Enabling chat in Kerio Connect Client	187
3.6.5 Configuring clients for instant messaging	189
3.6.6 Initiating group chat in instant messaging	194

3.6.1 Configuring instant messaging in Kerio Connect

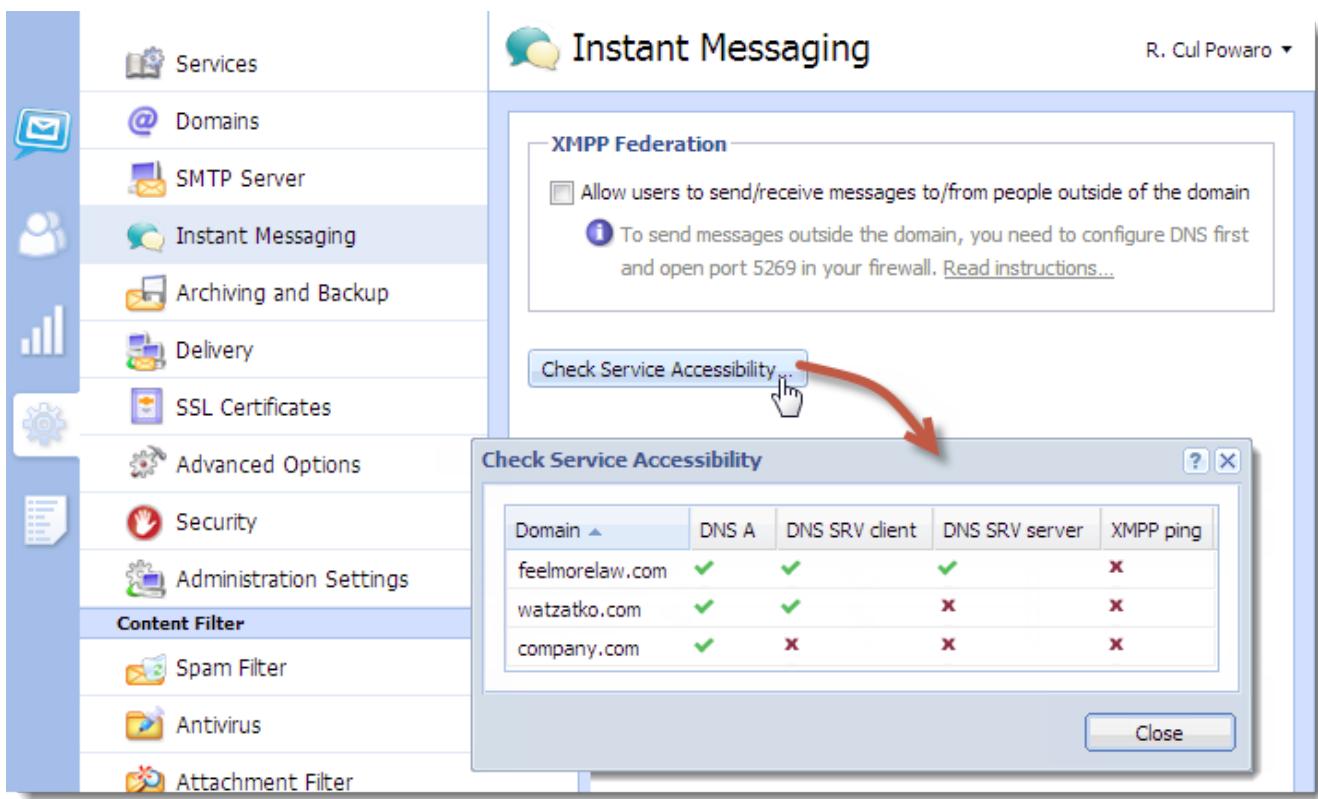
NOTE

For information about sending 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**.



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. For more information, refer to [Configuring DNS for instant messaging](#) (page 184).

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**).

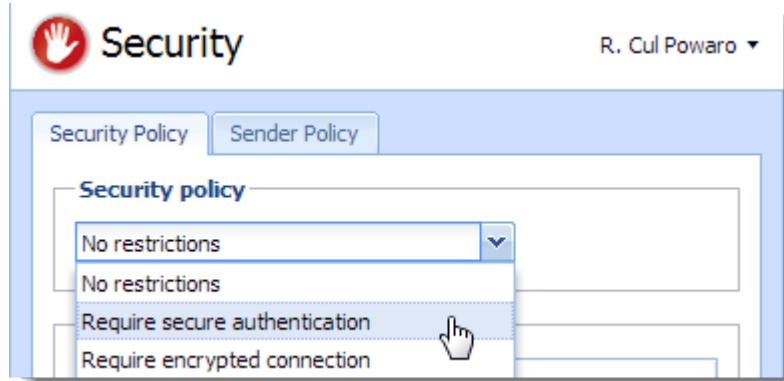
NOTE

Remember to configure DNS for instant messaging.

Securing instant messaging

We recommend to secure instant messaging by using TLS:

- » set [security policy](#) to require encrypted connection or secure authentication in section **Configuration > Security > tab Security Policy** ([Configuration > Advanced Options > tab Security Policy](#) for Kerio Connect 8.1 and older)



- » use unsecured instant messaging [service](#) (port 5222)

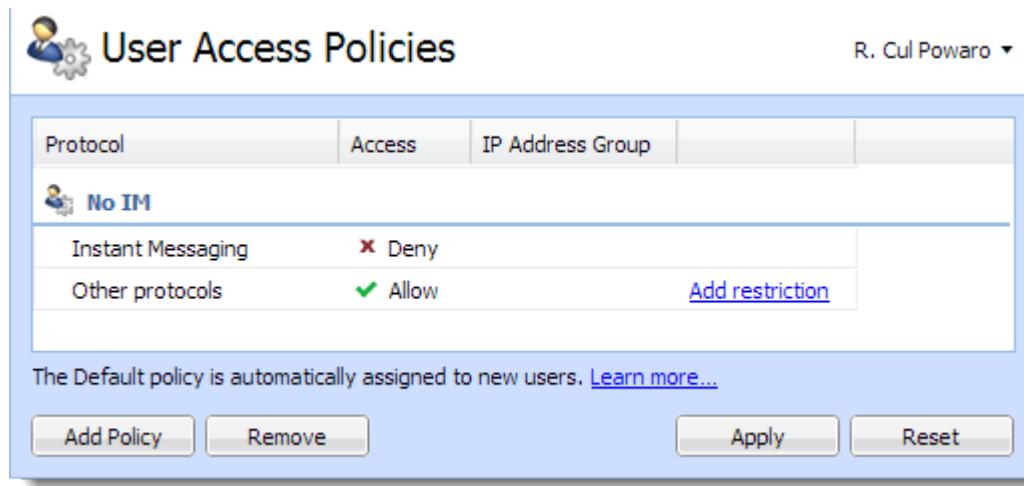
You can also enable only the secure instant messaging service (port 5223) and use SSL.

Security policy is applied to all services in your Kerio Connect.

Limiting access to instant messaging

If you need to restrict access to any users, you can define [User Access Policies](#) to:

- » disable access to IM
- » restrict access IM to specific addresses



To display which users are connected to the IM server, go to section [Active Connections](#) in the administration interface.

Disabling instant messaging

You can disable instant messaging by stopping the instant messaging services. (For more information, refer to [Services in Kerio Connect](#) (page 403).)

Archiving instant messages

For more information, refer to [Archiving instant messaging](#) (page 186).

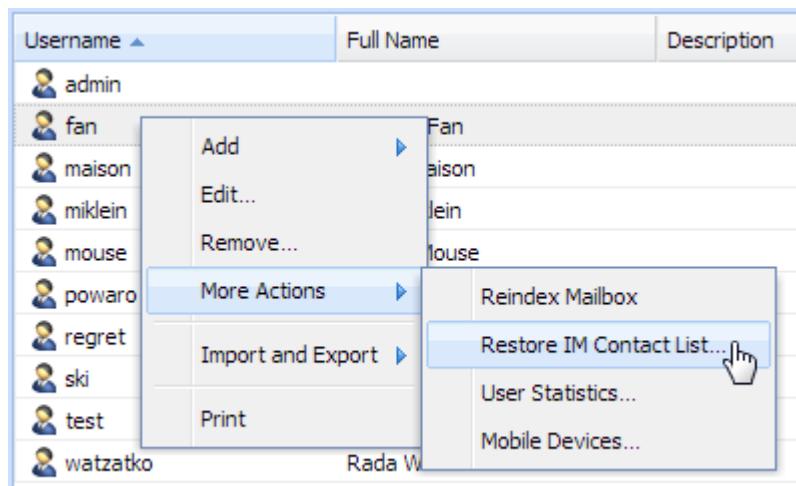
Automatic contact list

Kerio Connect automatically creates contact lists of all domain users who are published in the [global address list](#).

Once users login to an [IM client](#), their account will display list of contacts of users from their domain (**Colleagues**).

If a user is having problems with their contact list (e.g. if they delete any users), you can restore their contact list:

1. In the administration interface, go to section **Accounts > Users**.
2. Right-click the user and select **More Actions > Restore IM Contact List**.
3. Confirm.



Restoring contact lists discards any changes the user has made to their **Colleagues** list. Added contacts will remain preserved.

Maximum size of the automatic contact list

Maximum number of users in the automatic contact list is set to 300. The users who exceed this number are not included in the **Colleagues** contact list and also their contact list is empty.

To change the maximum size of the contact list:

1. Stop the Kerio Connect engine.
2. Open the `mailserver.cfg` file.
3. Edit the following line:
`<variable name="RosterMaximum">300</variable>`

To disable the automatic contact list completely, set the `MaximumRoster` value to 0 (zero).

4. Save the file.
5. Start the Kerio Connect engine.

Kerio Connect saves the information about exceeding the maximum number of users in the [Warning log](#).

NOTE

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 more information, refer to [Configuring clients for instant messaging](#) (page 189).

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.

3.6.2 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 more information, refer to [Configuring instant messaging in Kerio Connect](#) (page 180).

You must add SRV records on your DNS server or use the management interface of your DNS registrar to add the records.

NOTE

Visit [XMPP wiki](#) 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.
```

Fields	Description
Service	<code>_xmpp-server</code>
Protocol	<code>_tcp</code>
Hostname/Name	Your domain name

Fields	Description
Priority	Priority of the target
Weight	Weight for records of the same priority
Port	5269
Target/Value	Your server hostname
TTL	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)

IMPORTANT

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.
```

Fields	Description
Service	<code>_xmpp-client</code>
Protocol	<code>_tcp</code>
Hostname/Name	Your domain name
Priority	Priority of the target
Weight	Weight for records of the same priority
Port	Port for communication from client to server
Target/Value	Your server hostname
TTL	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

3.6.3 Archiving instant messaging

NOTE

If you want to archive chat messages from Kerio Connect Client, read [Archiving chat in Kerio Connect Client](#).

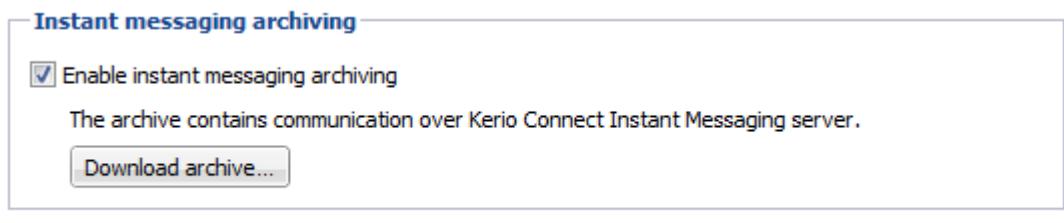
If you want to look at any instant message later, Kerio Connect can archive all [instant messages](#) sent to or from your users.

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).

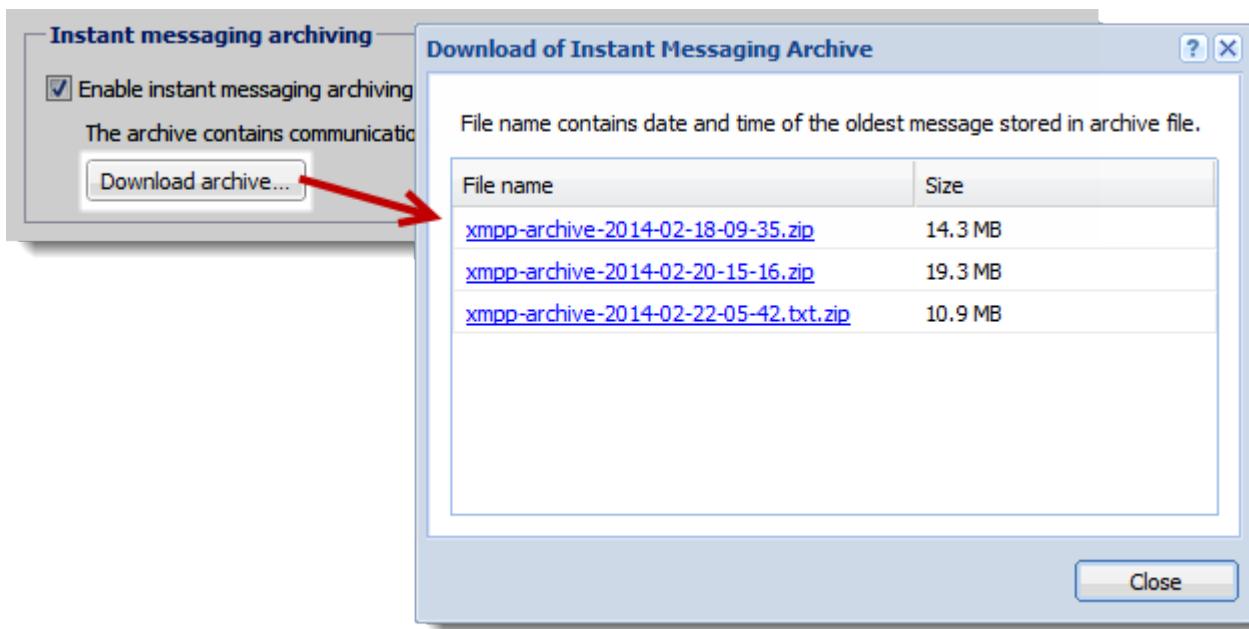
The default maximum size of the archive files is 50 MB. Once the archive file reaches 50 MB, a new file is created.

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:

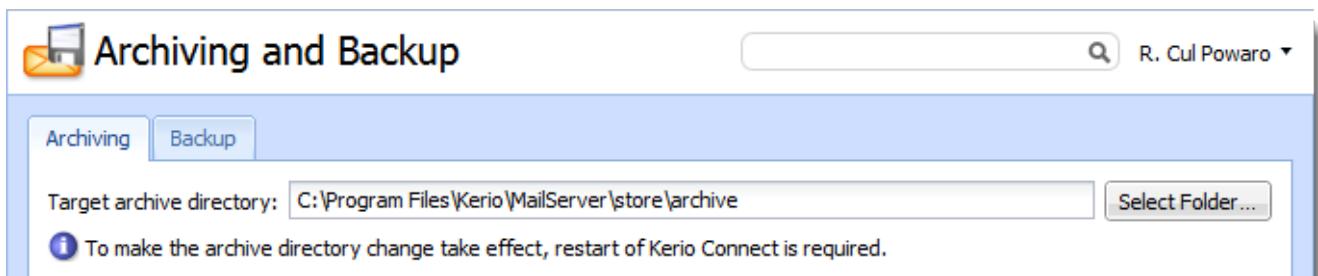
1. Go to **Configuration > Archiving and Backup > tab Archiving**.
2. In **Instant messaging archiving**, click **Download archive**.



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.



3.6.4 Enabling chat in Kerio Connect Client

NOTE

New in Kerio Connect 9.1!

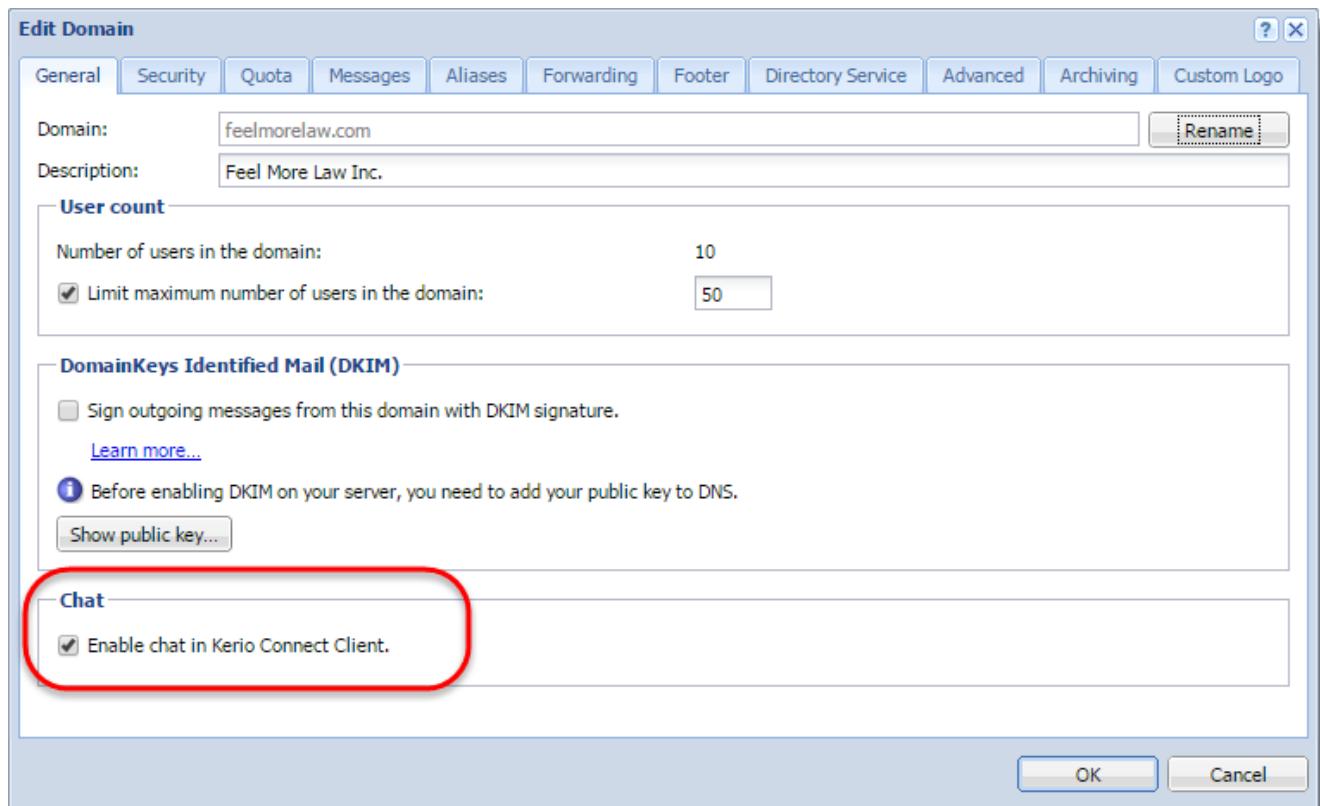
Kerio Connect Client includes a **Chat** feature for exchanging instant messages. Chat enables users to view their colleagues' online status, and to chat with them in real time. This is useful when they cannot wait for an email response or prefer a quick back-and-forth conversation without the use of 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**.
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. For more information, refer to [Archiving chat in Kerio Connect Client](#) (page 163).

Using Kerio Connect Client chat

For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1902

Troubleshooting

If any problem with Kerio Connect Client chat occurs, consult the following [logs](#):

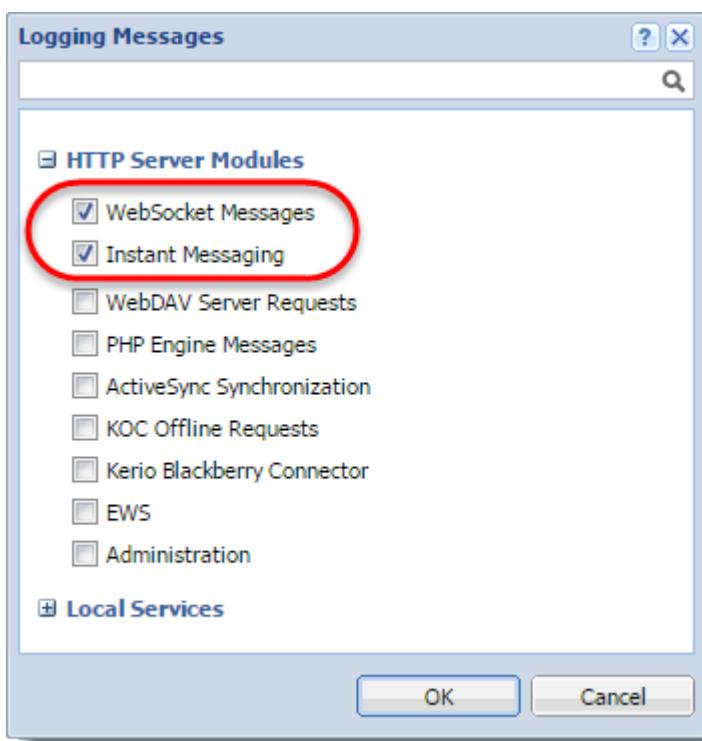
- » **Warning**
- » **Error**
- » **Debug**

To enable Debug:

1. Right-click in the Debug log area, and click **Messages**.
2. Select the **Instant Messaging** and **WebSocket Messages** options.
3. Click **OK**

NOTE

After debugging, clear those options. Otherwise, the logging may slow down server performance.



3.6.5 Configuring clients for instant messaging

Recommended IM clients

NOTE

For information about sending chat messages through Kerio Connect Client, read [Sending chat messages in Kerio Connect Client](#).

Kerio instant messaging service is based on XMPP, an open technology for real-time communication.

Kerio Connect recommends the following instant messaging clients:

- » [Pidgin](#) for Microsoft Windows
- » [Psi](#) for Linux

- » [Messages \(iChat\) for Mac OS X](#)

Supported features

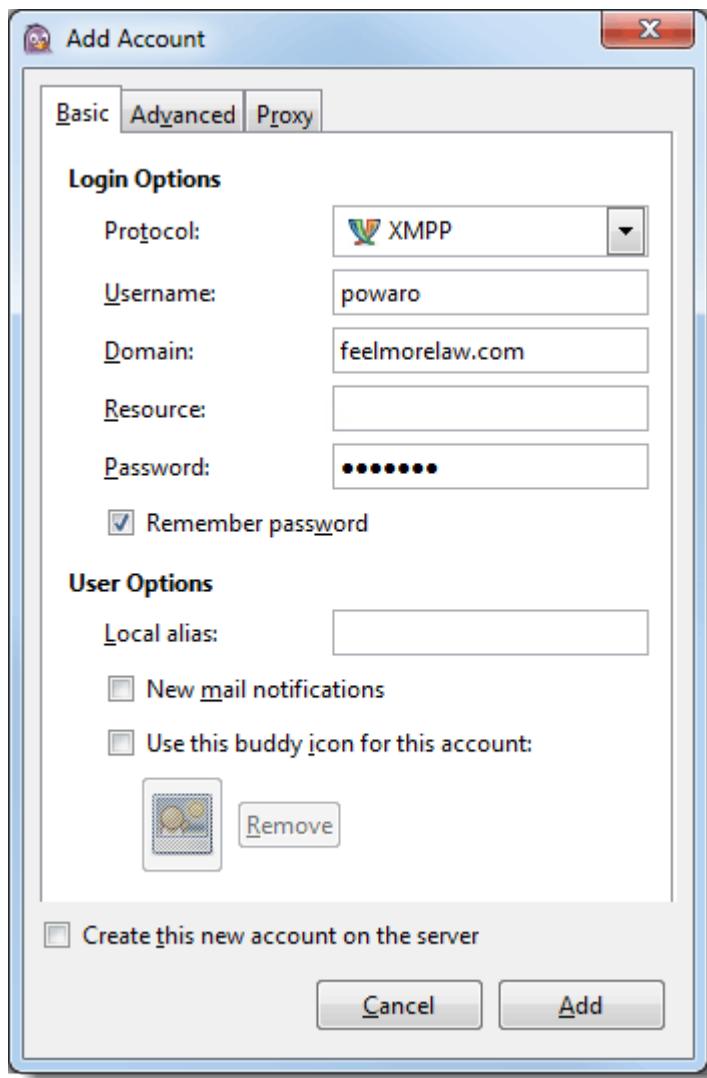
Kerio instant messaging service supports the following features:

- » sending rich text messages
- » presence notifications
- » sharing files
- » auto-populated contact list of your colleagues
- » synchronization of contact photos
- » auto-configuration on Mac
- » audio/video chat (availability depends on your IM client)
- » talking with multiple users in a single chat room (For more information, refer to [Initiating group chat in instant messaging](#) (page 194).)

Configuring Pidgin for Microsoft Windows

To configure the Pidgin client, follow these steps:

1. Download and install [Pidgin](#).
2. Run the application and click **Accounts > Manage Accounts > Add**.
3. Fill in the information — protocol (**XMPP**), your username and password, your domain.
4. Save the account.



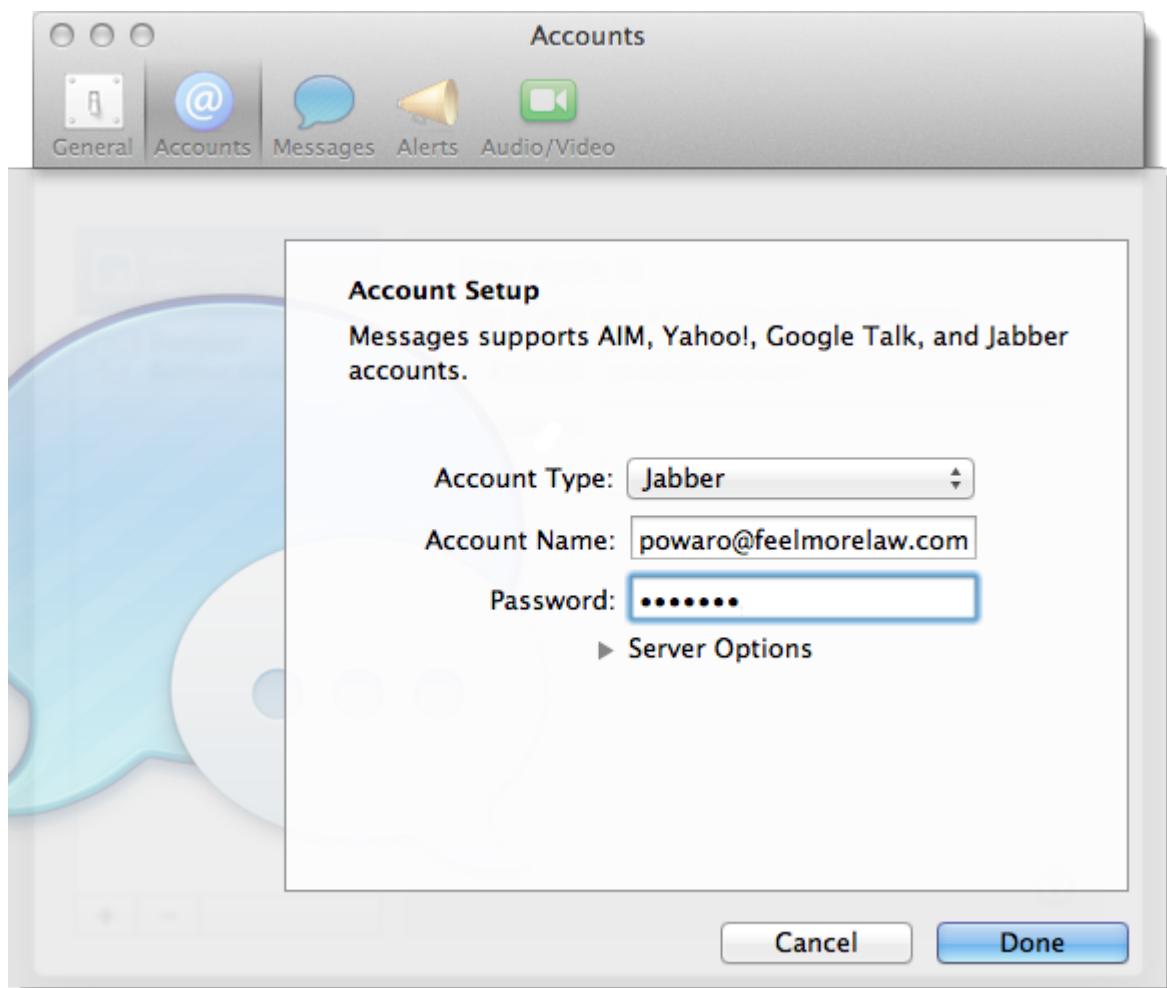
Configuring Messages on Mac OS X

To auto-configure **Messages** on Mac OS X, use [Kerio Connect Account Assistant](#).

For manual configuration, follow these steps:

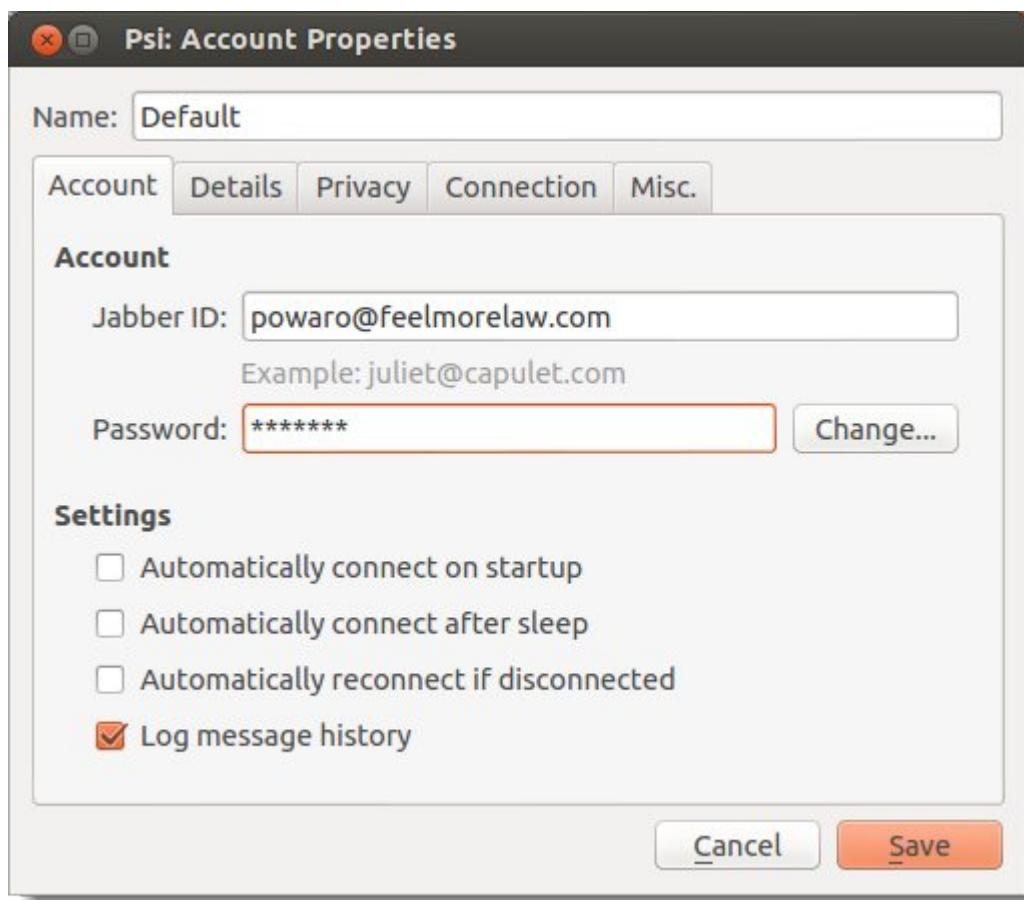
1. Go to Messages to **Preferences > Accounts**, and click the plus sign.
2. Fill in the information — protocol (**Jabber**), account name (you username including the domain) and password.
3. Save the account.

Use similar settings for iChat.



Configuring Psi on Linux

1. Download and install [Psi](#).
2. Run the application and click **General > Account Setup > Add**.
3. Fill in the information — XMPP address (your username including the domain) and password.
4. Save the account.



Contact lists

When you login to your account in an IM client for the first time, a list of all your **Colleagues** will be created. You can move them into other folders or delete them (see section [Troubleshooting](#) on how to restore this contact list).

You can create additional contact lists and add other contacts depending on the client you use.

Troubleshooting

Contact list

If you have problems with your company contacts (**Colleagues**), ask your administrator to restore your contact list.

NOTE

Any change you have previously made to the **Colleagues** list will be lost. Your external contacts will remain preserved.

Cannot connect to your account

If you cannot connect to your account, check your [DNS settings for client auto-configuration](#) or configure the clients manually:

Pidgin

Go to **Modify Account > tab Advanced** and use one the following configurations:

- » uncheck option **Require encryption**, add your server address and port 5222, or
- » set Connection Security to **Use old-style SSL**, add your server address and port 5223

Messages

Go to **Account Settings > tab Server Settings** and use one the following configurations:

- » uncheck option **Use SSL**, add your server address and port 5222, or
- » check option **Use SSL**, add your server address and port 5223

Psi

Go to **Modify Account > tab Connection**, check option **Manually Specify Host/Port** and use one the following configurations:

- » set Encryption Connection to **Always**, add your server address (Host) and port 5222, or
- » set Encryption Connection to **Legacy SSL**, add your server address (Host) and port 5223

3.6.6 Initiating group chat in instant messaging

About group chat in instant messaging

NOTE

New in Kerio Connect 8.2!

If you use [instant messaging](#) in Kerio Connect and want to chat with multiple users and share thoughts with all of them together, you can create a temporary chat room, i.e. **group chat**.

Kerio Connect does not require any additional settings to use group chats.

The server address for group chats is `conference . [your_domain_name]`, for example `conference.feelmorelaw.com`.

This article describes group chat in:

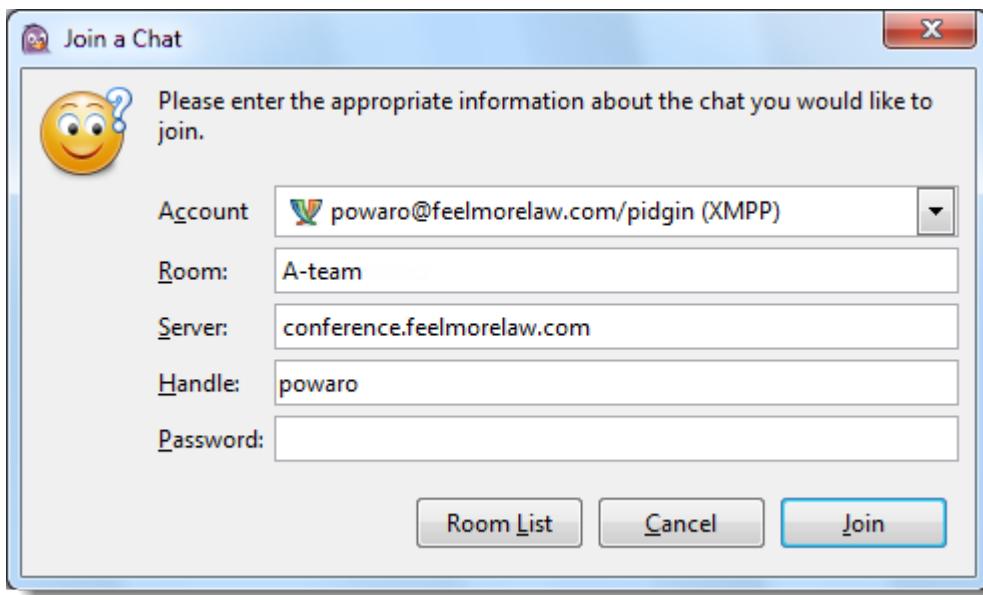
- » [Pidgin for Microsoft Windows](#)
- » [Messages for Mac OS X](#)
- » [Psi for Linux](#)

For information on initial configuration of instant messaging clients, read article [Configuring clients for instant messaging](#).

[Pidgin for Microsoft Windows](#)

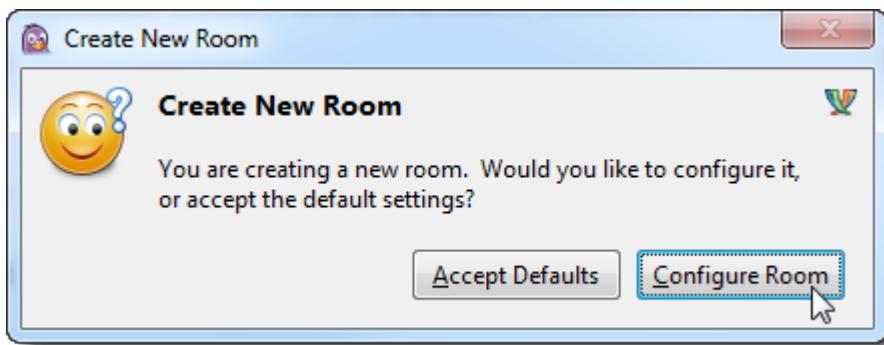
[Initiating group chat in Pidgin](#)

1. In your Pidgin, click **Buddies > Join a Chat**.
2. Select account, type a room name, server, your nickname (**Handle**).



3. Click **Join**.

4. To configure the chat room (e.g. secure the room with a password), click **Configure Room** and set parameters. You cannot change the parameters later.



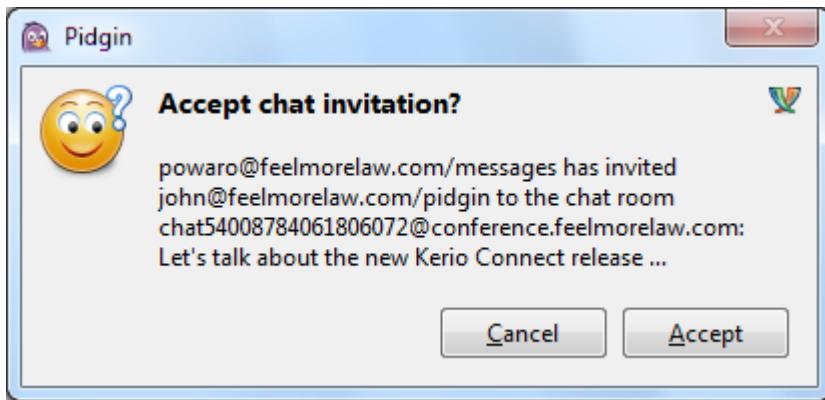
5. Confirm the settings.

Inviting people to group chat in Pidgin

To invite people to a group chat, drag them from your contact list to the room list or click **Conversation > Invite**.

Joining and leaving group chats in Pidgin

If you receive an invitation, click **Accept** to join the group chat.



You can also search through existing chat groups by clicking on **Buddies > Join a Chat > Room List > Find Rooms**.

To leave a room, close the chatroom window.

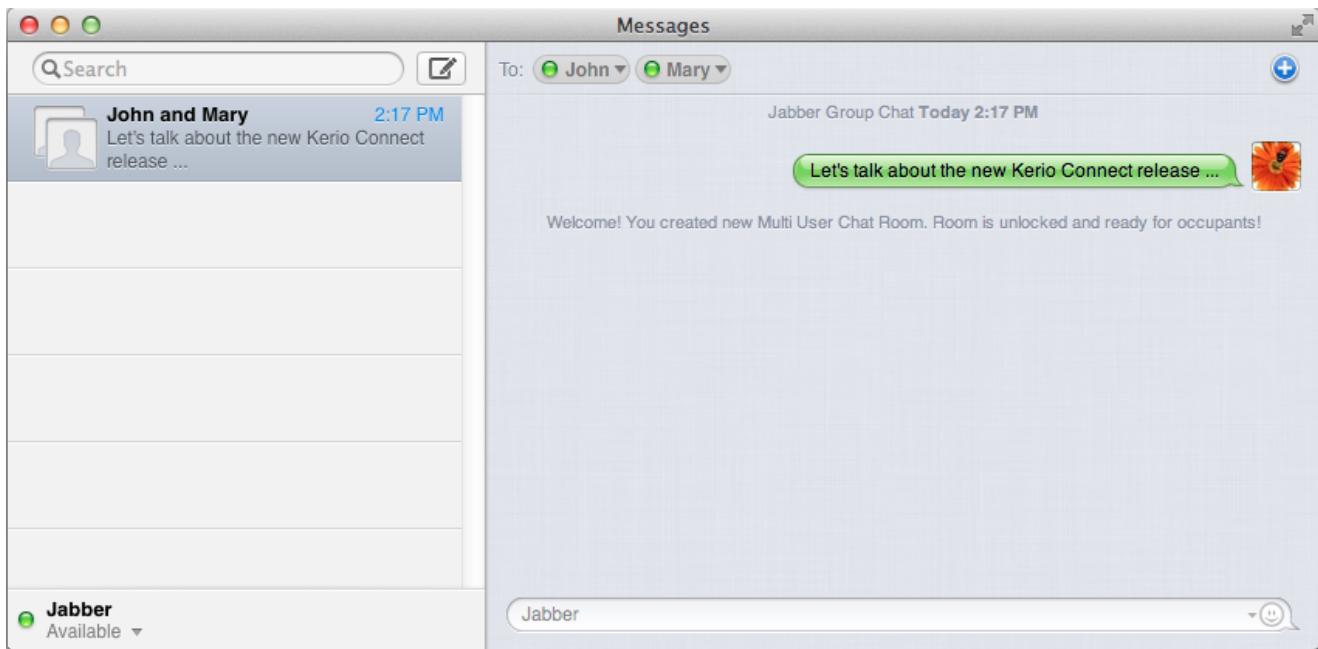
Messages for Mac OS X

Initiating group chats in Messages

To create a group chat, add at least two users to a conversation.

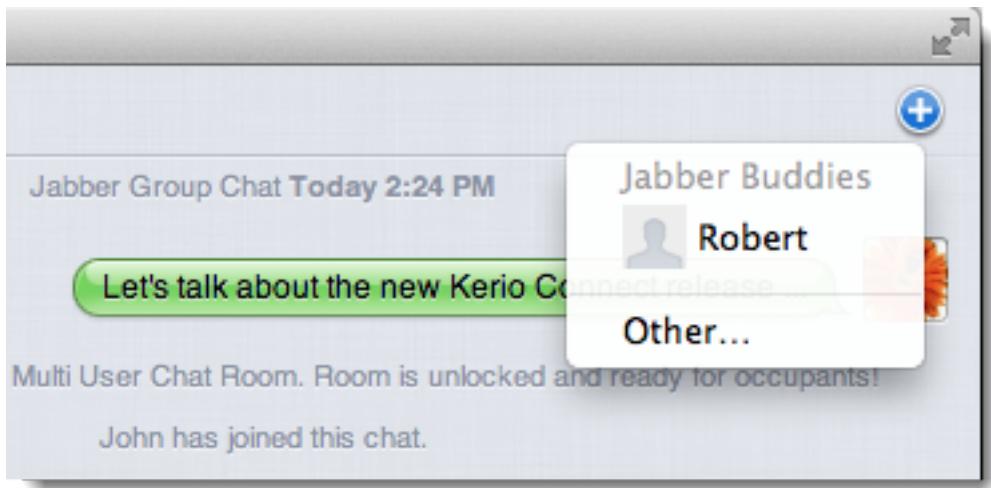
1. Initiate a conversation in **Messages**.
2. Add users to this conversation.

Users receive an invitation and you can start chatting.



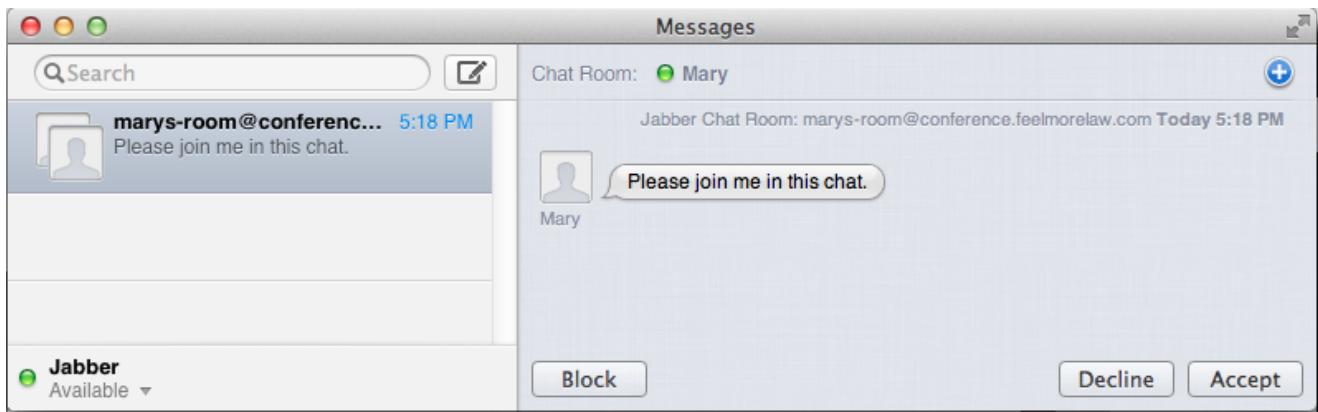
Inviting people to group chats in Pidgin

To invite people to a multi user chat room, click the blue plus icon and invite users.



Joining and leaving group chats in Messages

To join a group chat, select it from the list of chats and click **Accept**.



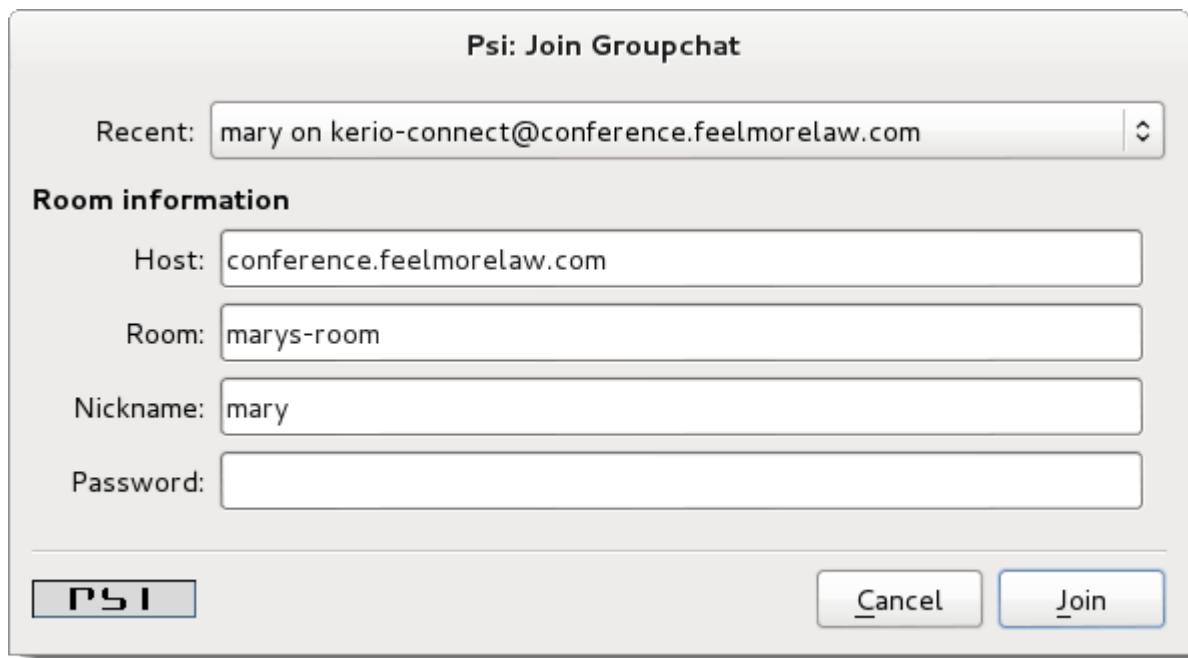
To leave a chat room, delete it from the list of chats.

Psi for Linux

Initiating group chat in Psi

1. In your Psi, click **General > Join Groupchat**.
2. Type a conference host, room name, server, your nickname.

If you want to protect the chat room, type a password.



3. Click **Join**.

4. To configure the chat room (e.g. secure the room with a password), click the down arrow above the user list and select **Configure Room**.

Room Configuration

Affiliations General

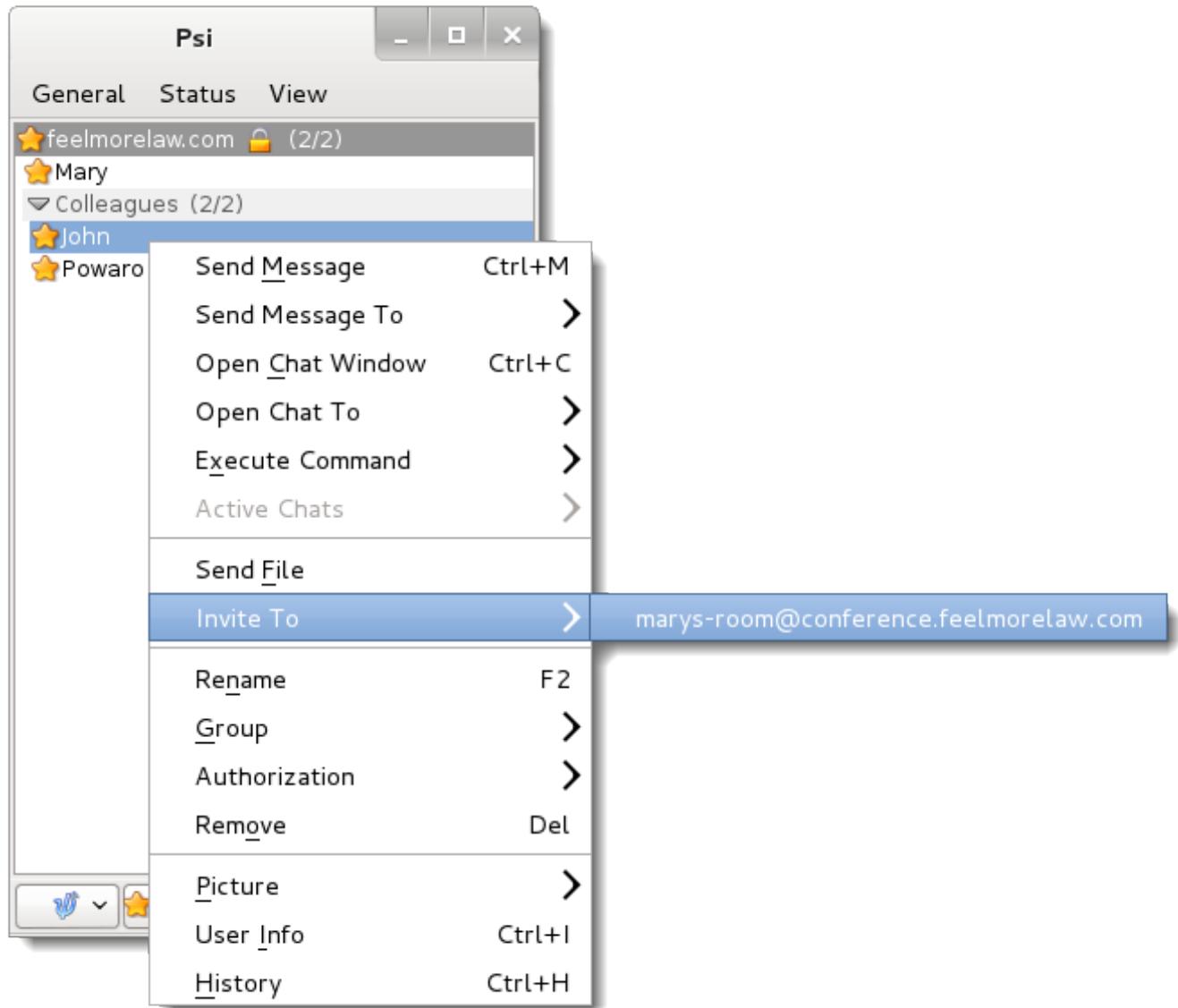
Natural-Language Room Name:	<input type="text"/>
Short Description of Room:	<input type="text"/>
Make Room Persistent?:	<input type="checkbox"/>
Make Room Publicly Searchable?:	<input checked="" type="checkbox"/>
Make Room Moderated?:	<input type="checkbox"/>
Make Room Members Only?:	<input type="checkbox"/>
Password Required to Enter?:	<input type="checkbox"/>
Password:	<input type="password"/>
Room anonymity level::	<input type="button" value="Semi-Anonymous Room"/>
Allow Occupants to Change Subject?:	<input type="checkbox"/>
Enable Public Logging?:	<input type="checkbox"/>
Logging format::	<input type="button" value="HTML"/>
Maximum Number of History Messages Returned by Room:	<input type="text" value="50"/>

PSI

5. **Apply** the settings.

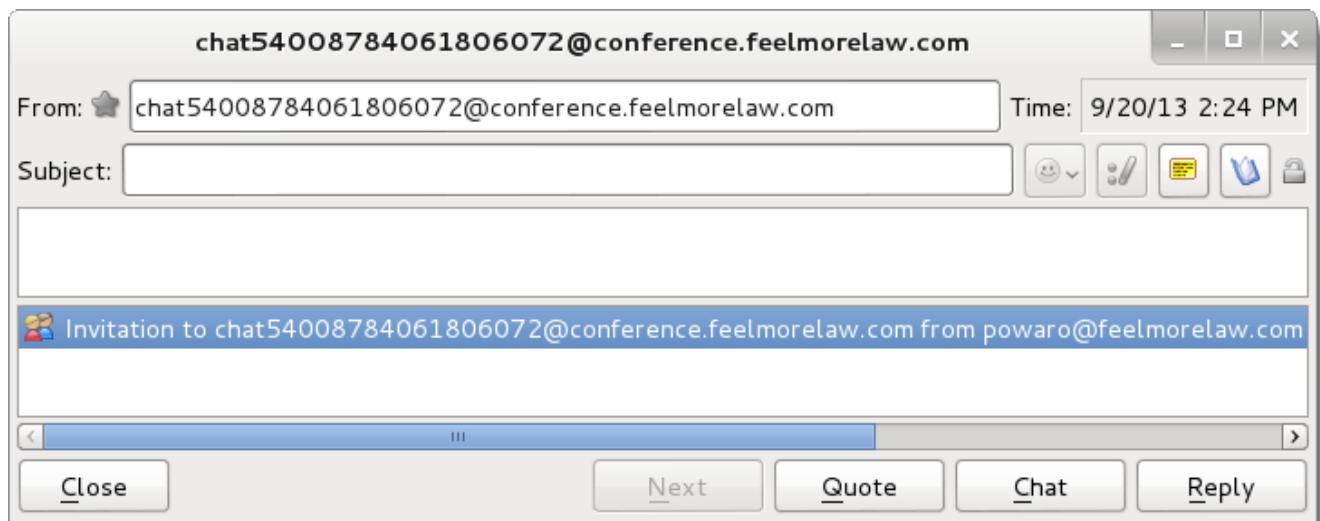
Inviting people to group chat in Psi

To invite people to a group chat, select a person in your contact list and click **Invite To**.



Joining and leaving group chats in Psi

To accept an invitation to a group chat, double-click the invitation text inside the event dialog and click **Join**.



To leave a room, close the chat room window.

4 Settings

This section contains information about:

4.1 Basic configuration	202
4.2 Administration	242
4.3 Domains	248
4.4 Accounts	268
4.5 Directory service	293
4.6 Security	323
4.7 Mail delivery and DNS records	390
4.8 Services	403

4.1 Basic configuration

This section contains information about:

4.1.1 Accessing Kerio Connect	203
4.1.2 Authenticating users through PAM	204
4.1.3 Public folders in Kerio Connect	205
4.1.4 Setting access rights in Kerio Connect	209
4.1.5 Creating time ranges in Kerio Connect	212
4.1.6 Configuring IP address groups	213
4.1.7 Managing logs in Kerio Connect	215
4.1.8 Customizing Kerio Connect	217
4.1.9 Customizing the Kerio Connect Client login page	222
4.1.10 Filtering messages on the server	224
4.1.11 Integrating Kerio Connect with Kerio Operator	234
4.1.12 Joining two servers with different domains into one server	235
4.1.13 Changing the time zone definitions in <code>timezones.xml</code> file in Kerio Connect	236
4.1.14 How to change from individual public folders to global public folders and keep your existing public folder data	238
4.1.15 Upgrading the MAPI property database in Kerio Connect 9.1	239
4.1.16 Using Kerio Assist tool	241

4.1.1 Accessing Kerio Connect

Kerio Connect includes two interfaces:

- » Kerio Connect administration for administrators
- » Kerio Connect Client for users

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 administration

For more information, refer to [Accessing Kerio Connect administration](#) (page 242).

NOTE

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.

Kerio Connect Client

For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1961

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:
 - **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....**

NOTE

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:	<input type="text" value="1"/>	hours	<input type="button" value="▼"/>
Maximum session duration:	<input type="text" value="2"/>	hours	<input type="button" value="▼"/>

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

NOTE

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

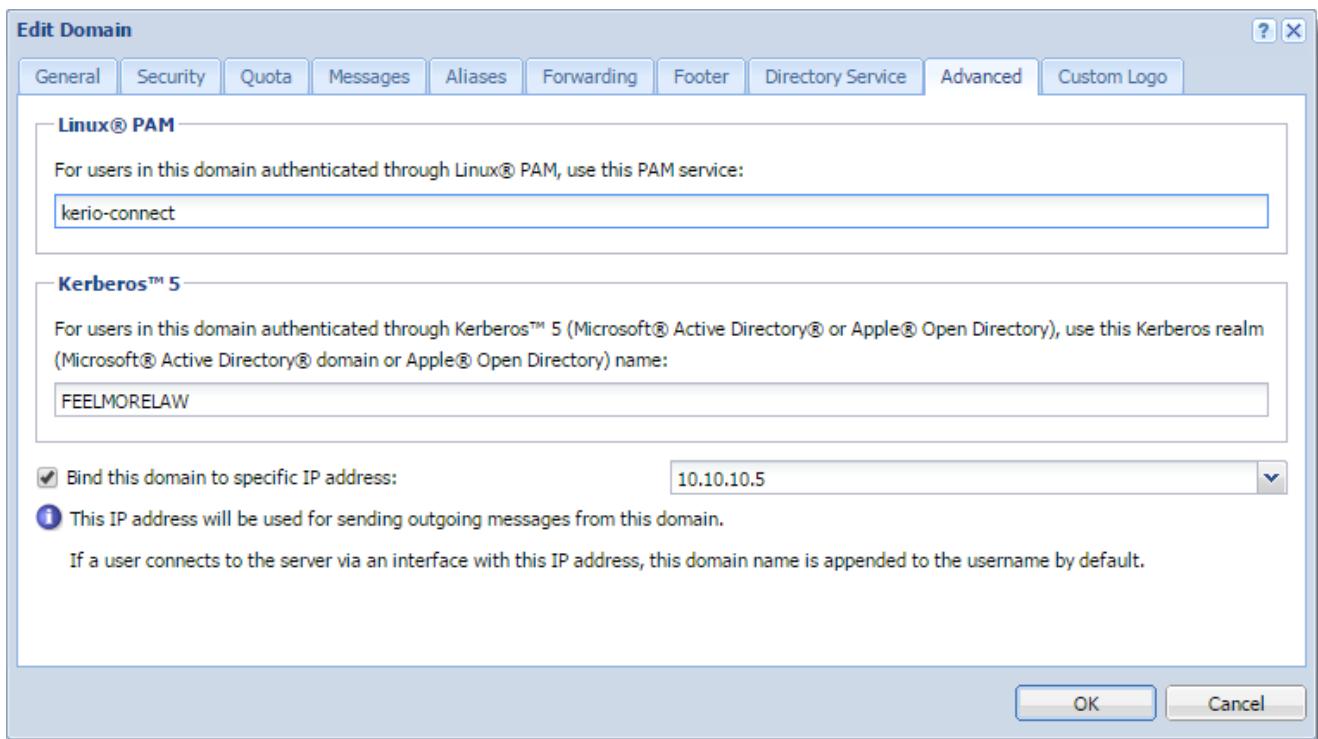
4.1.2 Authenticating users through PAM

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**



4.1.3 Public folders in Kerio Connect

Public folders are folders available to all users in a domain or the whole server. You can create public folders of these types:

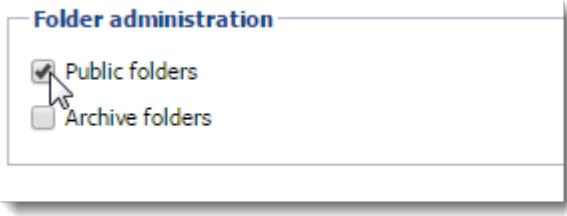
- » Mail
- » Calendar
- » Contacts
- » Tasks
- » Notes

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

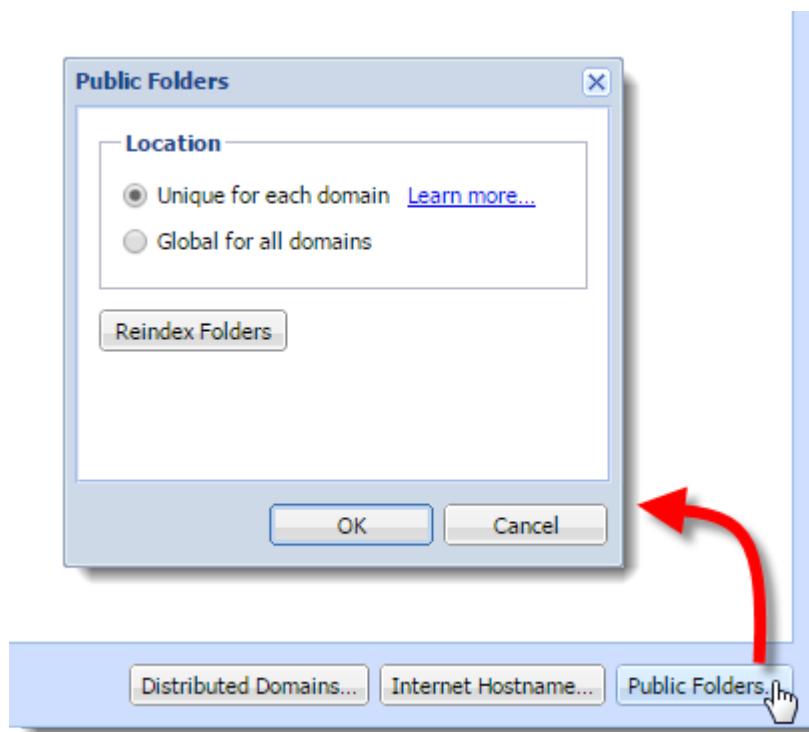
The contacts that users can chat with depend on the public folder settings:

- » **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**



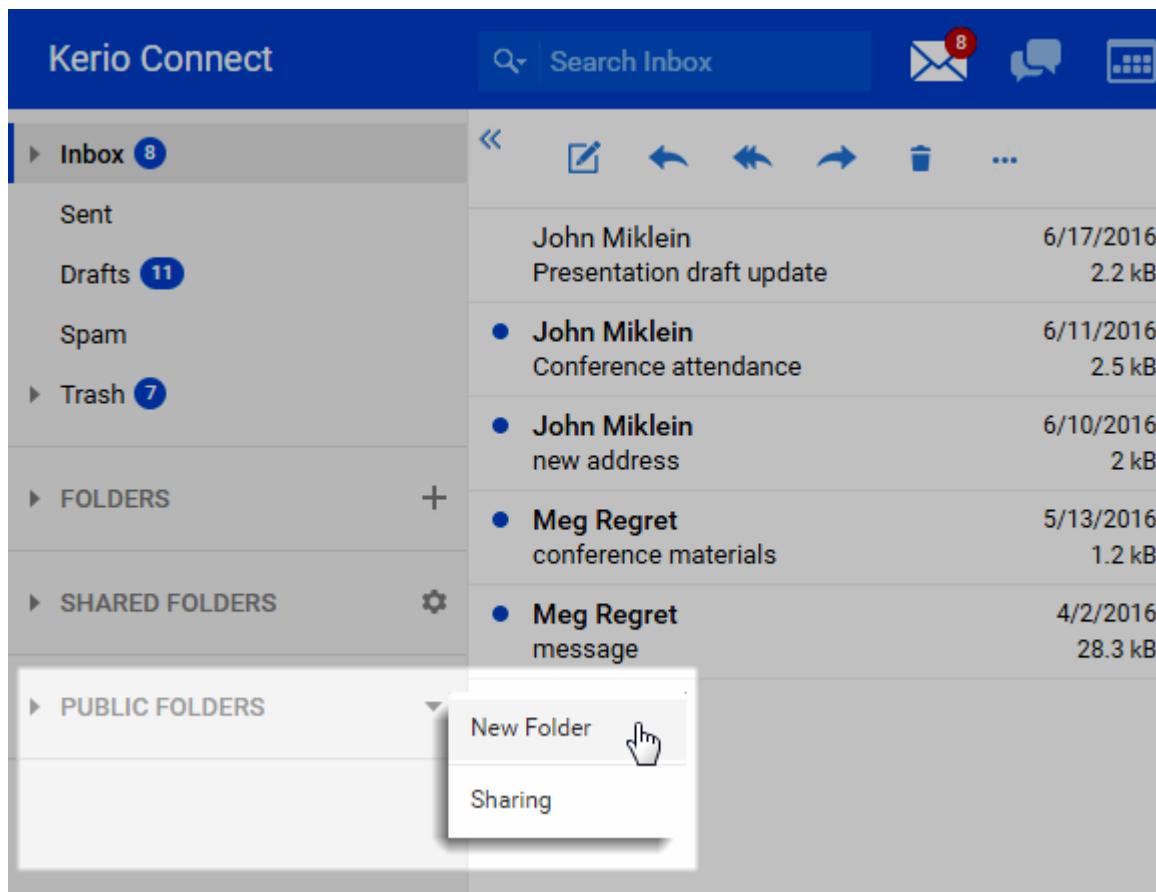
NOTE

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.

For more information, refer to [How to change from individual public folders to global public folders and keep your existing public folder data](#) (page 238).

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. For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1502

NOTE

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:

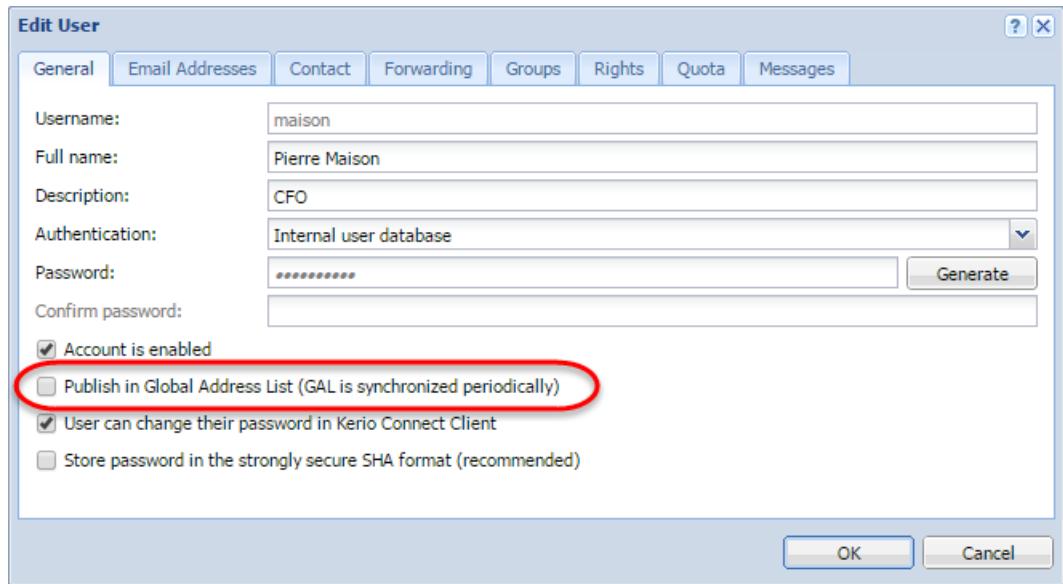
Account	Email	Contacts	Calendar	Tasks	Notes
Kerio Outlook Connector (Offline Edition)	YES	YES	YES	YES	YES
Kerio Outlook Connector	YES	YES	YES	YES	YES
Kerio Connect Client	YES	YES	YES	YES	YES
Microsoft Outlook for Mac	YES	YES	YES	YES	YES
Exchange account in Apple Mail	YES	YES	YES	YES	YES
IMAP (any client 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

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.



NOTE

If users are mapped from Active Directory or Apple Open Directory, the entire LDAP database synchronizes every hour automatically. For more information, refer to [Mapping accounts from a directory service](#) (page 271).

4.1.4 Setting access rights in Kerio Connect

In Kerio Connect, you can set access rights to:

- » **Kerio Connect Administration** (see below)
- » **Public folders** (For more information, refer to [Public folders in Kerio Connect](#) (page 205).)
- » **Archive folders** (For more information, refer to [Archiving in Kerio Connect](#) (page 159).)

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

NOTE

For more information, refer to [Accessing Kerio Connect administration](#) (page 242).

Enabling the built-in administrator account

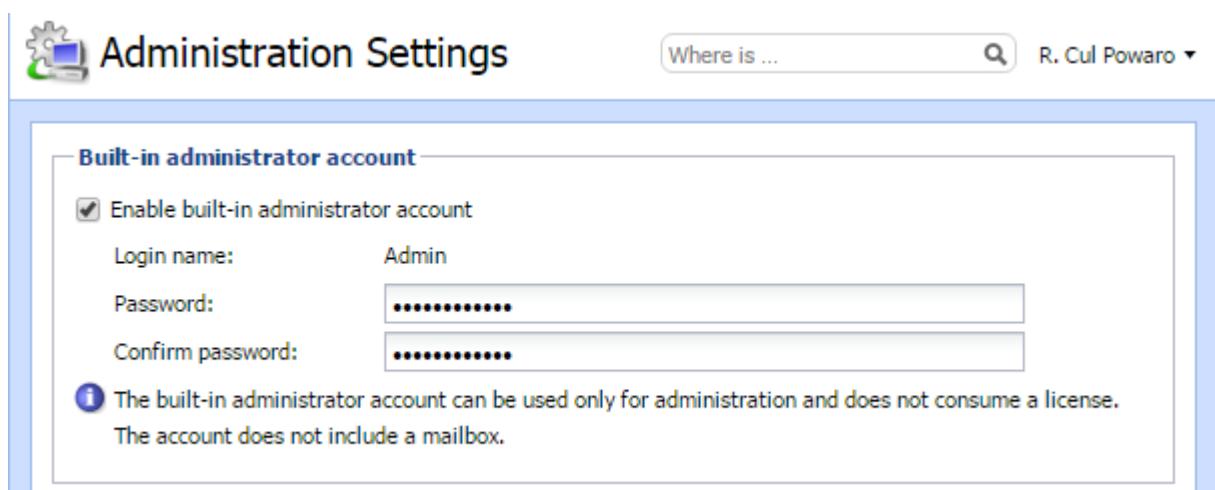
In Kerio Connect, you can enable a special administrator account. This account is available only for accessing the administration interface.

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**.



NOTE

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** (For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).)
- » **User groups** (For more information, refer to [Creating user groups in Kerio Connect](#) (page 272).)
- » **Aliases** (For more information, refer to [Creating aliases in Kerio Connect](#) (page 283).)
- » **Mailing lists** (For more information, refer to [Creating mailing lists in Kerio Connect](#) (page 281).)
- » **Resources** (For more information, refer to [Configuring resources in Kerio Connect](#) (page 287).)

The domain admin cannot assign the archive admin rights, and set the items clean-out.

Username	Full Name	Description
admin		
fan	Thomas Fan	
laboratory	Laboratory Mailbox	
maison	Pierre Maison	CFO
miklein	John Miklein	
mouse	Hector Mouse	Coroner

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**

Edit User

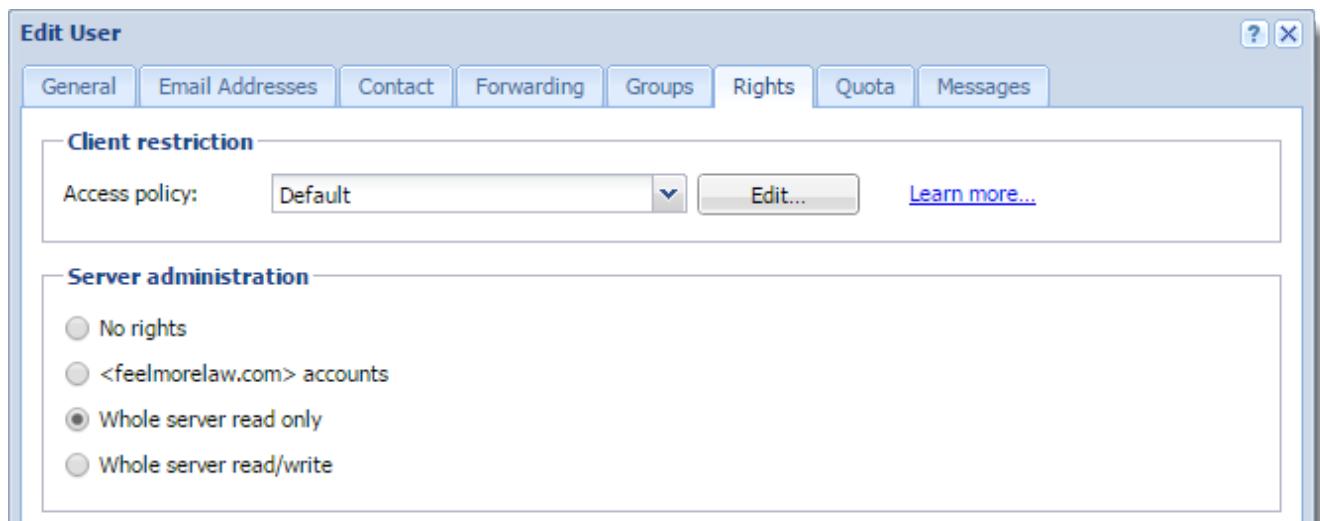
General Email Addresses Contact Forwarding Groups Rights Quota Messages

Client restriction

Access policy: Default Edit... Learn more...

Server administration

No rights
 <feelmorelaw.com> accounts
 Whole server read only
 Whole server read/write



NOTE

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

4.1.5 Creating time ranges in Kerio Connect

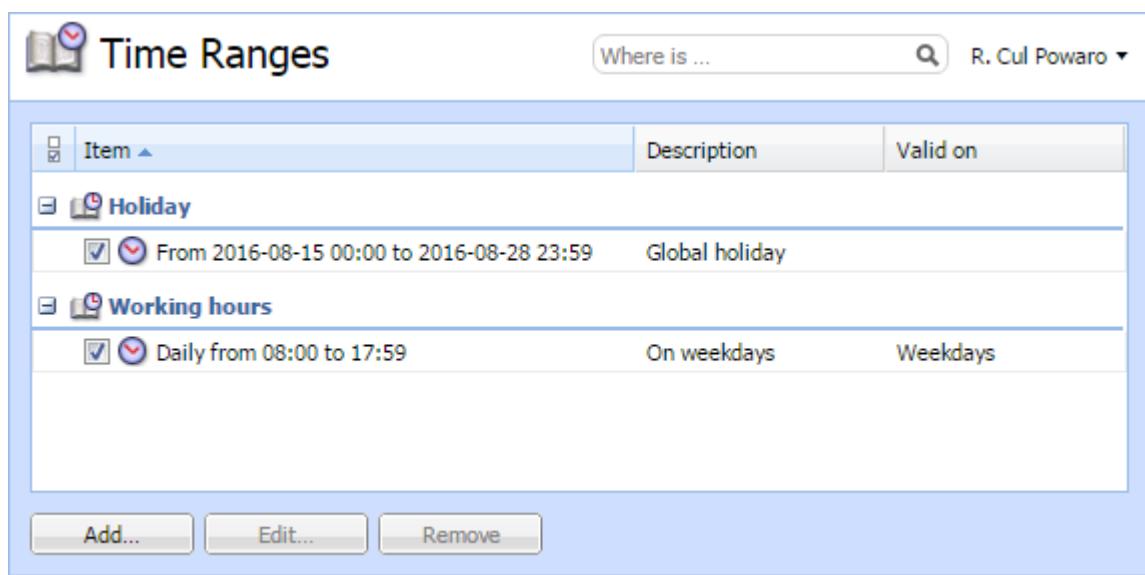
You can restrict all scheduled tasks in Kerio Connect to certain time intervals — **time ranges**.

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

Time Ranges Where is ... R. Cul Powaro ▾

Item	Description	Valid on
<input type="checkbox"/> Holiday	From 2016-08-15 00:00 to 2016-08-28 23:59	Global holiday
<input type="checkbox"/> Working hours	Daily from 08:00 to 17:59	On weekdays Weekdays

Add... Edit... Remove

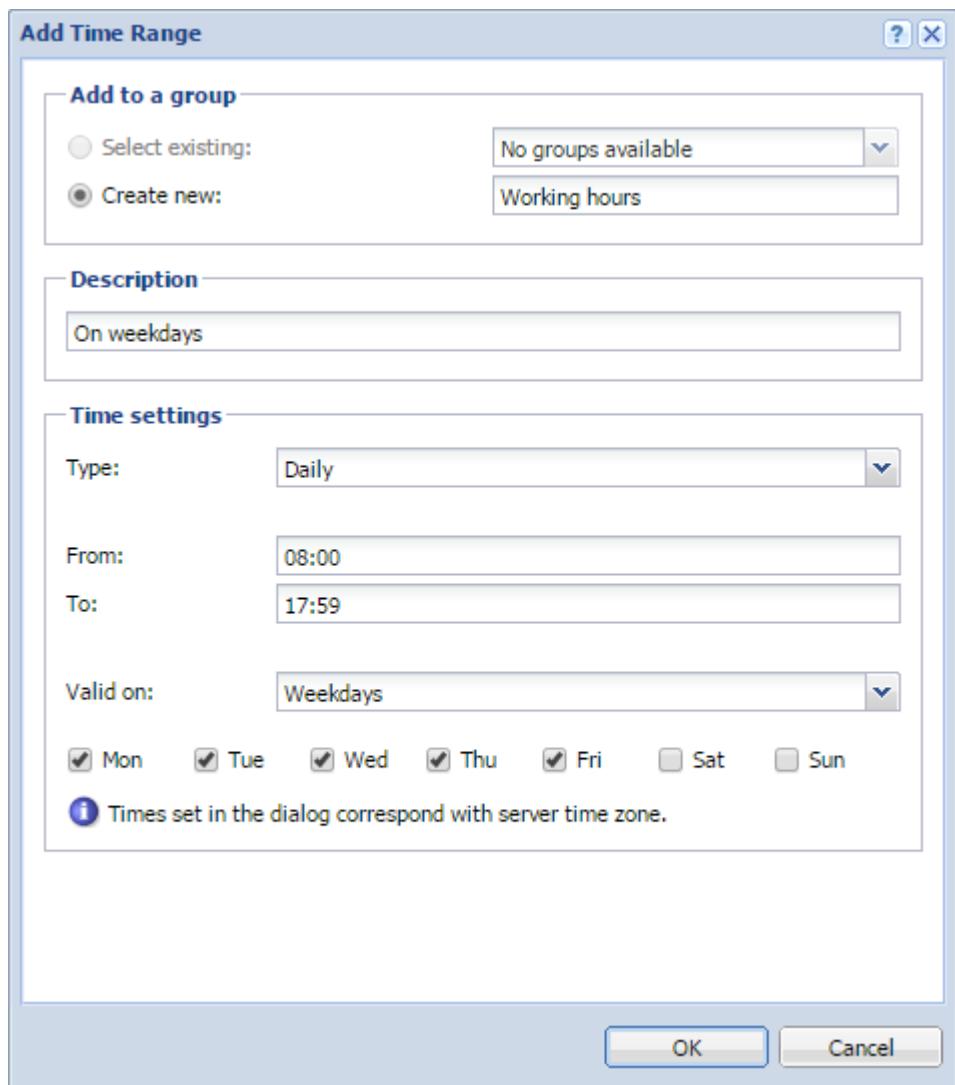


Creating time ranges

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**



4.1.6 Configuring IP address groups

NOTE

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

The screenshot shows the 'IP Address Groups' section in the Kerio Connect administration interface. The left sidebar lists several groups: 'Admins', 'Blacklist', 'Local clients', 'My list of spammers', 'Not spam', 'Voicemail', and 'Whitelist'. The 'Local clients' group is expanded, showing a list of IP address ranges and their descriptions. At the bottom of the main pane are three buttons: 'Add...', 'Edit...', and 'Remove'.

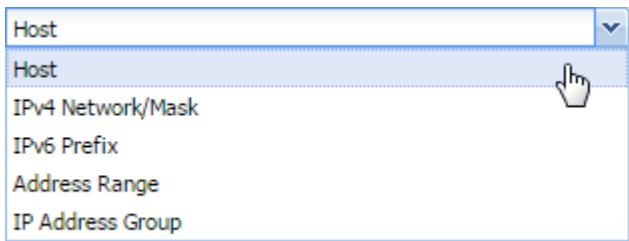
Item	Description
192.168.25.25	Private address space for local networks
125.45.5.5	Private address space for local networks
10.0.0.0 / 255.0.0.0	Private address space for local networks
127.0.0.1	Private address space for local networks
172.16.0.0 / 255.240.0.0	Private address space for local networks
192.168.0.0 / 255.255.0.0	Private address space for local networks
::1	Private address space for local networks
fc00:: / 7	Private address space for local networks
fe80:: / 10	Private address space for local networks

Configuring IP address group

NOTE

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

1. In the administration interface, go to the **Configuration > Definitions > IP Address Groups** section.
2. Click **Add**
3. To create a new IP address group, select **Create new**. To add IP addresses to an existing group, select the IP address group in **Select existing**.
4. Select the type and specify the IP address.



5. Add a description for better reference.

6. Click **OK**

4.1.7 Managing logs in Kerio Connect

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.

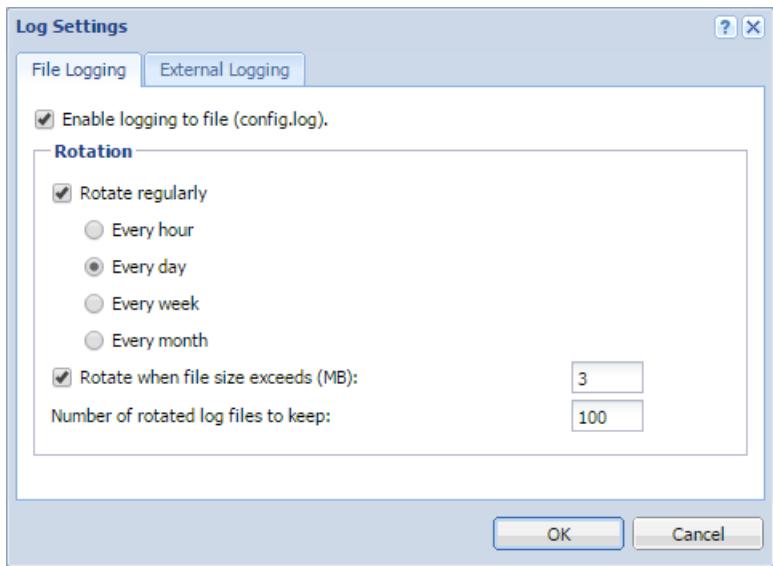
[Highlighting](#)

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**

NOTE

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

NOTE

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.

4.1.8 Customizing Kerio Connect

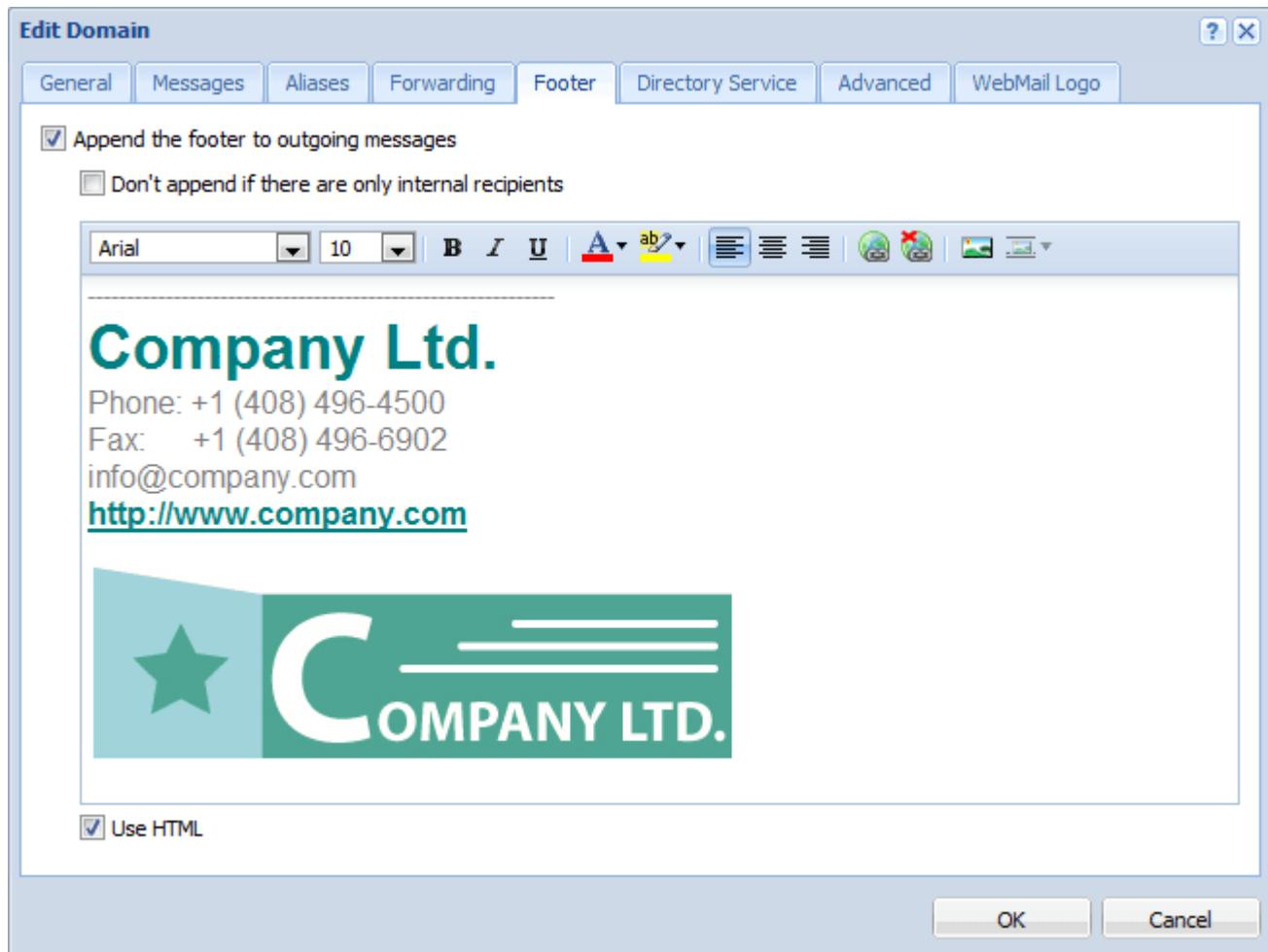
In Kerio Connect, you can:

- » Define custom email footers
- » Translate the interfaces into another language
- » Create a custom page for Kerio Connect Client (For more information, refer to [Customizing the Kerio Connect Client login page](#) (page 222).)
- » 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.

NOTE

If users send [digitally signed](#) or [encrypted](#) messages, Kerio Connect does not append any footers to the message.

Adding automatic user and company details to domain footers

You can use special field identifiers to add user and/or company details to the footer:

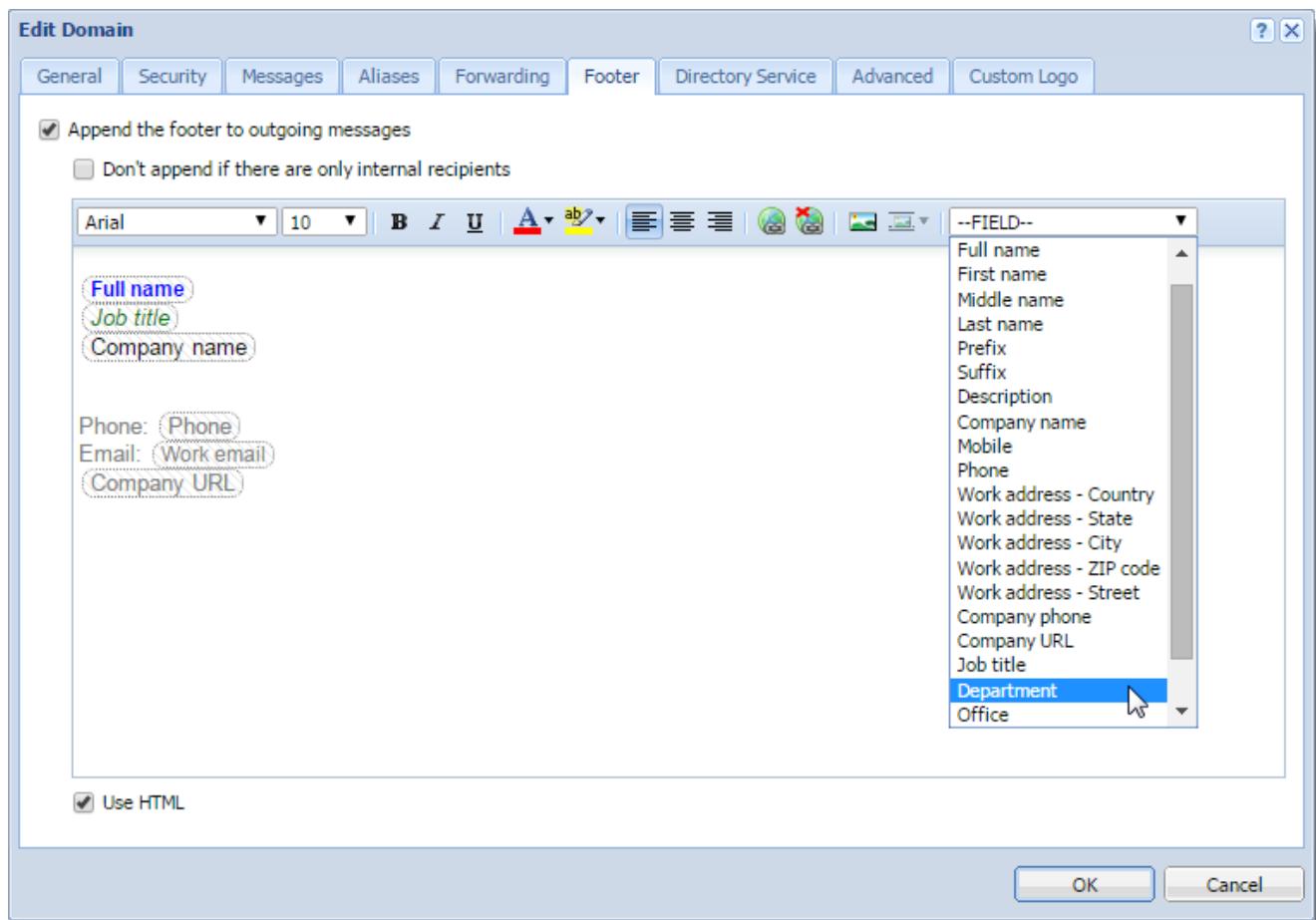
1. Fill in the information in the users' account details.
2. Create company locations.

3. In the administration interface, go to the **Configurations > Domains** section.

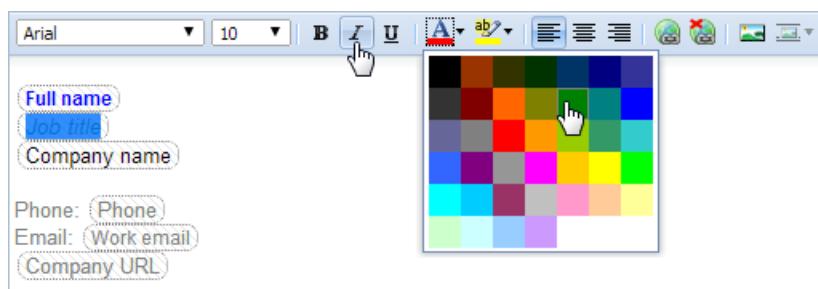
4. Select a domain and click **Edit**.

5. Click the **Footer** tab.

6. Define the footer using items in the **Field** drop-down list.



7. If you select the **Use HTML** option, you can format the fields: select the field and apply formatting attributes.



8. Click **OK**

The final footer might look like this:

REPLY REPLY ALL FORWARD DELETE SPAM ... PRINT

Conf. materials

R. Cul Powaro 10:27 AM

► Meg Regret

Hi Meg,

Have you prepared the materials for tomorrow's conference?

RC

R. Cul Powaro

Vice President

Feel More Law

Phone: +123456789

Email: powaro@feelmorelaw.com

www.feelmorelaw.com

NOTE

If users send [digitally signed](#) or [encrypted](#) messages, Kerio Connect does not append any footers to the message.

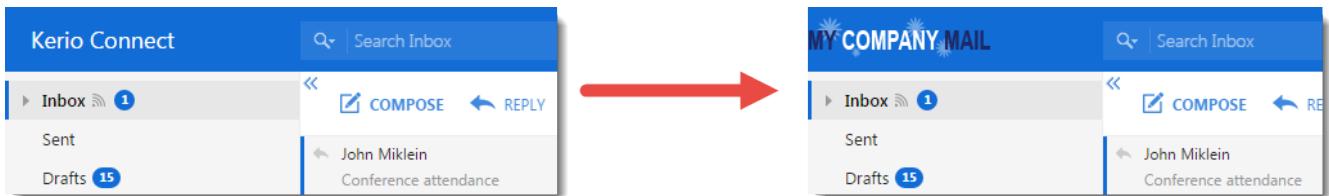
Adding a custom logo to Kerio Connect Client

Kerio Connect Client displays a default logo in the top left corner.

For version 8.5 and newer, you can change the logo:

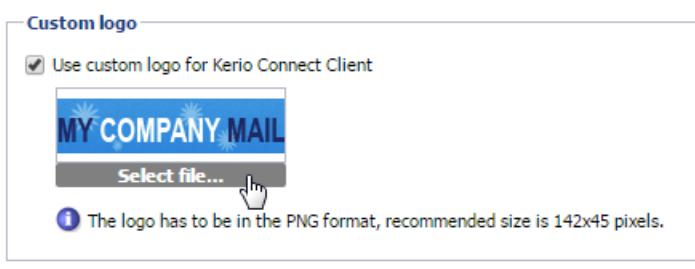
- » Globally for all domains
- » For each domain separately

If you set both logos, Kerio Connect Client displays the logo configured for a particular domain.



Changing the logo for all domains

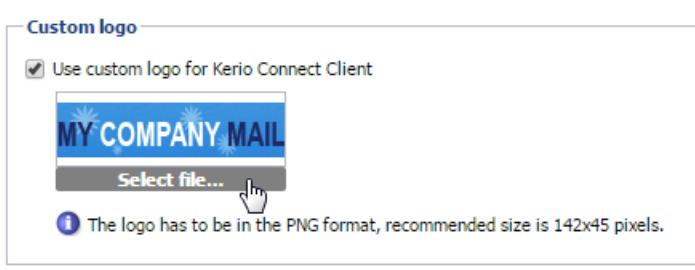
1. In the administration interface, go to **Configuration > Advanced Options > Kerio Connect Client**.
2. In the **Custom logo** section, select **Use custom logo for Kerio Connect Client**.
3. Click **Select file** and locate your image.



4. Click **Apply**.

Changing the logo for individual domains

1. In the administration interface, go to **Configuration > Domains**.
2. Double-click a domain and go to the **Custom Logo** tab.
3. Select the **Use custom logo for Kerio Connect Client** option.
4. Click **Select file** and locate your image.



5. Click **OK**.

Localizing the user interface

Kerio Connect Client 8.1 and later

For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1382

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.

IMPORTANT

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

4.1.9 Customizing the Kerio Connect Client login page

In Kerio Connect 8.4 and later, you can customize the login page for Kerio Connect Client.

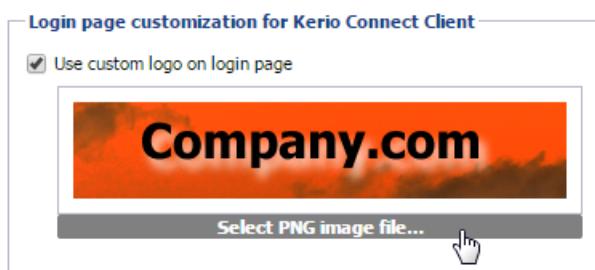
You can change the login page for all domains created in your Kerio Connect, but not for individual domains.

NOTE

The login page of the administration interface does not change.

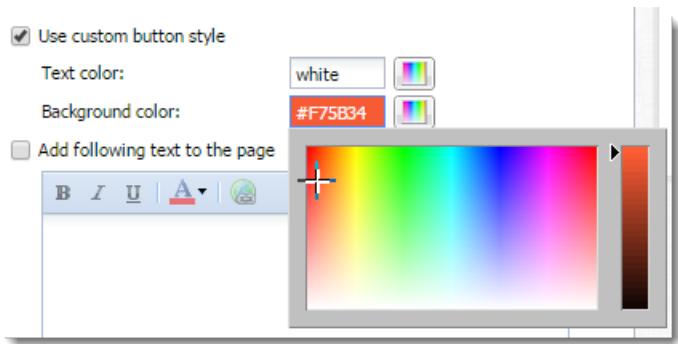
Customizing the login page

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. 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

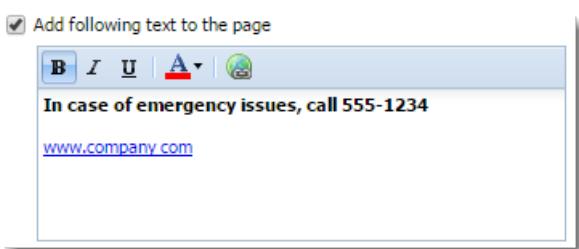


Kerio Connect immediately shows your changes in the **Login page preview**.

NOTE

New in Kerio Connect 8.5!

5. Click **Add the following text to the page** to append text to the bottom of the login page.



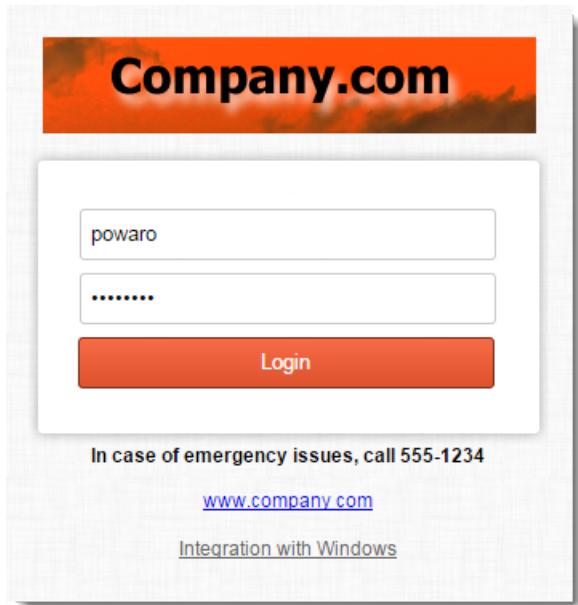
Kerio Connect immediately shows your changes in the **Login page preview**.

NOTE

New in Kerio Connect 8.5!

6. Save your settings.

Kerio Connect Client login pages for all your domains are now customized.



4.1.10 Filtering messages on the server

NOTE

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.

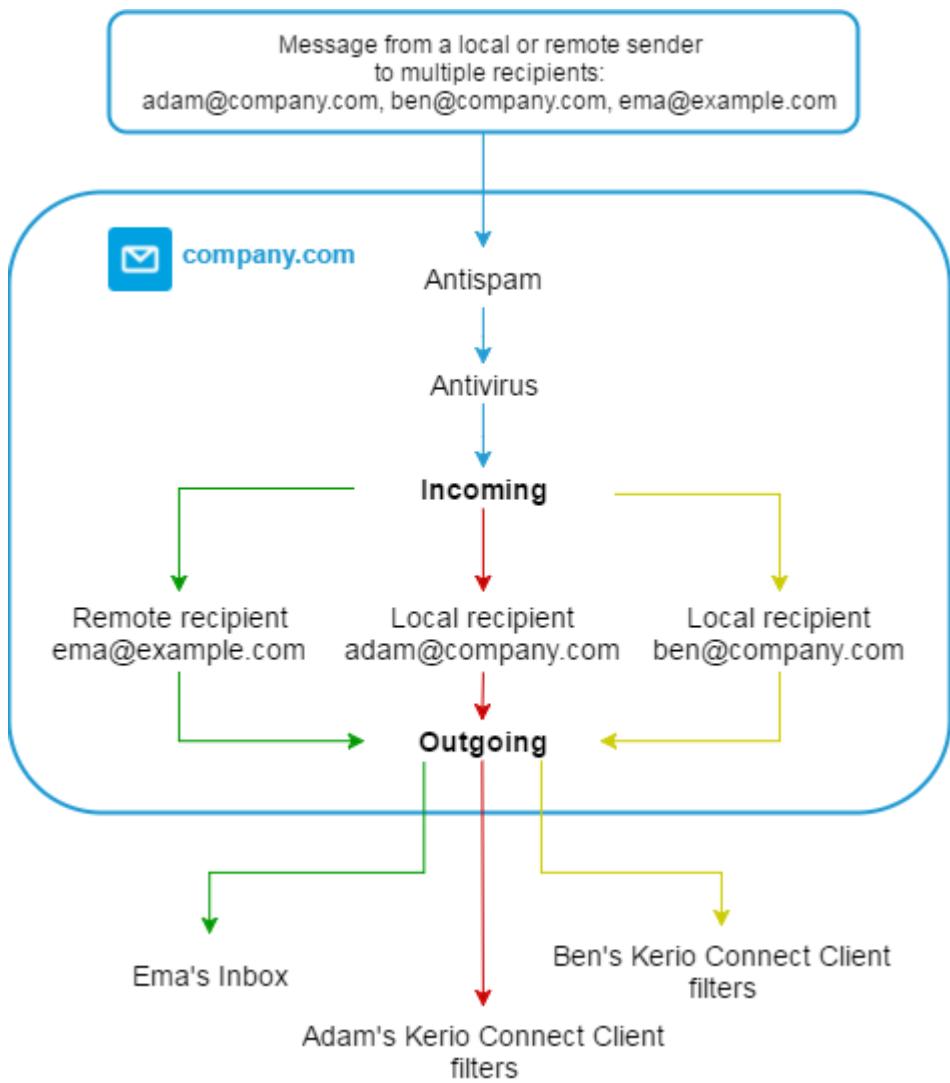
For example, you can:

- » 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** (previously Receiving rules) to all recipients in the message. In the **Outgoing rules** (previously Sending 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:



You can find specific examples below.

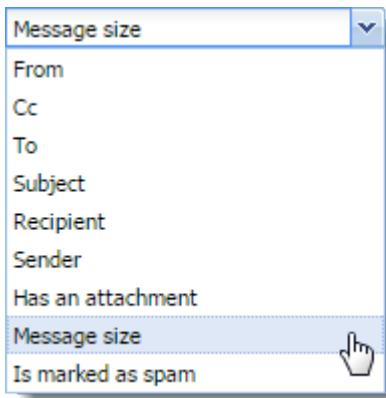
- » Forwarding messages to public folders
- » Prohibiting sending messages to remote recipients for individual users
- » Sending a copy of a message to another email address
- » Rejecting messages with large attachments
- » Sending an auto-reply message

Creating incoming rules

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

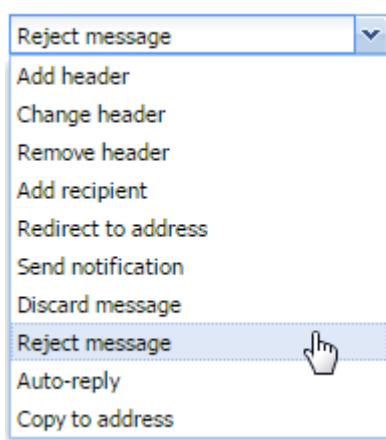
These rules are applied before the outgoing rules and before the user filters in Kerio Connect Client.

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:



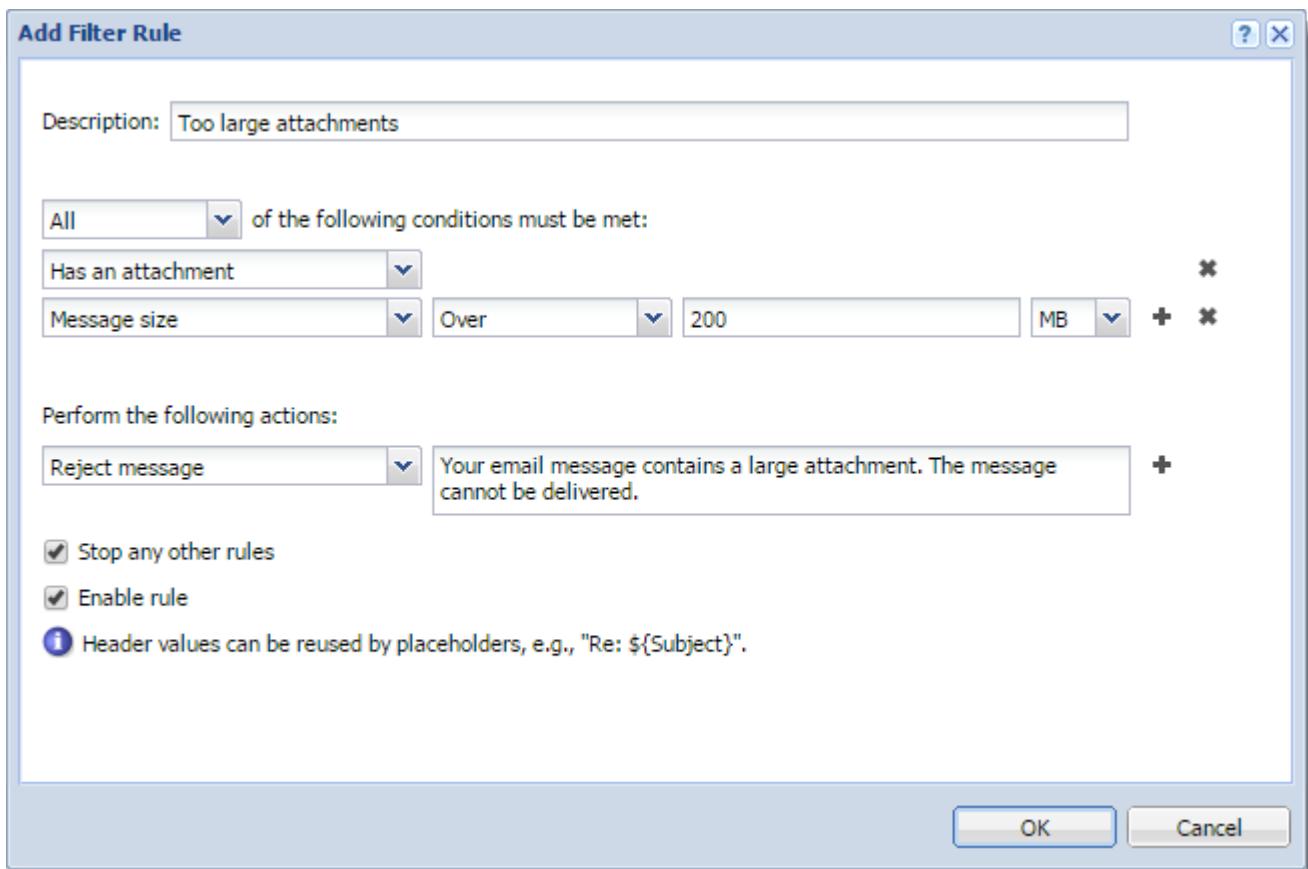
NOTE

You can use placeholders for headers values — **\${size}** for message size, **\${subject}** for message subject, and so on.

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**.

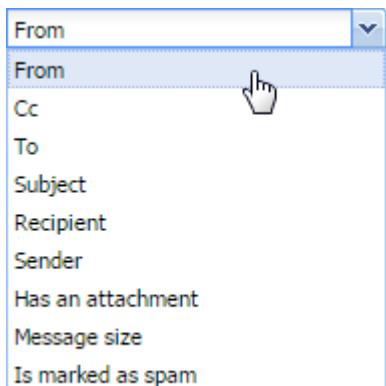


Creating outgoing rules

Kerio Connect applies **outgoing rules** to all messages that Kerio Connect sends to local or remote recipients.

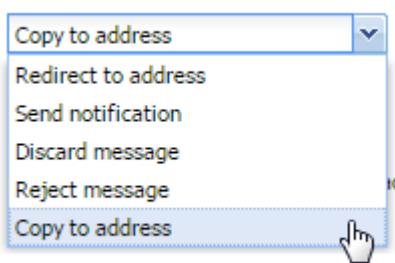
These rules are applied after the incoming rules and before the user filters in Kerio Connect Client.

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:



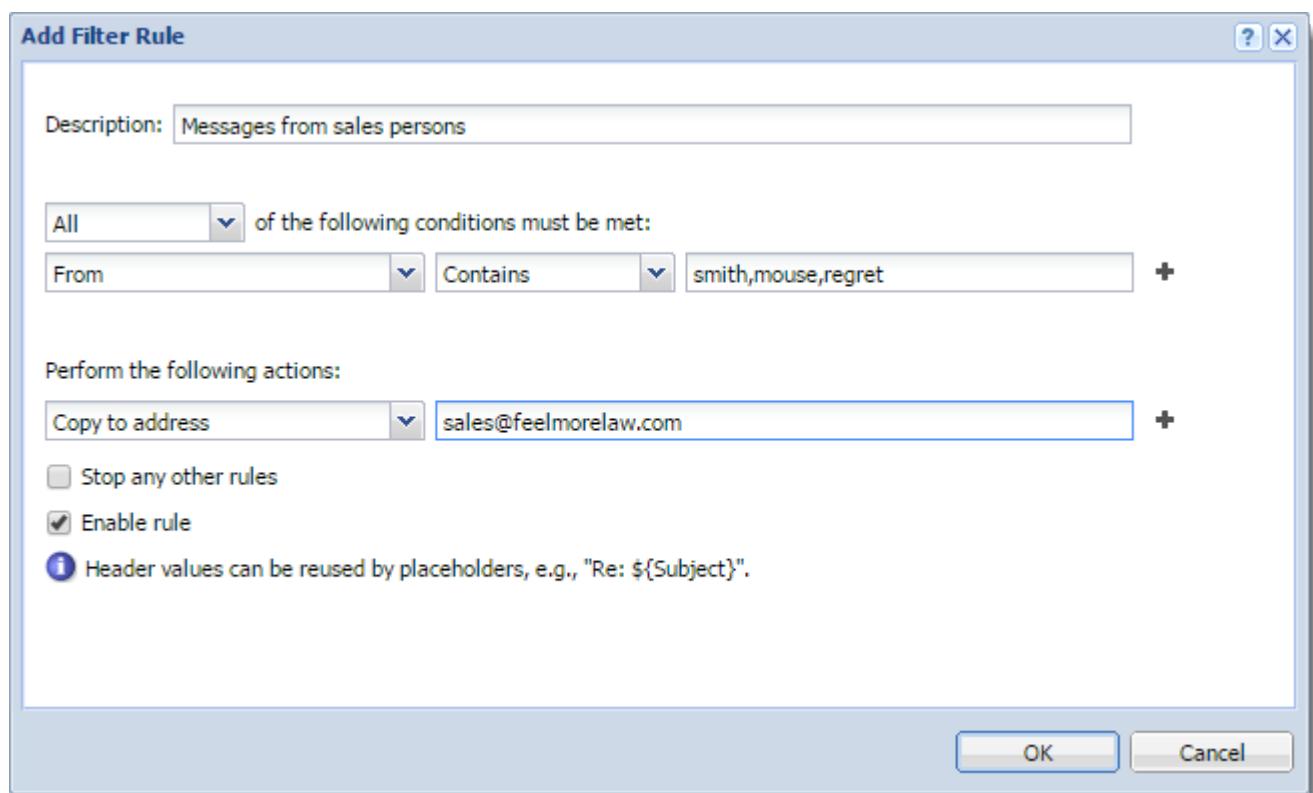
NOTE

You can use placeholders for headers values — **\${size}** for message size, **\${subject}** for message subject, and so on.

6. (Optional) Select the **Stop any other rules** option. The rules are processed from the top. If the message matches the rule, no other rules are processed.

7. Click **OK**

8. Click **Apply**.



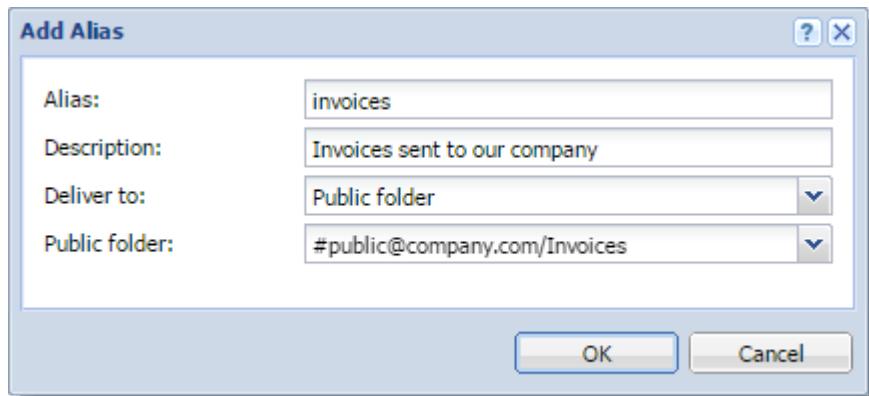
Example 1 - Forwarding messages to public folders

To forward messages to public folders, you must create:

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

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

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

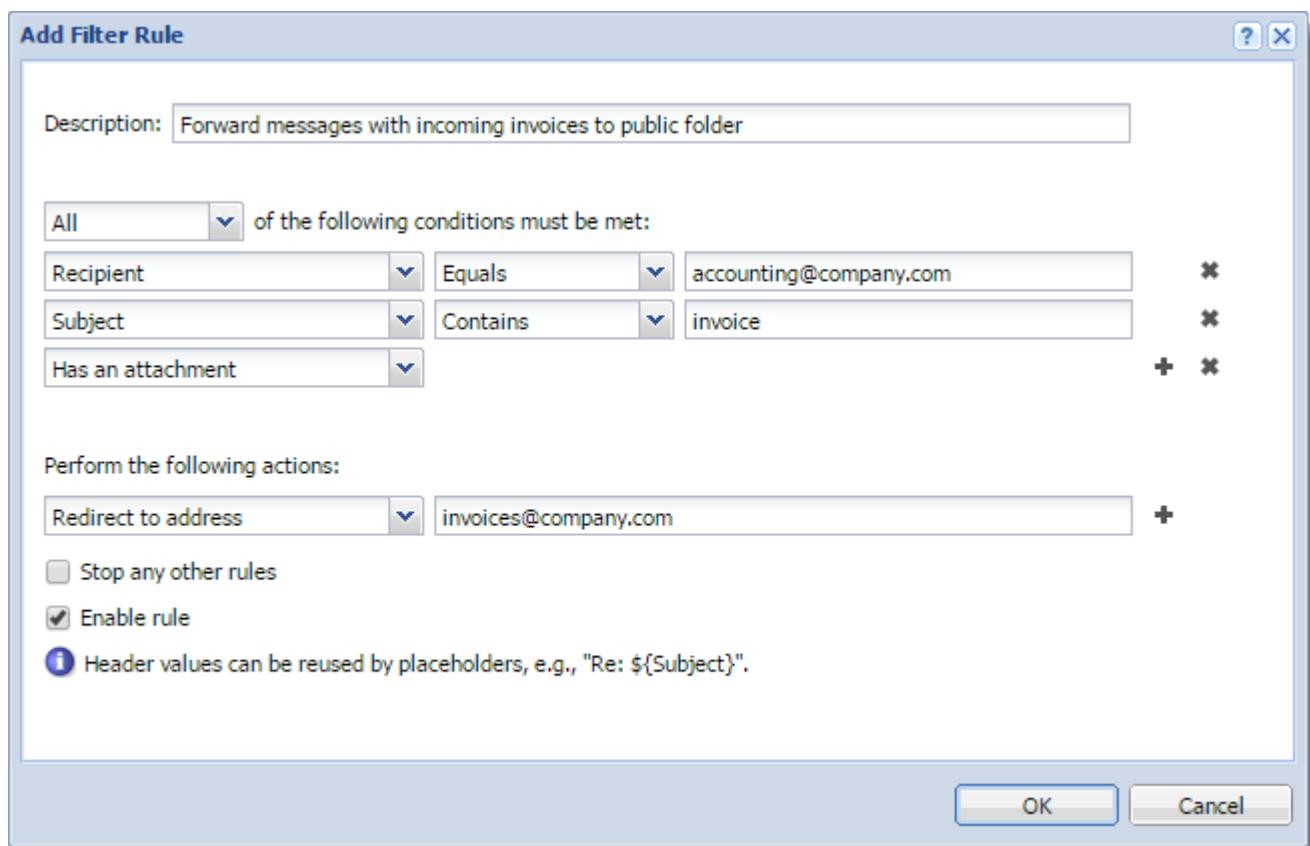


2. Go to the **Configuration > Content Filter > Message Filters** section.
3. In the **Incoming rules** section, click **Add**.
4. Set the condition to **Recipient > Equals > accounting@company.com**.
5. Click the plus sign to add another condition.
6. Set the condition to **Subject > Contains > invoice**.
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.

NOTE

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

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

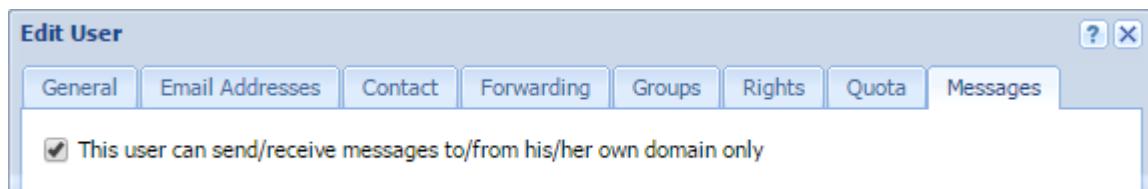


NOTE

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 (`j.smith@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**.

NOTE

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 and 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

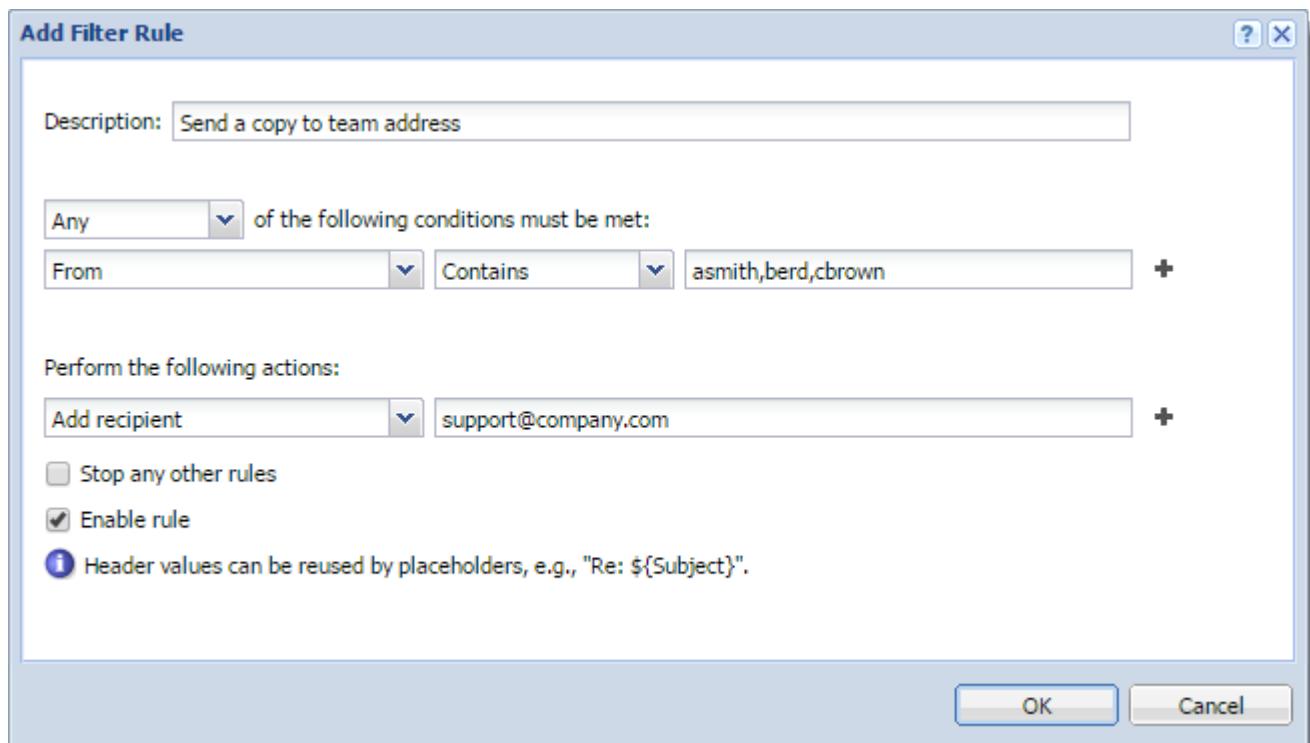
A team of support technicians help customers solve their problems. They communicate via their email addresses:

- » 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**.



NOTE

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**.

NOTE

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

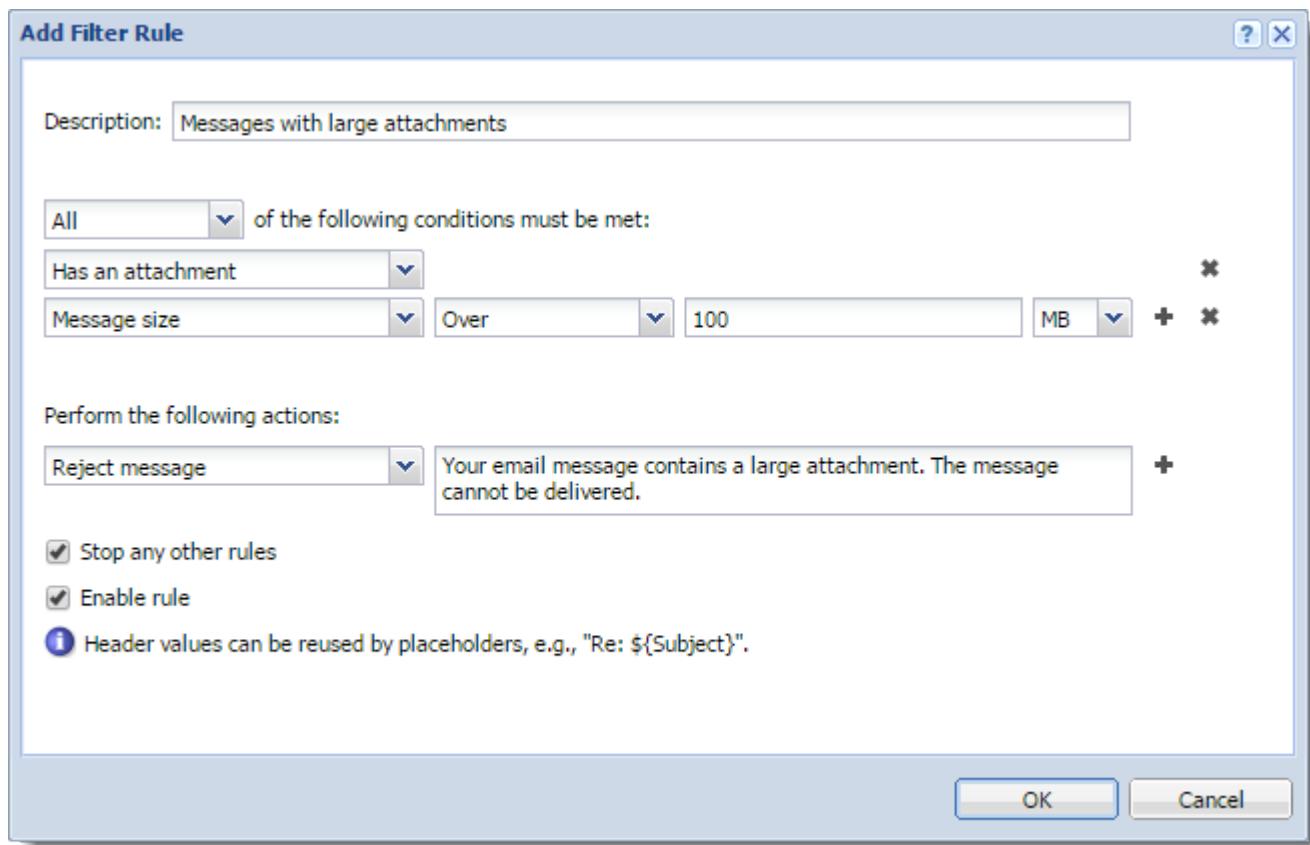
2. Select **All** in the drop-down list.
3. Set the condition to **Has an attachment**.
4. Click the plus sign to add another condition.
5. Set the condition to **Message size > Over > 100MB**.
6. Set the action to **Reject message** and type the reason for rejecting that the sender receives.

NOTE

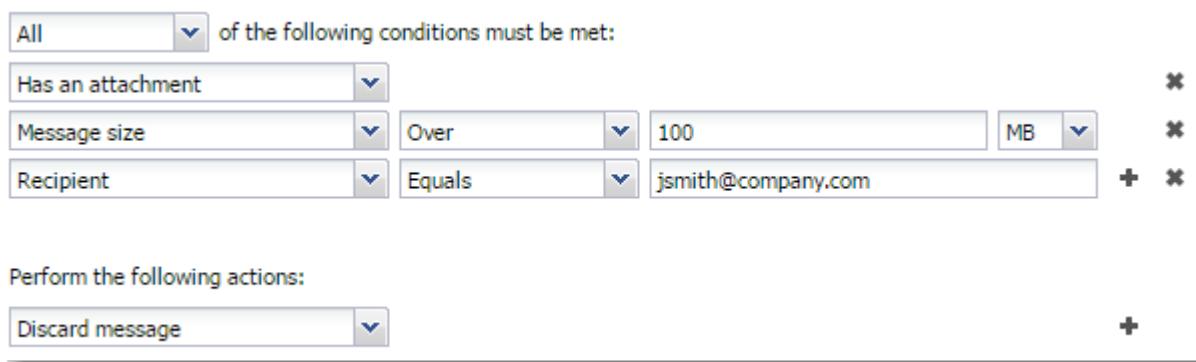
If you select **Discard message**, the sender is not notified.

7. Select **Stop any other rules**.

8. Click **OK** and **Apply**.



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



Examples 5 - Sending an auto-reply message

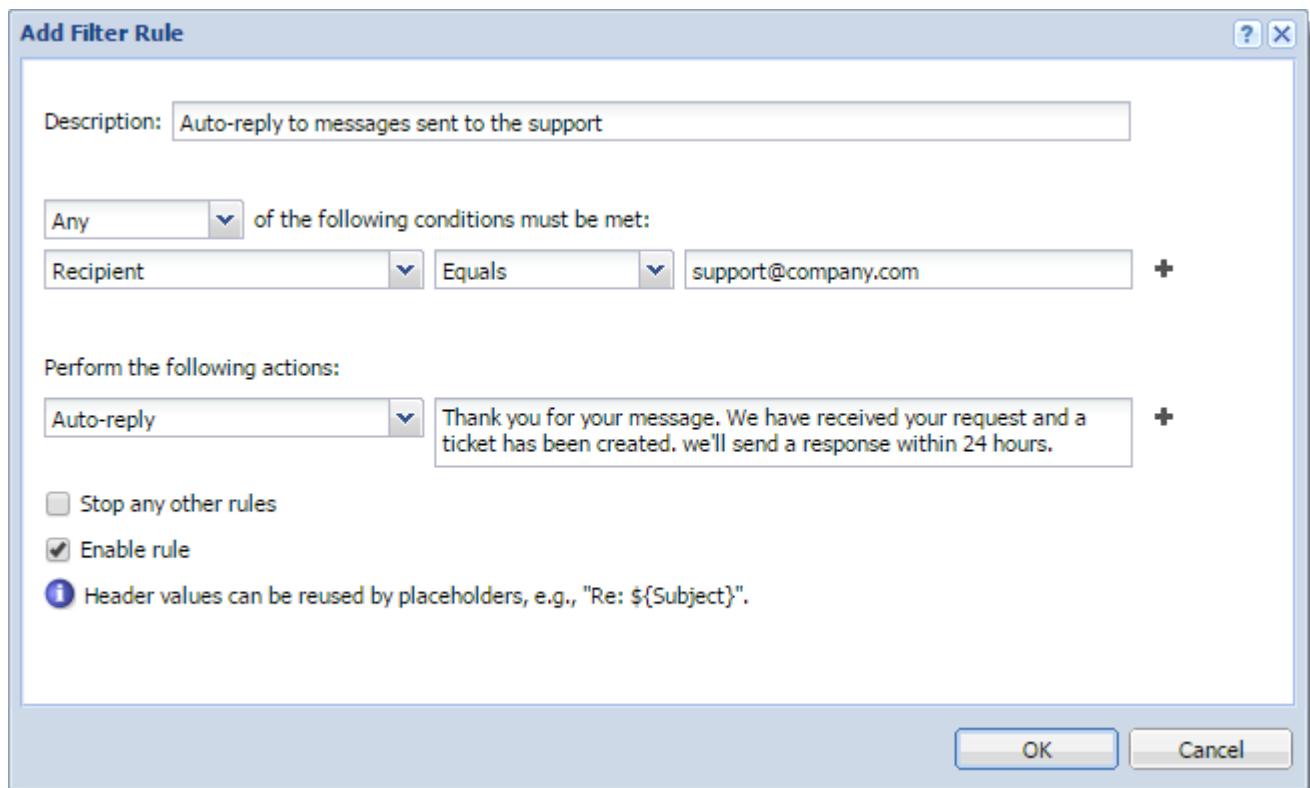
You want to send an automatic reply to each message that Kerio Connect delivers to your support team address.

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

2. Set the condition to **Recipient > Equals > support@company.com**.

3. Set the action to **Auto-reply** and type the text.

4. Click **OK** and **Apply**.



4.1.11 Integrating Kerio Connect with Kerio Operator

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.

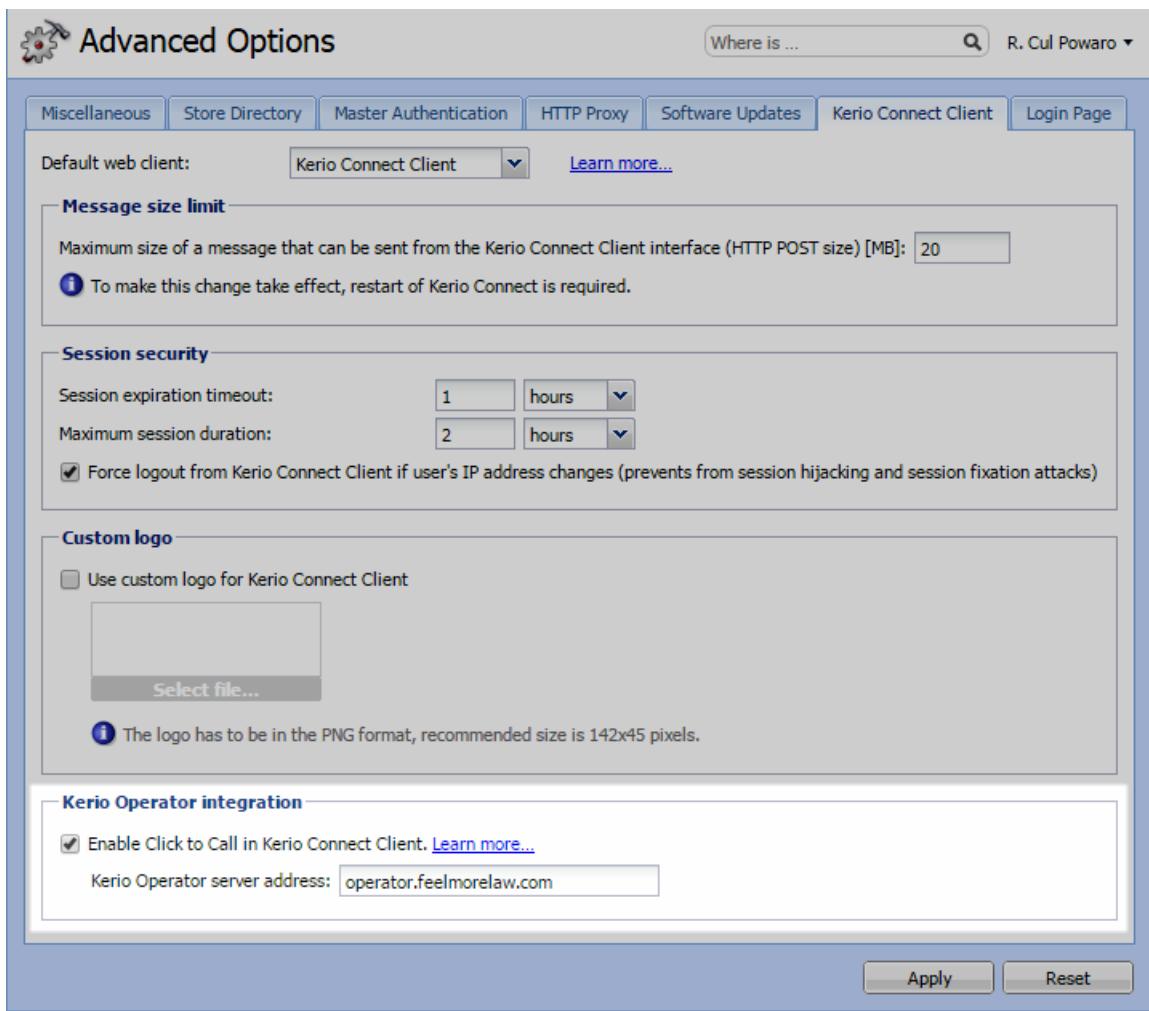
Configuring Kerio Connect

An administrator with full access rights must connect Kerio Connect to Kerio Operator.

NOTE

Users must have identical usernames in both Kerio Connect and Kerio Operator to use the **Click to Call** feature.

1. Login to Kerio Connect Administration.
2. Go to the **Configuration > Advanced Options** section.
3. On the **Kerio Connect Client** tab, type the name of the Kerio Operator server.



Configuring Kerio Operator

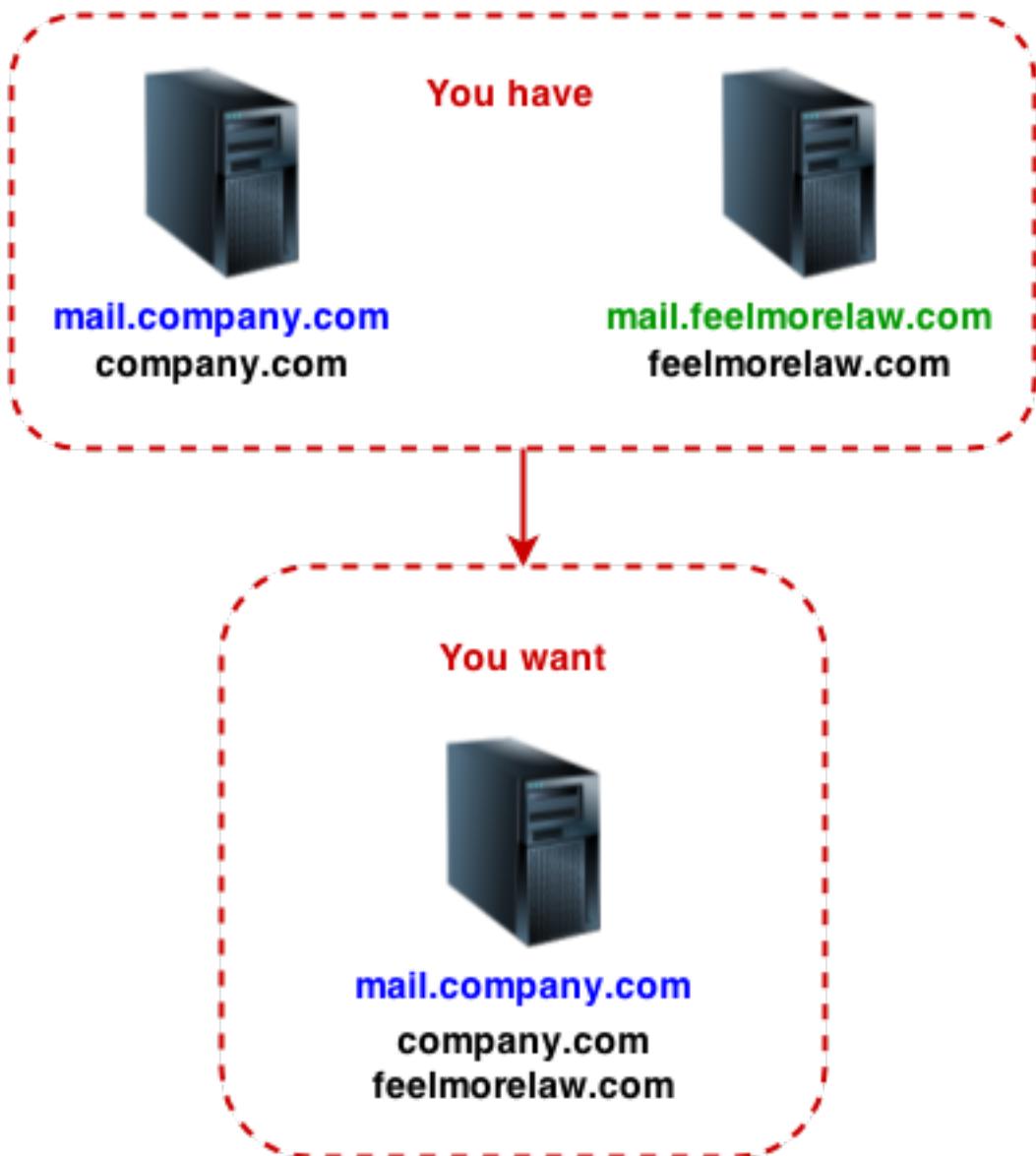
No special configuration is necessary in Kerio Operator. If you use an outgoing prefix in your environment, you must [add a number transformation rule](#) to Kerio Operator.

NOTE

See [Making calls from Kerio Connect Client](#) for more information on using Click to Call.

4.1.12 Joining two servers with different domains into one server

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**.
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.

4.1.13 Changing the time zone definitions in `timezones.xml` file in Kerio Connect

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.

NOTE

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

To update the file, follow these steps:

1. Stop the Kerio Connect server.
2. Replace the `timezones.xml` with a new one.

NOTE

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>`.

NOTE

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 $\pm PThhHmmM$ 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
- »

4.1.14 How to change from individual public folders to global public folders and keep your existing public folder data

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.

NOTE

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.

NOTE

Users with Kerio Outlook Connector (Offline Edition) must either clear the KOFF cache (in control **Panel > Mail > Email Accounts**) or re-create their profiles.

4.1.15 Upgrading the MAPI property database in Kerio Connect 9.1

NOTE

New in Kerio Connect 9.1!

Kerio Connect 9.1 includes a new type of database for storing MAPI properties. The property database upgrades automatically once you upgrade to Kerio Connect 9.1. The upgrade may take several minutes, depending on the size of your message store.

Kerio Connect retains the old database files in case you want to downgrade Kerio Connect. In that case, however, any changes since the upgrade are lost.

Monitoring the upgrade

The database starts upgrading immediately after the server upgrade.

To monitor the progress of the upgrade, open this URL in your browser: `http://<domain_name>:4040`

NOTE

If you enable `Message Folder Operations` in the debug log before the upgrade, Kerio Connect displays the result of the upgrade in the debug log for each upgraded database file.

Enabling and disabling the upgrade

Kerio Connect upgrades the database type immediately after you upgrade to Kerio Connect 9.1. The upgrade is enabled by default.

To disable the upgrade in the Kerio Connect configuration file:

1. Stop Kerio Connect.
2. Open the **mailserver.cfg** file.
3. Set the `EnableMetadataUpgrade` variable to 0 (zero).

NOTE

If the variable is not available in the configuration file, add the following to the `MessageStore` table:

```
<variable name="EnableMetadataUpgrade">0</variable>
```

4. Save the configuration file.
5. Start Kerio Connect.
6. If you have Kerio Connect 9.0 or an earlier version, run the upgrade to Kerio Connect 9.1.

NOTE

To enable the upgrade again, set the `EnableMetadataUpgrade` variable to 1.

Using the old database type after upgrading

1. Stop Kerio Connect.
2. Open the `mailserver.cfg` file.
3. Set the `EnableMetadataUpgrade` variable to 0 (zero).
4. Set the `MetadataVersion` variable to 0 (zero).
5. Save the file.
6. Start Kerio Connect.

Re-enabling the new database type

To start using the new database type again after downgrading to the original type:

1. Stop Kerio Connect.
2. Delete all `metadata.dbo` and `metadata.dbb` files in the Kerio Connect installation folder.
3. Open the `mailserver.cfg` file.
4. Set the `EnableMetadataUpgrade` variable to 1.
5. Save the file.
6. Start Kerio Connect.

Troubleshooting

If any problems occur, consult the Kerio Connect logs.

You can also run the upgrade again:

1. Stop Kerio Connect.
2. Set the `MetadataVersion` variable in the configuration file to 0 (zero).
3. Set the `EnableMetadataUpgrade` variable to 1.
4. Delete all `metadata.dbb` and `metadata.dbo` files in each folder.
5. Restart Kerio Connect.

4.1.16 Using Kerio Assist tool

Whenever a problem occurs (e.g. when connection is closed improperly, connection "freezes" or Kerio Connect crashed etc.), automatic restart is initiated by the corresponding process. Initiation of the application's restart also generates and saves a crashdump log that might help discover the problem's cause. Then, when an administrator connects to Kerio Connect, a Kerio Assist dialog asks them to decide whether the crashdump log would be sent to Kerio Technologies for analysis. Behaviour of the Kerio Assist differs in dependence on the operating system.

- » Windows — the Kerio Assist dialog is opened immediately upon the incident.
- » Mac OS X, Linux — the Kerio Assist dialog is opened upon the first startup of the Kerio Administration Console after the incident.

However, you can be asked by technical support engineer to initiate kassist manually. In that case, you have to specify some of the parameters. A complete list of parameters is available under the --help option.

NOTE

If you are running Windows 8, make sure you run kassist as Administrator.

EXAMPLES

A/ Windows

```
cd "C:\Program Files (x86)\Kerio\MailServer\"  
kassist -n "description of the problem" -P KMS -e "your@email.com" -N "C:\Program  
Files (x86)\Kerio\MailServer\user.dmp"
```

B/ Linux

```
sudo /opt/kerio/mailserver/kassist -n"description of the problem" -P KMS -e  
"your@email.com" -N "/opt/kerio/mailserver/core.PID"
```

NOTE

PID is process identifier number. A higher number doesn't mean a newer process. It is better to sort core files by date to locate the latest one.

You will be prompted for your system password.

C/ Mac OS X

```
sudo /usr/local/kerio/mailserver/kassist -n "description of the problem" -P KMS -e  
"your@email.com" -N "/cores/core.PID"
```

NOTE

PID is process identifier number. A higher number doesn't mean a newer process. It is better to sort core files by date to locate the latest one.

You will be prompted for your system password.

NOTE

The kassist utility must have access to system folders! It's recommended to start it as superuser. Paths in examples may be different on various Linux distributions and platforms. Also, you should have a ticket from your Support team, before performing the upload. This ticket number must be included in any uploads you perform, as part of the investigation of your crash.

4.2 Administration

This section describes how to work with the administration interface.

4.2.1 Accessing Kerio Connect administration	242
4.2.2 Navigating through the Kerio Connect administration interface	244
4.2.3 Using Dashboard in Kerio Connect	245
4.2.4 Gathering usage statistics	246
4.2.5 What ports are used by Kerio Connect for remote administration?	248

4.2.1 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`

IMPORTANT

Use only the officially supported browsers

NOTE

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**.



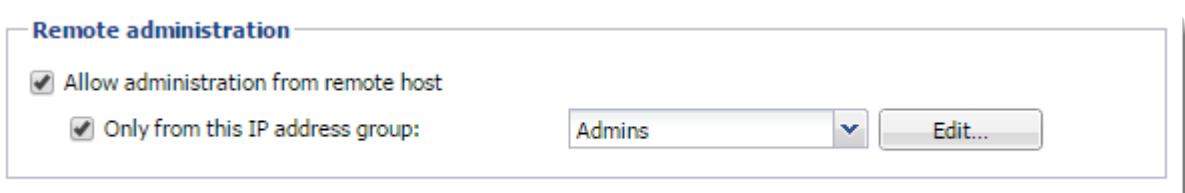
Accessing the administration interface remotely

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 more information, refer to [Setting access rights in Kerio Connect](#) (page 209).

Automatic logout

NOTE

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.

NOTE

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	<input type="button" value="▼"/>
Maximum session duration:	2	hours	<input type="button" value="▼"/>
<input checked="" type="checkbox"/> Force logout from Kerio Connect client if user's IP address changes (prevents from session hijacking and session fixation attacks)			

4.2.2 Navigating through the Kerio Connect administration interface

NOTE

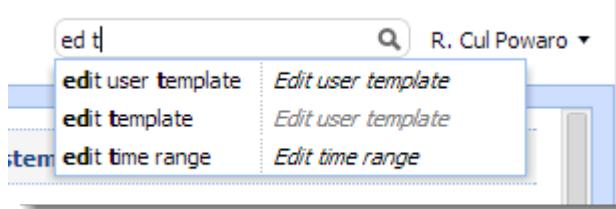
New in Kerio Connect 8.3!

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.

The diagram illustrates the search process in Kerio Connect. It shows three main components:

- highlighted section:** Points to the "Miscellaneous" tab in the "Advanced Options" dialog, which is currently selected.
- keywords and phrases:** Points to the search input field containing the word "message".
- names of sections and dialogs:** Points to the search results list on the right side of the screen, which displays various sections and dialogs related to "message".

The search results list includes items such as:

- 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

On the far right, a vertical list of sections and dialogs is shown, including:

- Edit user
- Edit user
- Edit user
- Edit mailing list
- Edit mailing list
- Miscellaneous settings
- Miscellaneous settings
- Kerio Connect client / WebMail
- Antivirus
- Email archiving
- Email archiving
- Email archiving
- POP3 download
- Internet connection
- Scheduling delivery

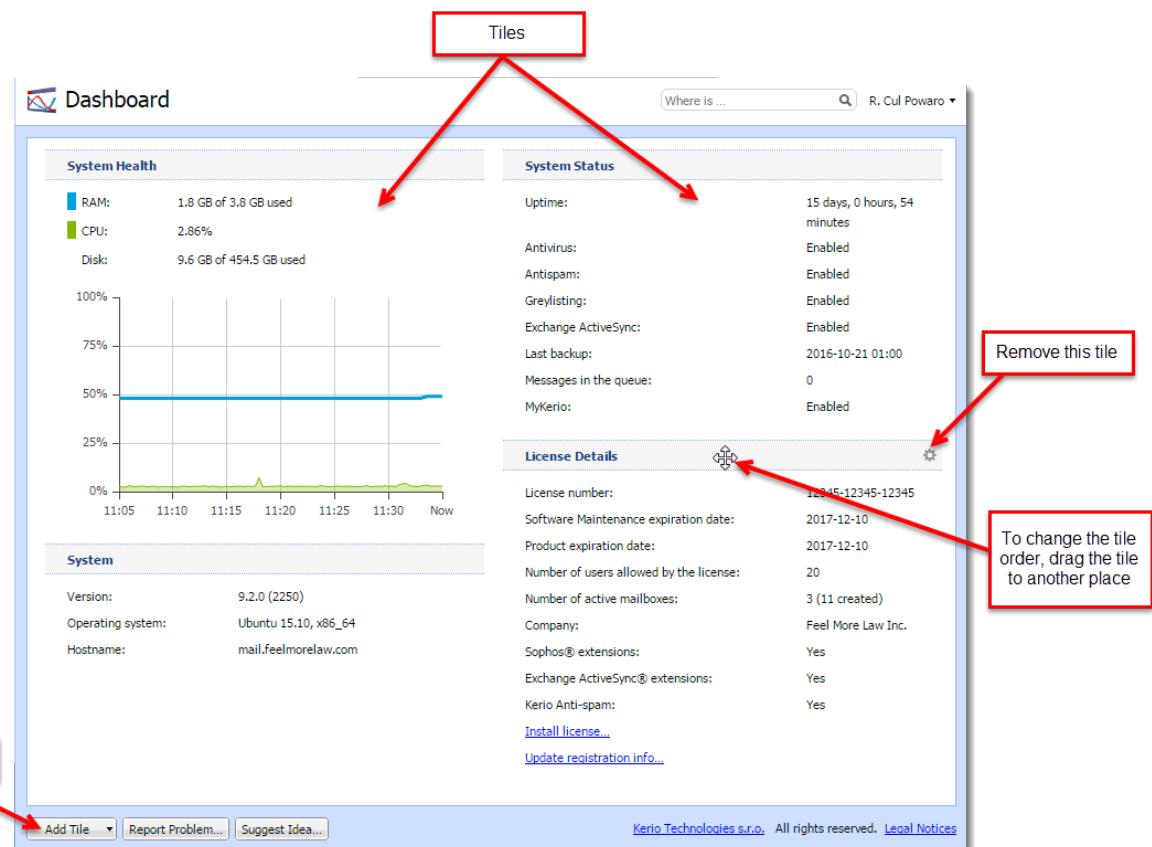
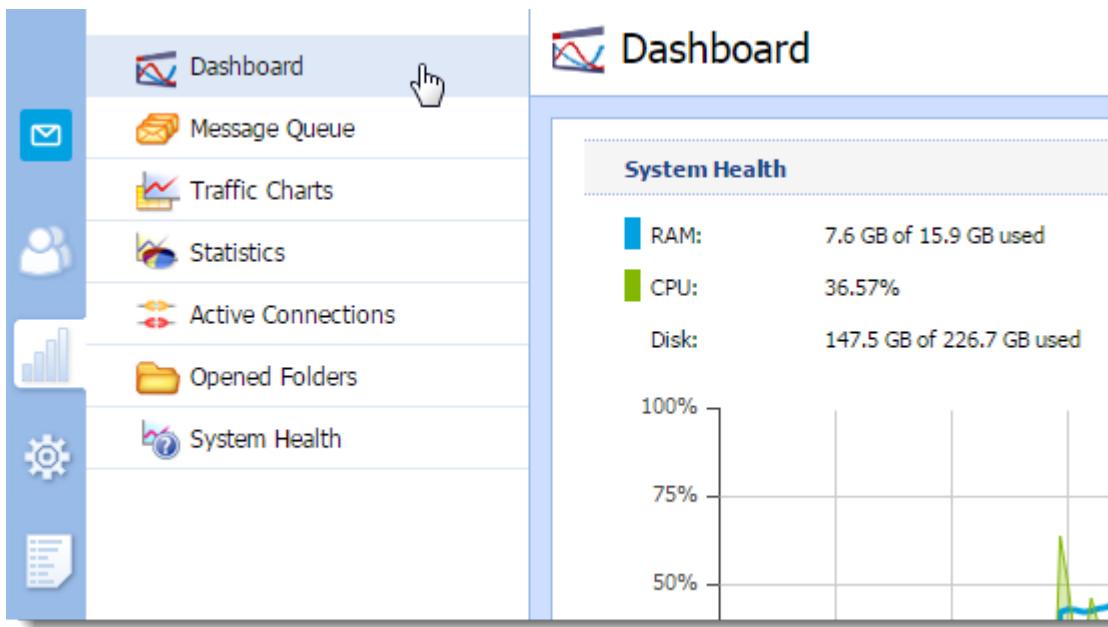
NOTE

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

4.2.3 Using Dashboard in Kerio Connect

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**.



4.2.4 Gathering usage statistics

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

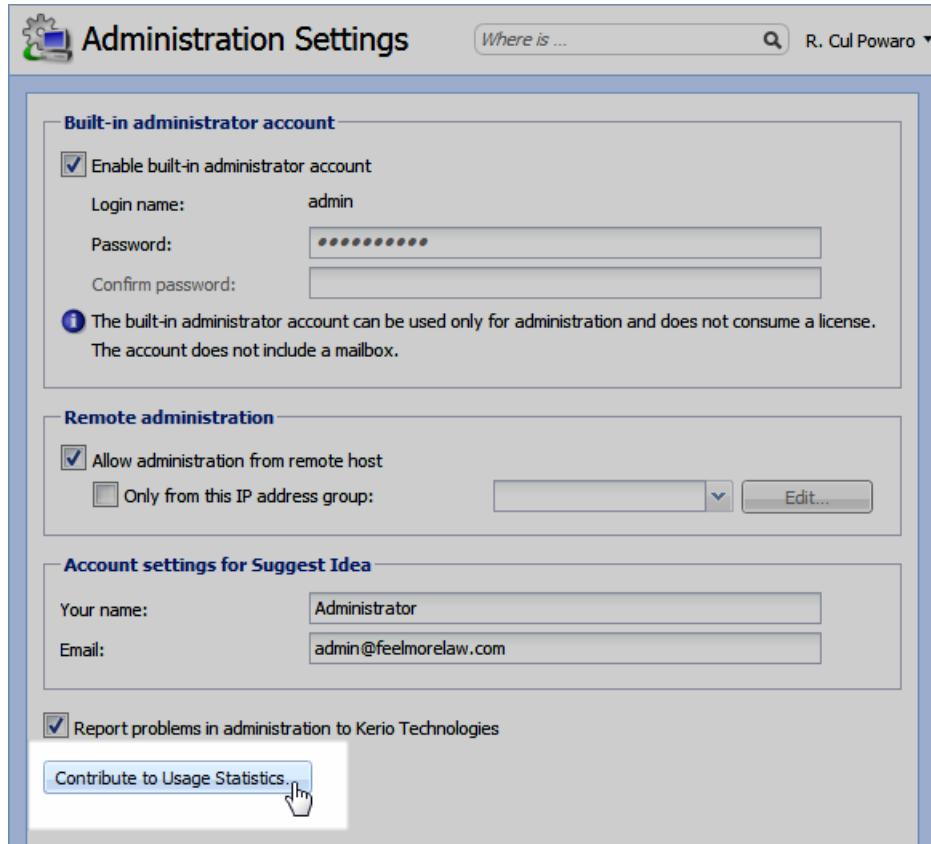
Sending this data does not affect the performance of your Kerio Connect.

Enabling data gathering

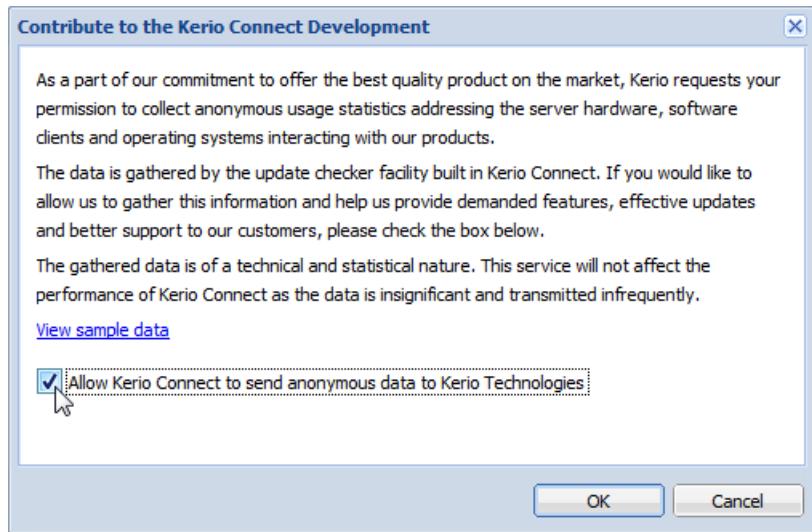
You can allow Kerio to receive anonymous usage statistics during the first activation of Kerio Connect.

To change the settings later, follow these steps:

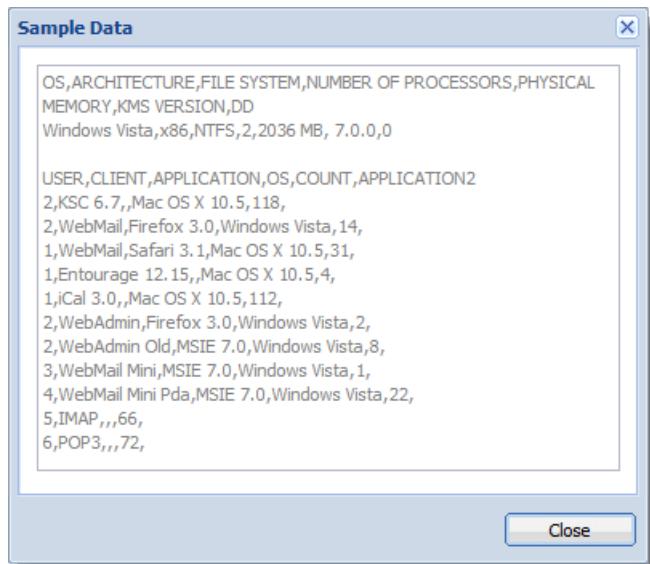
1. Login to the Kerio Connect administration.
2. Go to section **Configuration > Administration Settings**.
3. Click the **Contribute to Usage Statistics** button.



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



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



6. Click **OK**.

4.2.5 What ports are used by Kerio Connect for remote administration?

Kerio Connect uses HTTP and HTTPS over port 4040 for the WebAdmin and this can be accessed from any of the supported browsers:

<http://www.kerio.com/connect/requirements>

NOTE

Older version of Kerio MailServer uses the Admin Console application. It uses TCP port 44337 for management and UDP port 44337 for transmission of log data.

4.3 Domains

This section provides information domains and their settings.

4.3.1 Domains in Kerio Connect	248
4.3.2 Creating domains in Kerio Connect	251
4.3.3 Adding company and user contact information in Kerio Connect	255
4.3.4 Renaming domains in Kerio Connect	257
4.3.5 Distributed domain	258
4.3.6 How to change a user's authentication method from internal, to Active Directory or Open Directory	268

4.3.1 Domains in Kerio Connect

An 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 — feelmorelaw.com
- » Email domain name — mail.feelmorelaw.com
- » User email address — user@feelmorelaw.com

Kerio Connect may include **any number** of email domains.

NOTE

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.

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

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.

NOTE

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

To change the internet hostname:

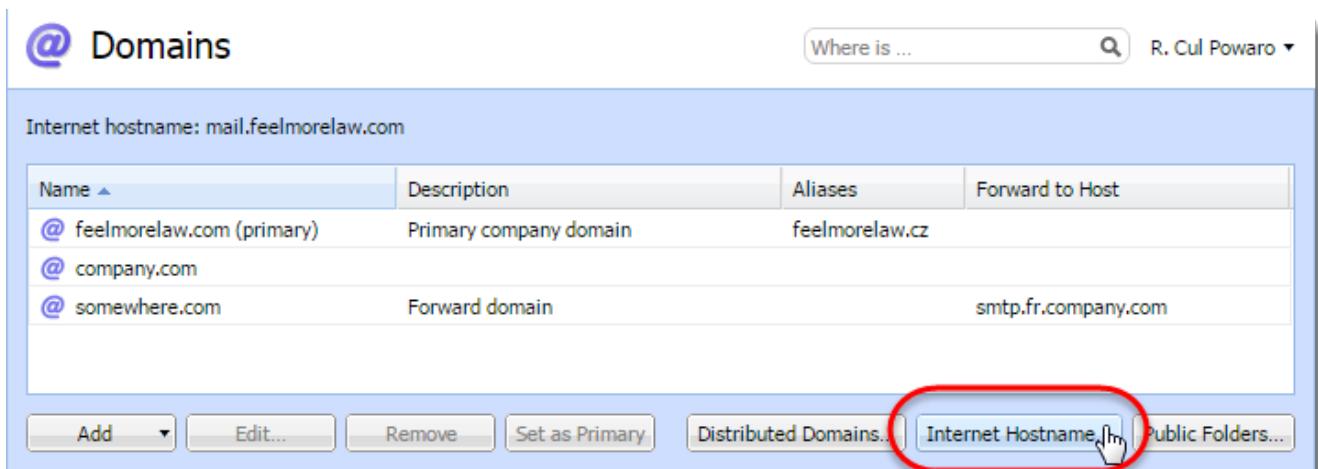
1. In the administration interface, go to **Configuration > Domains**.
2. Click the **Internet hostname** button.

@ Domains

Internet hostname: mail.feelmorelaw.com

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

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



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



Primary domain

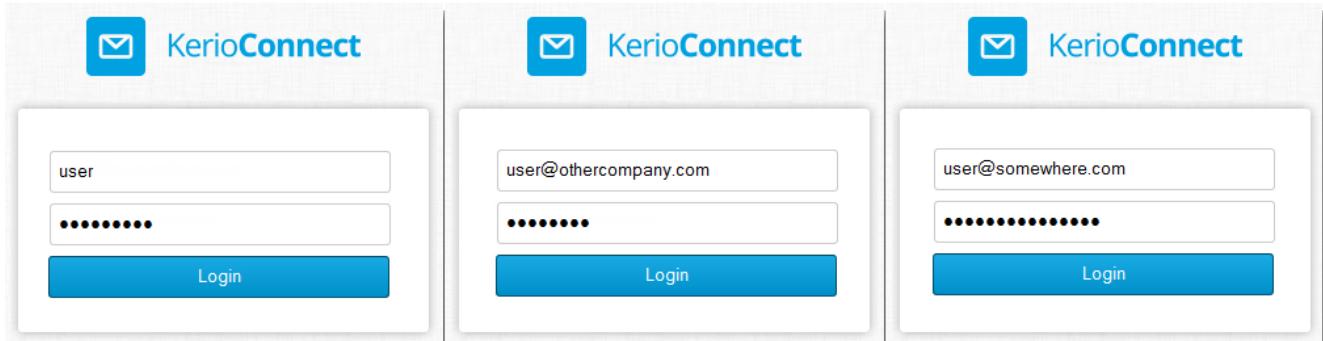
One domain in Kerio Connect must be set as **primary**. Users defined in a primary domain use only their username for authentication, not the whole email address.

@ Domains

Internet hostname: vlucakova-nb.kerio.local

Name	Description	Aliases	Forward to Host	Quota	DKIM enabled
@ feelmorelaw.com (primary)	Feel More Law Inc.			41 %	Yes
@ company.com	Domain of other company	company.cz	mail1.company.com	12 %	No
@ somewhere.com	Forward domain		smtp.fr.company.com		No

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



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**.

@ Domains

Internet hostname: vlucakova-nb.kerio.local

Name	Description	Aliases	Forward to Host	Quota	DKIM enabled
@ feelmorelaw.com (primary)	Feel More Law Inc.			41 %	Yes
@ company.com	Domain of other company	company.cz	mail1.company.com	12 %	No
@ somewhere.com	Forward domain		smtp.fr.company.com		No

Add Edit... Remove **Set as Primary** (highlighted with a red circle) Distributed Domains... Internet Hostname... Public Folders...

Adding new domains

For more information, refer to [Creating domains in Kerio Connect](#) (page 251).

4.3.2 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**.

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

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

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**

Domain:	feelmorelaw.com	Rename...
Description:	Feel More Law Inc.	
User count Number of users in the domain: 50 <input checked="" type="checkbox"/> Limit maximum number of users in the domain: 70		
DomainKeys Identified Mail (DKIM)		

NOTE

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

Limits the disk space per domain

NOTE

New in Kerio Connect 9.1!

You can limit the disk space occupied by a domain and have Kerio Connect sent 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.

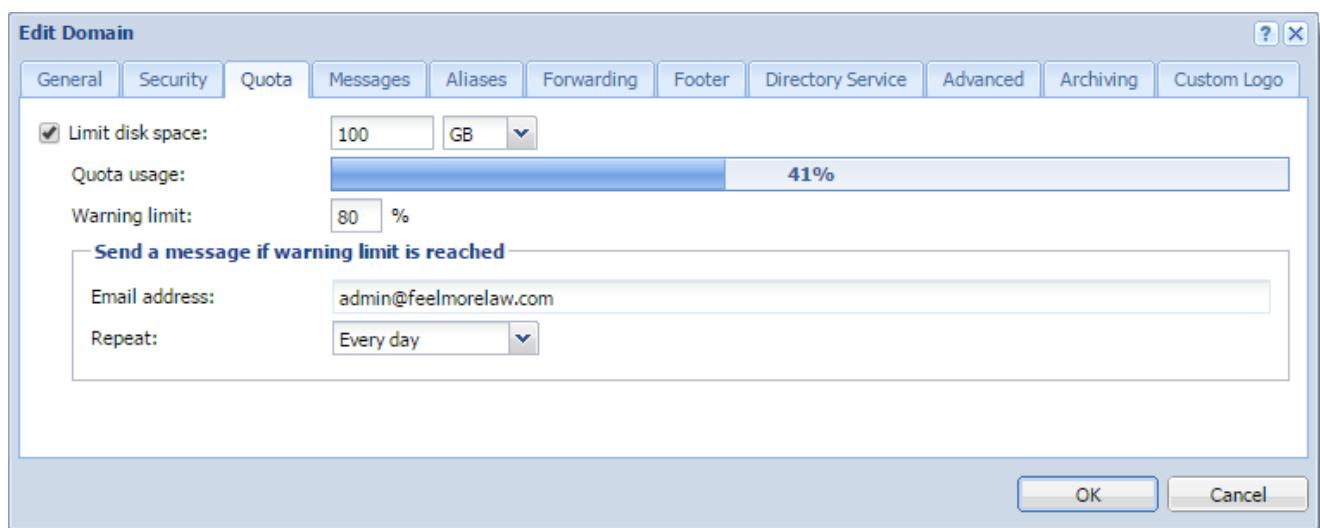
3. Select **Limit disk space** and set the quota.

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**.



Sign outgoing messages using DKIM

For more information, refer to [Authenticating messages with DKIM](#) (page 332).

Enabling chat in Kerio Connect Client

NOTE

New in Kerio Connect 9.1!

For more information, refer to [Enabling chat in Kerio Connect Client](#) (page 187).

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

For more information, refer to [Maintaining user accounts in Kerio Connect \(page 275\)](#).

Creating domain aliases

For more information, refer to [Domain aliases \(page 284\)](#).

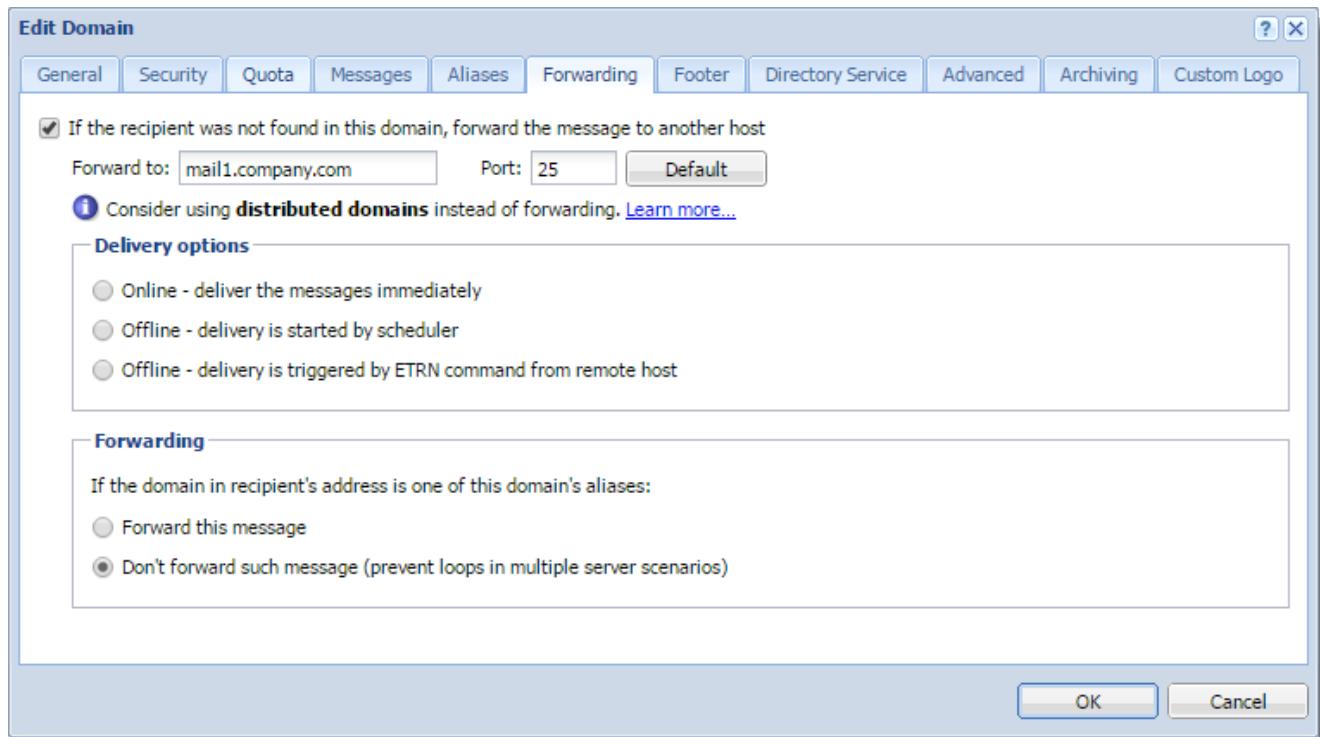
Forwarding messages to another server

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**
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.

NOTE

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



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

NOTE

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.

4.3.3 Adding company and user contact information in Kerio Connect

NOTE

New in Kerio Connect 8.3!

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 (For more information, refer to [Adding automatic user and company details to domain footers](#) (page 218).)

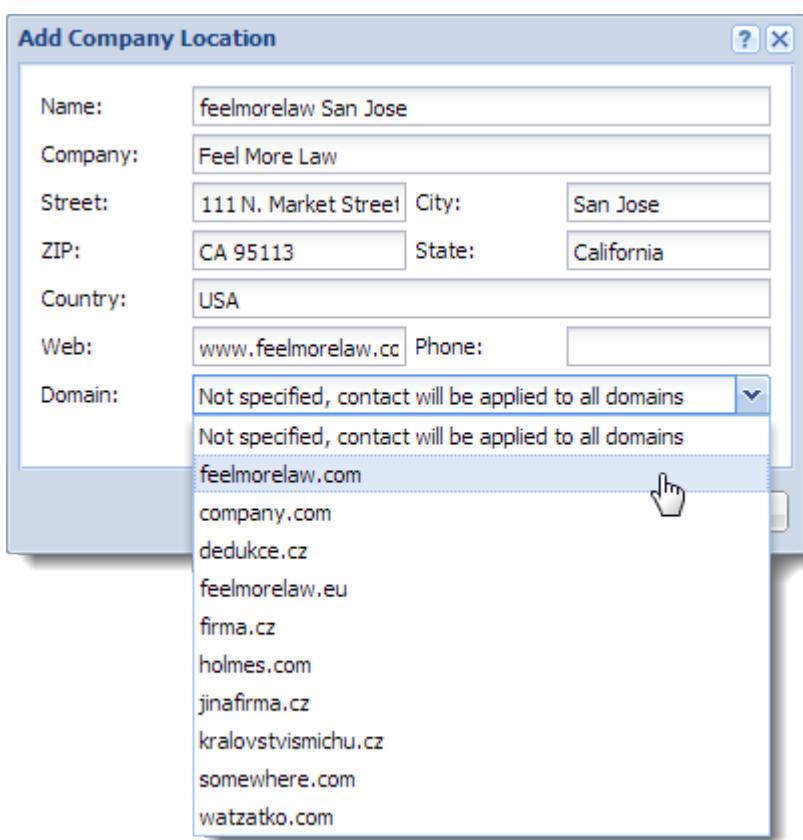
Setting company locations

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

Name	Company	Street	City	ZIP	Country	Web
feelmorelaw Plzen	Feel More Law	Anglické nábřeží	Plzen	30100	Czech Republic	www.feelmorelaw.com
feelmorelaw San Jose	Feel More Law	111 N. Market Street	San Jose	CA 95113	USA	

Add... Edit... Remove

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

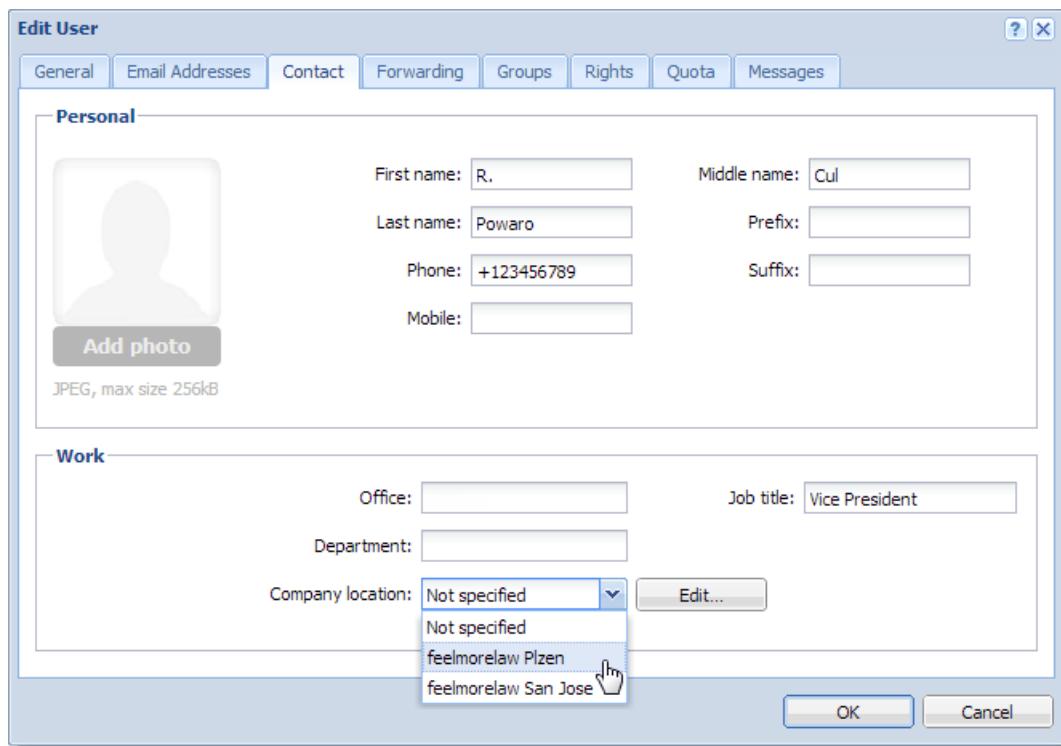


Adding contact details to users

- In the Kerio Connect administration interface, go to **Accounts > Users**.
- In the **Edit User** dialog box, click the **Contact** tab.
- Fill in the user's details.
- Add a photo of the user.

5. Select the user's company location.

6. Save the settings.



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

4.3.4 Renaming domains in Kerio Connect

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
domain name	old_domain.com
names_of_aliases	alias.com old_domain.com alias.com

The domain configuration does not change after renaming.

IMPORTANT

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

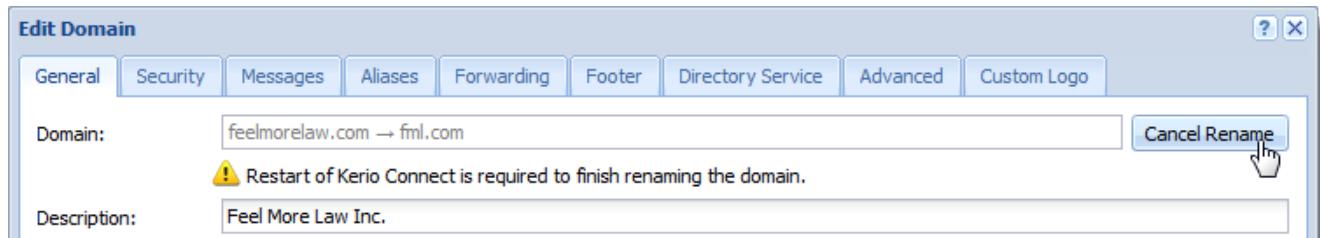
Prerequisites

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

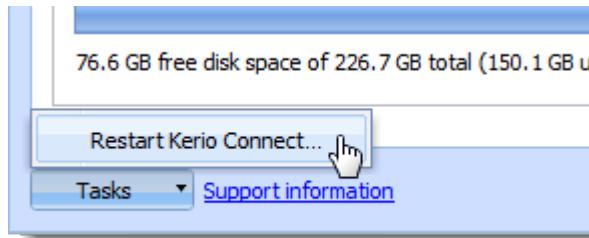
1. In the administration interface, go to **Configuration > Domains**.
2. Double-click the domain you want to rename.
3. On the **General** tab, click **Rename**.
4. Type a new name for the domain. You can cancel the renaming process before you restart the server. Click **Cancel Rename** in the domain's configuration.



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.

You can restart the server in the administration interface: Go to **Status > System Health** and click **Tasks > Restart Kerio Connect** at the bottom.



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.

4.3.5 Distributed domain

If your company uses more Kerio Connect servers physically scattered (located in different cities, countries, continents), you can now connect them together and move all users across all servers involved into a single email **domain** (distributed domain).

For proper functionality of the distributed domain, it is necessary that users are mapped from a **directory service**.

After the distributed domain is configured, the users can:

- » be members of common user groups,
- » access shared contacts (Global Address List),
- » reserve common resources,
- » plan meetings for all users in the distributed domain.

Distributed domain does not support:

- » load balancing,
- » folder sharing (including public folders),
- » sharing of local users and user groups (users and groups that are not mapped from the directory service).

The setting and administration of distributed domains is only possible through Kerio Connect Administration.

System requirements

Hardware configuration of computers on which servers involved in the distributed domain are installed is identical with the configuration used for any Kerio Connect installation.

It is only necessary to keep in mind that (both incoming and outgoing) traffic is processed through the master server and adapt the master server system requirements to the total number of users in the entire distributed domain.

Licensing policy

To add servers to the distributed domain, you will need a separate license for the corresponding number of users installed on each server.

Number of users is counted by email mailboxes/accounts created in the Kerio Connect or imported from the domain. Number of mailing lists, resources, aliases and domains is not limited.

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

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

If you attempt to migrate users to a server where the number of licensed users has already been reached, Kerio Connect will deny the migration.

How it works

To describe the function of distributed domain, it is necessary to separate the user accounts setting from mail delivery, resource sharing and Free/Busy server.

Master/Slave topology

The Kerio Connect distributed domain works on the master/slave basis.

Master server

One of the servers (e.g. in the company headquarters) is set as the master server. To be added to the distributed domain, other servers must connect to the master server.

Master server:

- » is the central (input and output) point of the distributed domain,
- » receives mail and forwards it to the addressee home server,

- » sends mail received from slave servers,
- » has an MX record set for the entire domain,
- » provides antivirus and antispam check of the delivered mail.

For master server, it is recommended to use Kerio Connect with the integrated Sophos antivirus engine.

For correct communication of the master server with its slave servers, it is necessary to allow bi-directional traffic on the following ports:

- » 587, 80, 44337 (TCP and UDP).

WARNING

To enable periodic archiving of traffic in the distributed domain, the mail must be both sent and received through a single central server (master server). It is therefore recommended to set the master server as the relay SMTP server for outgoing email on every slave server.

WARNING

To make the traffic as secure as possible, it is recommended to interconnect all servers in the distributed domain via a VPN (Virtual Private Network).

Slave server

Any other servers connected to the distributed domain are so called slave servers.

For correct communication between slave servers, it is necessary to allow bi-directional traffic on the following ports:

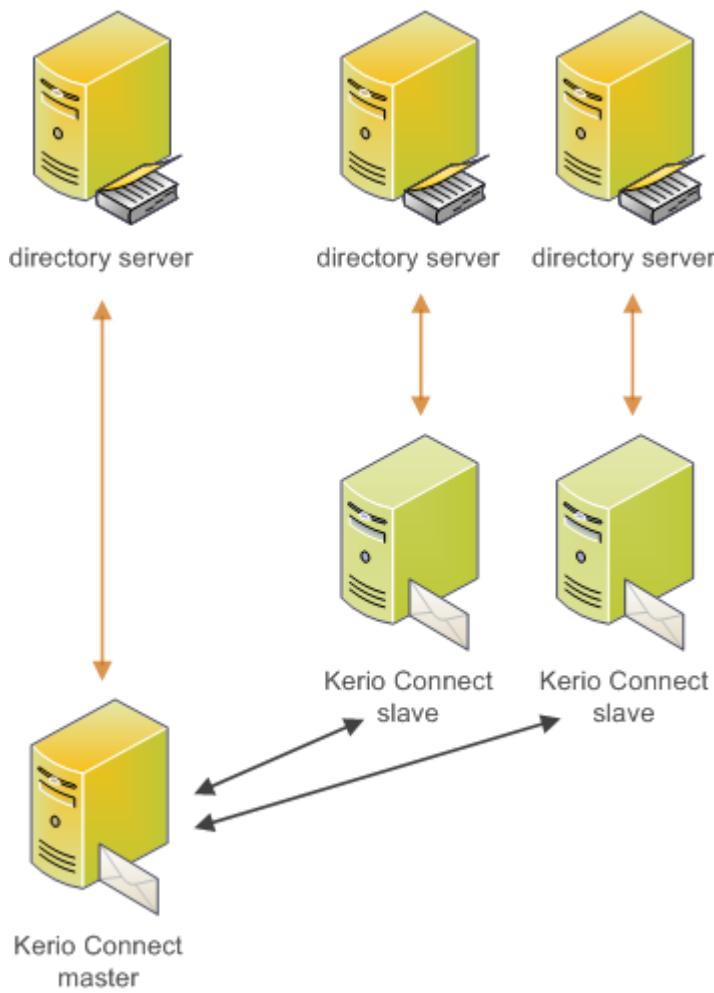
- » 587 and 80.

WARNING

Upon connection, slave servers inherit all domain settings of the distributed domain (including settings of shared folders) from the master server.

[User accounts and their setting](#)

Every server in the distributed domain (either slave or the master) is connected directly to the server with a directory service. Any changes made in the directory service take effect on all the servers in the distributed domain.

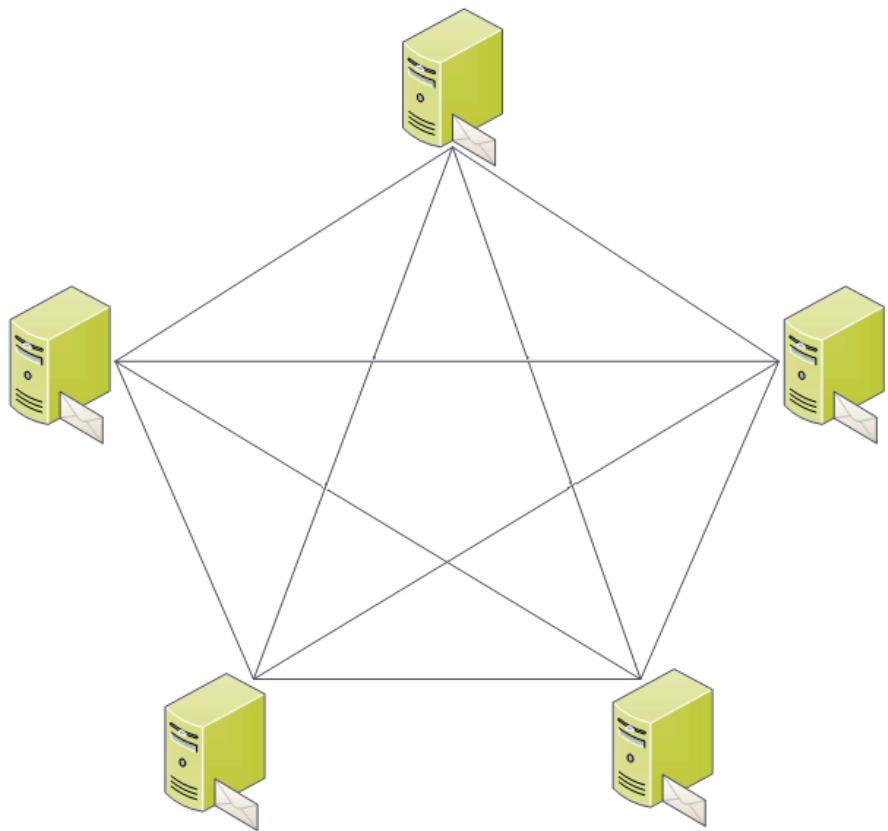


NOTE

It is recommended to use a separate directory server for each server. If you use a single directory server for multiple servers in the distributed domain, make sure that the traffic is fast enough between the servers and the directory service.

Forwarding mail and data sharing

Forwarding emails to the server with the users mailbox, requests for the Free/Busy server and resource administration are not managed by any of the servers. Each server sends the update to other servers. The communication is therefore peer-to-peer.



Distributed domain setting

You do not have to set any of the servers as master or slave. It will be done automatically by connecting the slave servers to their master. Decide which of the servers will be master. For more information, refer to [User accounts and their setting](#) (page 260).

Generally, two scenarios may occur that will be described in the following sections:

- » You have just purchased Kerio Connect and want to install it at several offices which should be interconnected via the distributed domain.
- » You have been using several Kerio Connect servers and now you want to interconnect them via the distributed domain.
- » Clean installation of the servers and their interconnection via distributed domain

The scenario is as follows:

- » Your company has just installed clean copies of Kerio Connect at the headquarters (*mail.company.com*) and two branch offices (*newyork.company.com* and *seattle.company.com*).
- » You want to interconnect all the servers via an only distributed domain called *company.com*. Select the server at the headquarters as the master.

The easiest way to do that is to create a local domain *company.com* on the very master server and map users and groups to the domain from the directory service. Then add the distributed domain on the other servers connection to the master server and the new domain at the branch office will be created within a single operation.

On the master server (at the headquarters with server *mail.company.com*), set the following parameters:

1. Under **Configuration > Domains**, add a new local domain called *company.com*.
2. Now map users from the directory service to this domain.

Other settings must be done on the other servers (slave servers):

1. In **Configuration > Domains**, click on **Add > Distributed Domain**. The first page of the wizard gets opened providing information on how to proceed.

2. Click on **Next**.

3. Enter DNS name of the master server and username and password of a user with admin rights for the master server. Click on Next.

Distributed domains allow mail delivery and free-busy across multiple Kerio Connect servers.

Before you continue, you need to:

- Have a master server. If you don't have one yet, use any Kerio Connect server.
- Have there the domain that you want to add. You can rename an existing one. Domain must be mapped from directory service.

[More information...](#)

Master server name:
mail.company.com

Administrator username:
Administrator

Administrator password:

4. Now select a domain to be added (*company.com*) and click on **Finish** to complete the process. Copies of the company.com domain will be created on slave servers from the original on the master server (including configuration).

5. In the domain list under **Configuration > Domains**, a new column (**Distributed**) appears providing the information whether the domain is distributed or not.

If the distributed domain has been added correctly, the icon next to the distributed domain name in section **Configuration > Domains** is red.

Name	Description	Distributed	Aliases	Forward to Host
company.com (primary)		Yes	company.cz	mail1.company.com
othercompany.com	Domain of other company	No	product.com	
somewhere.com	Forward domain	No		smtp.fr.company.com

NOTE

Another method is to create a local domain (with an identical name and directory service) on all servers and then connect them to the master server.

Interconnecting existing servers via distributed domain

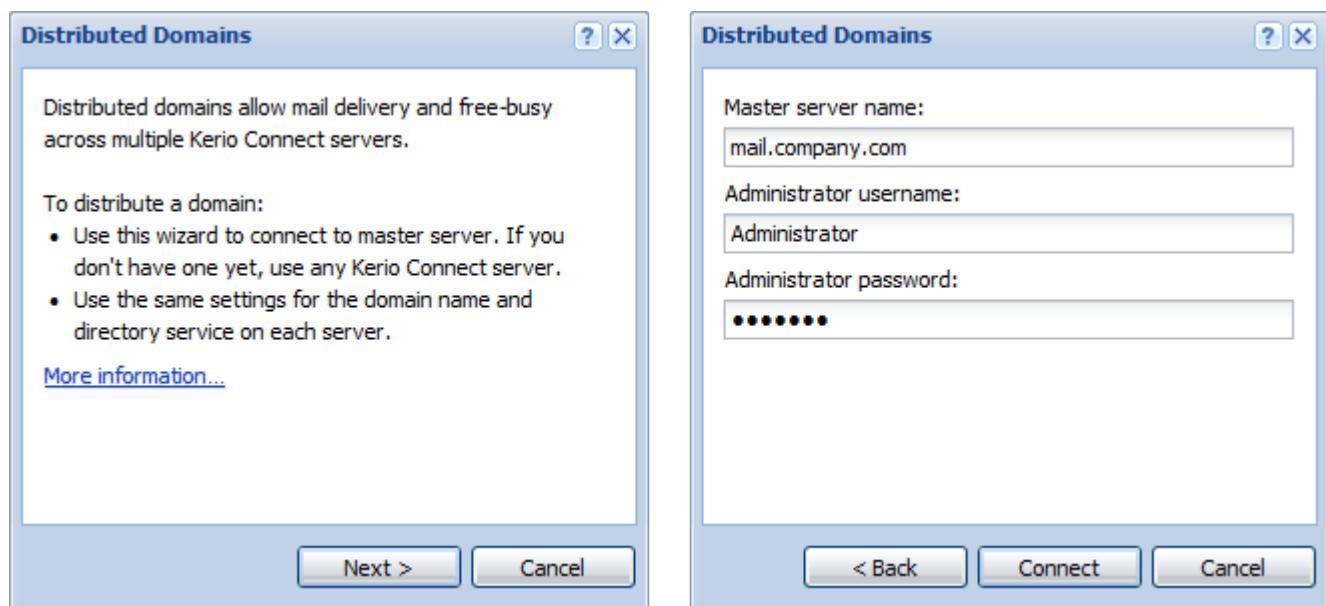
The following scenario will be used as example:

- » The company uses server *mail.company.com* with domain *company.com* at the headquarter and two branch offices with servers *newyork.company.com* (domain *newyork.company.com*) and *seattle.company.com* (domain *seattle-company.com*).
- » All the servers are connected to the same LDAP server.
- » You want to interconnect all the servers via an only distributed domain called *company.com*. Select the server at the headquarters as the master.

Since there are email domains that are supposed to be kept (so that it is not necessary to create new ones), it is necessary to rename these domains. It is recommended to rename domains at the branch offices (i.e. *newyork.company.com* and *seattle.company.com* to *company.com*) and then connect servers at the offices to the master server at the headquarters (*mail.company.com*).

In the administration interface of servers *newyork.company.com* and *seattle.company.com*, set the following parameters:

1. Rename domain *newyork.company.com* and *seattle.company.com* to *company.com*.
2. After server restart, go to **Configuration > Domains**.
3. Click on **Distributed domains**, the wizard first page providing information on how to proceed: Click on **Next**.
4. Enter DNS name of the master server and username and password of a user with admin rights for the master server and click on **Connect**.



5. The server will connect to the distributed domain.

In the domain list under **Configuration > Domains**, a new column (**Distributed**) appears providing the information whether the domain is distributed or not.

If the configuration is correct, the icon next to the distributed domain name in **Configuration > Domains** will get red on all the servers.

Renaming distributed domains

If you wish to rename the distributed domain, follow these instructions:

1. Disconnect all servers from the distributed domain. For more information, refer to [Disconnecting server from distributed domain](#) (page 265).
2. On each server, rename the domain to your desired name.
3. Connect all servers to the distributed domain again. For more information, refer to [Interconnecting existing servers via distributed domain](#) (page 264).

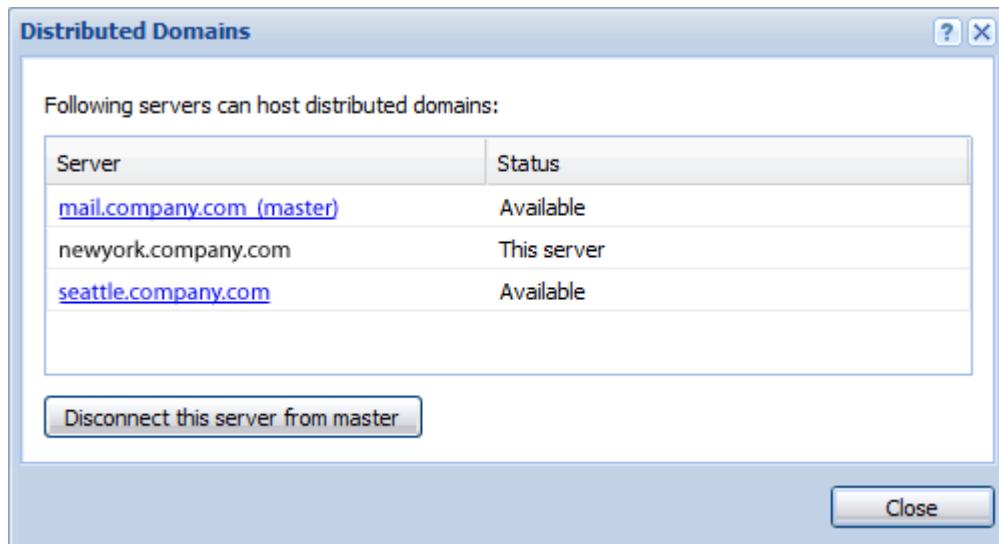
WARNING

Do not forget to first restart the server after you rename the domains and then reconnect them to the distributed domain.

Disconnecting server from distributed domain

To disconnect a server from the distributed domain, use the **Distributed domains** button in section **Configuration > Domains**. Only slave servers can be removed. Once the last slave server is disconnected, the distributed domain is removed automatically.

In **Configuration > Domains**, click the button to open the **Distributed Domains** dialog and click on the **Disconnect** this server from master.



WARNING

The domain can be disconnected only through its own administration interface. If you are connected to a different server, click on its name in **Configuration > Domains > Distributed Domains**. A Kerio Connect Administration login page for this domain will open in your browser.

User accounts in distributed domains

If you use the distributed domain, you administer all users in a directory service. To add a new account to the distributed domain, it is necessary to map it from a directory service. To remove a user from the distributed domain, follow the standard procedure.

You can still add local users to any of the servers. However, they will not belong to the distributed domain and no changes in these accounts will be revealed in the directory service. Local users will be able to use resource planning, Free/Busy server and such but only with accounts of the same server. Users from other servers will not see them.

For administration of domain aliases, mailing lists and resources, please use always the administration interface on the home server.

WARNING

Even though you can keep creating and administrating local items in distributed domain, it is strongly recommended not to do that. However, it can be beneficial to have one local administration account to which it will be possible to connect in case that for example a directory service server is not available.

Administration of distributed domains

Administration roles in distributed domain are as follows:

Kerio Connect administrator

User with rights set as **Whole server read/write**.

- » This user can connect servers to and disconnect them from the distributed domain.
- » The user can also view, edit and migrate users mapped from the directory service on all the servers in the distributed domain.

Administrator of their domain

Users with rights set as **<your.domain> accounts**:

- » The user can also view, edit and migrate users mapped from the directory service on all the servers in the distributed domain.

Migration of user mailboxes in distributed domains

Kerio Connect allows you to move a mailbox physically from one server in distributed domain to another one (this option is useful when an employee is moving to a different company branch).

WARNING

Before migration, it is not necessary to shut servers down. However, it is recommended to make a full back-up of the data store.

Recommendations

- » We advise to perform the migration at night or at the weekend, because it may be very time-consuming (depending on the number of user accounts and message store size).
- » The user login will not be possible during the account migration. Messages which are delivered during the migration will remain in the queue and will be delivered to the new server after the migration.

Settings

Perform migration on the server to which you want to move the user accounts. Log in the Kerio Connect Administration interface as an administrator.

1. Under **Accounts > Users**, select one or more users to migrate. Accounts that can be migrated have the **Migrate Here** button active.
2. Clicking on **Migrate Here** starts migrating mailboxes to the target server. Mailboxes will be moved one by one.

The **Home server** column shows migration status of the accounts.

Migration can be canceled by the **Cancel migration** button, if necessary. All temporary files will be removed and the mailbox will stay unchanged on the original server.

After the migration of each account, the administrator gets a message with information about:

- » migration result (Completed successfully, Error, Canceled),
- » time of the migration,
- » size of the migrated mailbox.

The screenshot shows the 'Users' page in the Kerio Connect web interface. The domain is set to 'company.com'. A context menu is open over the row for 'jsmith', listing options: 'Migrate Here', 'Recover Deleted Items', 'User Statistics...', and 'Mobile Devices...'. The status for 'jsmith' shows 'seattle.company.com'. A message at the bottom left says 'Migration finished.'

Username	Full Name	Home Server	Description
Admin	Administrator	mail.company.com	
dpeterson	Diane Peterson	✓ seattle.company.com	4DD
spostman	Sam Postman	newyork.company.com	Sales dept.
jwayne	John Wayne	seattle.company.com	
jsmith	John Smith	✓ .com	

If the migration is successful, perform a new full backup (especially when a different backup is set).

To see which users (either local or from a directory service) have their account physically on the current server, check **Show only users from this server** on the right side of the distributed domain in the upper section of **Accounts > Users**.

WARNING

If the migrated user shares any folders with local users (users that are not members of the distributed domain), they will not be able to see; from the new server.

Communication problems

If connection to the master server is down, then:

- » all slave servers can communicate with each other locally,
- » incoming and outgoing email will be queued until connection to the master server gets restored.

If connection with any slave server is down, then:

- » users from this server will be unavailable unless the server connection gets restored,
- » incoming email for these users will be queued,
- » activity of the other slave servers and the master server will not be affected.

4.3.6 How to change a user's authentication method from internal, to Active Directory or Open Directory

In some situations, you may have users configured in Kerio Connect with internal authentication and you would like to change their authentication method to a Directory Service. This can be done quite easily, and with little or no disruption to the user. The steps for this procedure are described below:

1. Make sure that your Kerio Connect server is properly authenticated on the Kerberos domain of your Directory Server.
2. Make sure that your Kerio Connect server is properly mapped to the Directory Server and the schema extensions have been installed.
3. Log into the Web Administration and navigate to the Users dialog. (**Accounts > Users**).
4. Edit the user and take note of any custom configurations such as email addresses, quotas, rights, or message restrictions.
5. Remove the user you would like to authenticate against your Directory Server.
6. When prompted, choose "Do not delete the user's message folder". Also, uncheck the option to remove aliases and other memberships as you will be immediately re-adding the user.
7. Choose to add a user, and specify that they will be mapped from a directory service.
8. Locate the user from the list and add them. Update any custom configuration regarding email addresses, quotas, rights or message restrictions.

IMPORTANT

The login name of the Directory based account must match the login name of the internal user account. If they differ, you will need to follow the instructions outlined in [KB 243](#)

Note

You can also switch users from Directory based to Internal by reversing the instructions above.

4.4 Accounts

This section provides information how to maintain accounts in Kerio Connect.

4.4.1 Creating user accounts in Kerio Connect	269
4.4.2 Creating user groups in Kerio Connect	272
4.4.3 Maintaining user accounts in Kerio Connect	275
4.4.4 Creating mailing lists in Kerio Connect	281
4.4.5 Creating aliases in Kerio Connect	283
4.4.6 Configuring resources in Kerio Connect	287
4.4.7 Renaming user account	289
4.4.8 How do I create a catch-all email address?	290
4.4.9 How do I move a user to a different domain?	290

4.4.10 How do I re-index a user's folder if it has become corrupt?	291
4.4.11 Is there a convenient way for a list moderator or administrator to mass subscribe people?	291
4.4.12 Resource calendars hide the event subject. Can this behavior be modified?	292

4.4.1 Creating user accounts in Kerio Connect

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. For more information, refer to [Setting access rights in Kerio Connect](#) (page 209).

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

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

Screenshot 13: 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. For more information, refer to [Importing users in Kerio Connect](#) (page 143).

Creating local accounts

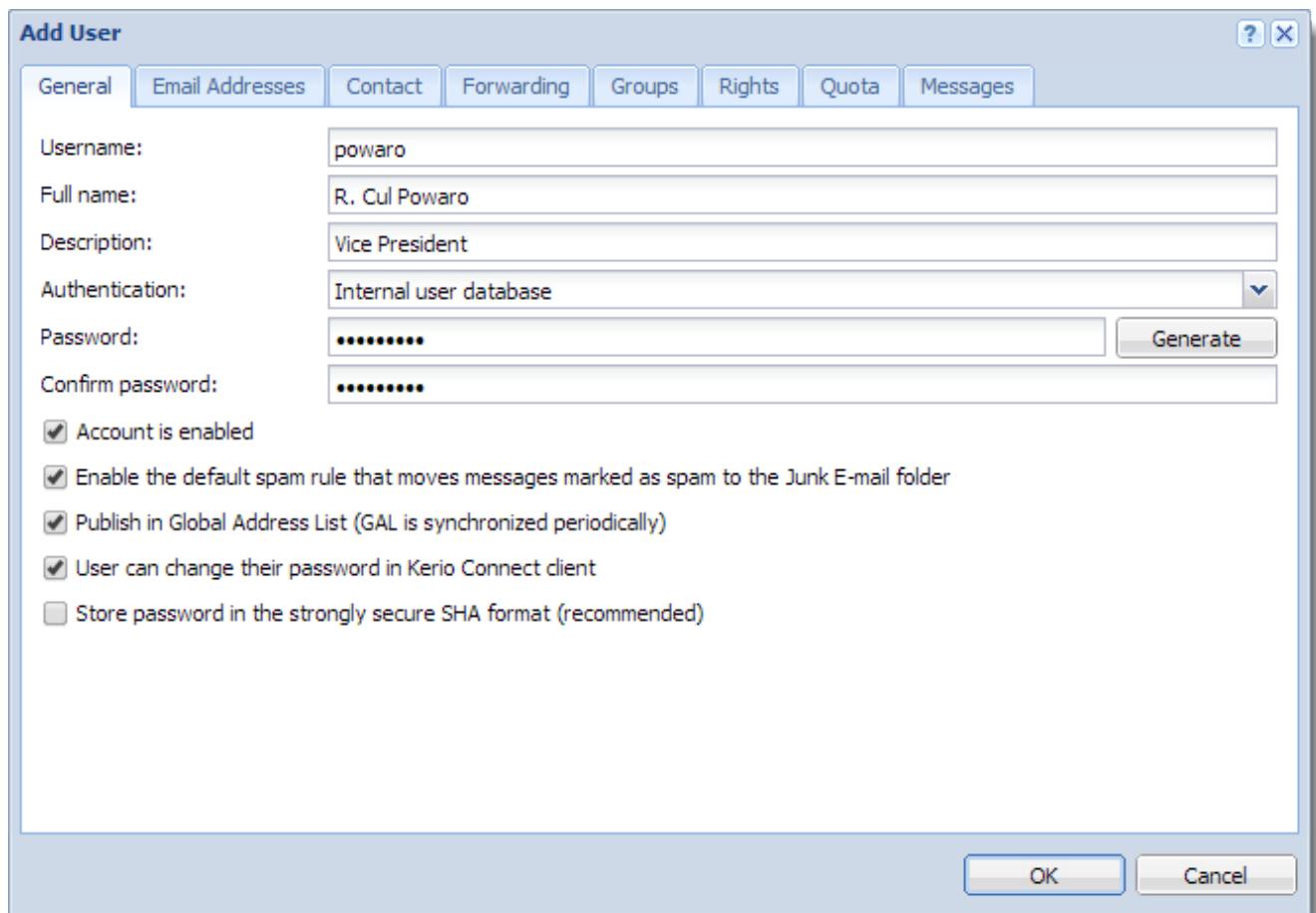
You can create and manage local accounts in the Kerio Connect administration interface.

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. (For more information, refer to [Password policy in Kerio Connect](#) (page 329).)

NOTE

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

4. Click **OK**.



Screenshot 14: Adding users

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

NOTE

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.

NOTE

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**.
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**

NOTE

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](#)

4.4.2 Creating user groups in Kerio Connect

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**.

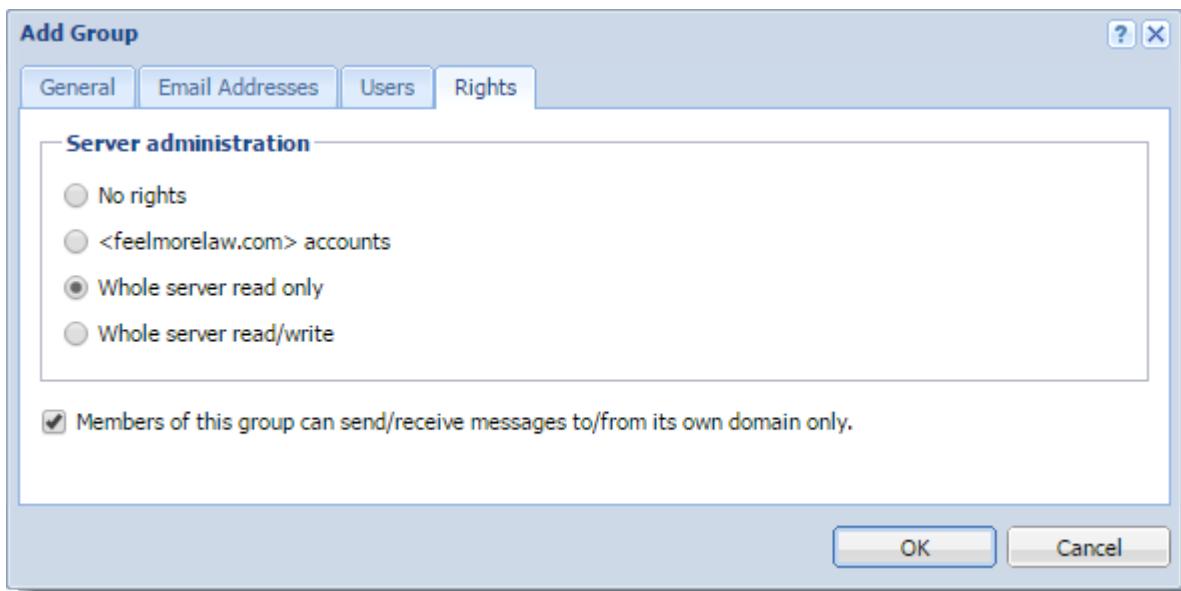
The screenshot shows the 'Groups' section of the Kerio Connect administration interface. At the top, there is a search bar and a user dropdown labeled 'R. Cul Powaro'. Below the header, a navigation bar includes 'Domain: @ company.com' and a 'Search:' field. The main content area displays a table with columns 'Name' and 'Description'. The table contains the following data:

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

At the bottom of the table, there are three buttons: 'Add...', 'Edit...', and 'Remove'.

Creating user groups

1. Go to section **Accounts > Groups**.
2. Select a domain in which you want to create a group.
3. Click **Add**.
4. On the **General** tab, type a name for the group and description.
5. On the **Email Address** tab, add email addresses for the user group. You can add any number of email addresses. You can also use an existing username as the email address — any messages sent to the group email address will also be delivered to the original user.
6. On the **Users** tab, click **Add**.
7. Select the local users you want to add to the group and click **OK**. You can also go to **Accounts > Users** and select a group in user's settings.
8. On the **Rights** tab, set the access right to the administration interface. (For more information, refer to [Setting access rights in Kerio Connect](#) (page 209).



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. For more information, refer to [Connecting Kerio Connect to directory service](#) (page 293).

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**.

NOTE

Kerio Connect does not map nested groups and users.

Exporting group members

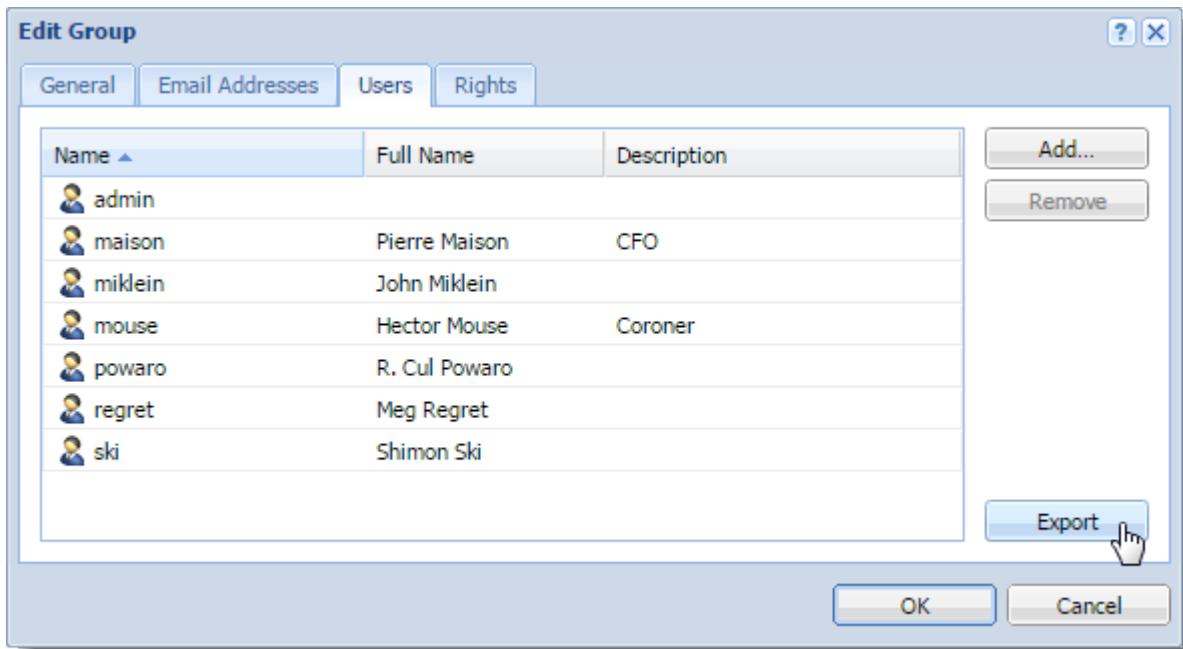
To see the list of members in each group, you can export members of individual groups into a CSV file.

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

To export,

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.

4.4.3 Maintaining user accounts in Kerio Connect

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**.

NOTE

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)

NOTE

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

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"/> years 

 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** 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

<input type="radio"/> Use the settings defined for this domain:	Trash: 30 days, Spam: 30 days, Sent: 30 days
<input checked="" type="radio"/> Use custom settings for this user	
Permanently delete old items in:	
<input checked="" type="checkbox"/> Trash folder, items older than:	55 days
<input checked="" type="checkbox"/> Spam folder, items older than:	55 days
<input checked="" type="checkbox"/> Sent folder, items older than:	55 days
<input type="checkbox"/> All folders except contacts and notes, items older than:	3 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**.

The screenshot shows the 'Users' management screen in Kerio Connect. A context menu is open over the 'maison' user account, listing options: 'Reindex Mailbox', 'Recover Deleted Items' (which is highlighted with a blue selection bar), 'Restore IM Contact List...', 'User Statistics...', and 'Mobile Devices...'. The main table lists users with their full names, descriptions, groups, and last login dates.

Username	Full Name	Description	Groups	Last Login
admin			admins	2015-11-23 1...
fan	Thomas Fan			2015-10-12 1...
laboratory	Laboratory Mailbox			2014-05-05 1...
maison	Pierre Maison	CFO	admins	2015-05-12 1...
miklein	John Miklein		admins	2015-11-17 1...
mouse	Hector Mouse			2015-11-17 0...
powaro	R. Cul Powaro			2015-12-02 1...
regret	Meg Regret			2015-11-27 1...
ski	Shimon Ski			2015-11-27 1...
watzatko	Rada Watzatko			2015-11-17 0...

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

The 'Recovery Result' dialog box displays a table with one row: 'maison' with a green checkmark icon and the message 'Recovered items: 36'. A 'Close' button is at the bottom right.

Name	Result	Message
maison	✓	Recovered items: 36

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

NOTE

If you do not enable 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 the 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)

NOTE

If both are configured, settings per user are applied. You can also use server filters. For more information, refer to [Filtering messages on the server](#) (page 224).

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.

NOTE

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

5. Click **OK**.



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. For more information, refer to [Installing Kerio Connect](#) (page 13).

Limits 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**.



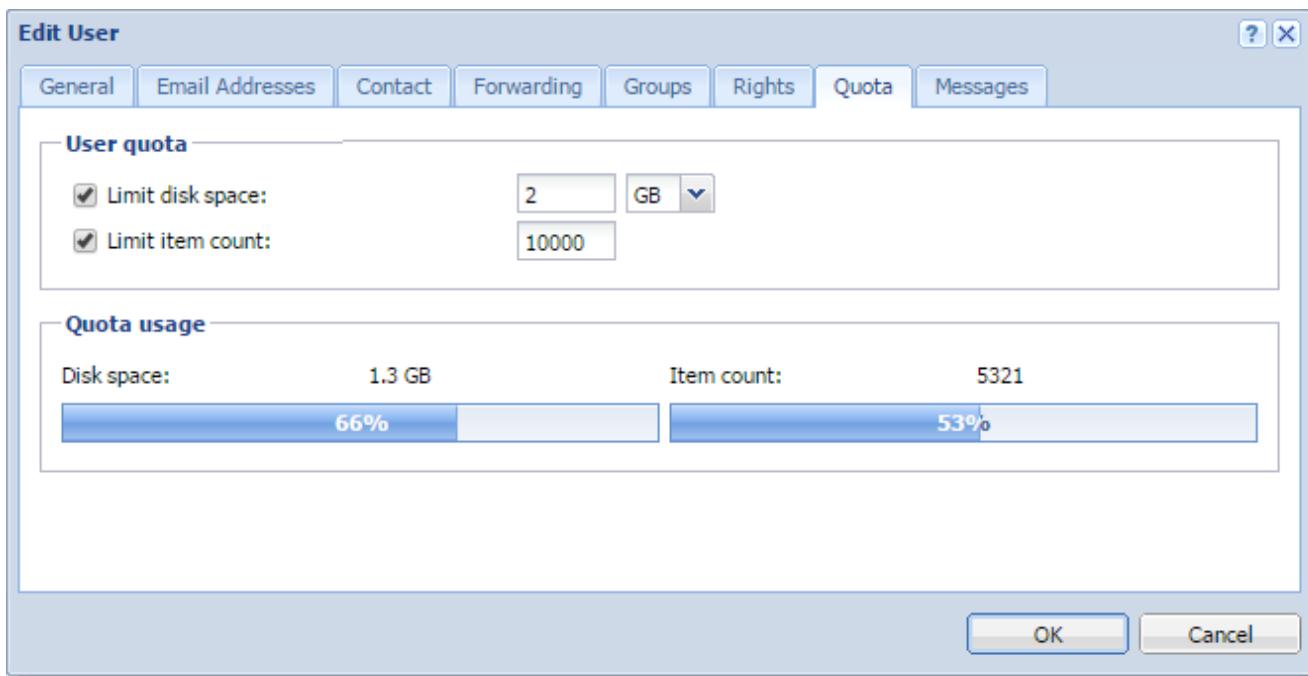
NOTE

You can also use server filters. For more information, refer to [Filtering messages on the server](#) (page 224).

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**.

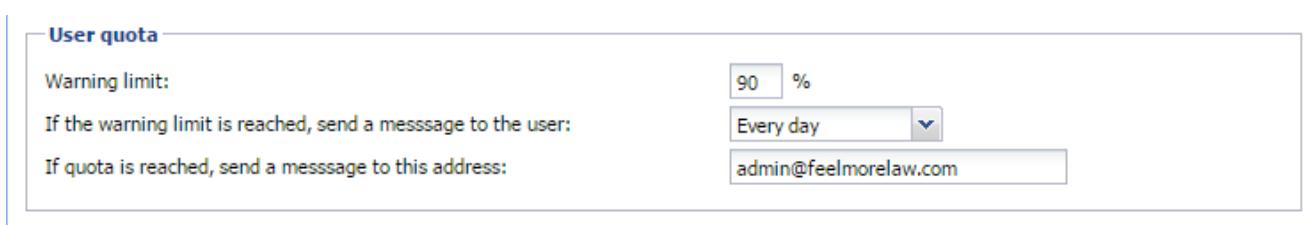


Notifying users about reaching their quotas

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

To 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:
 - 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**



4.4.4 Creating mailing lists in Kerio Connect

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**.

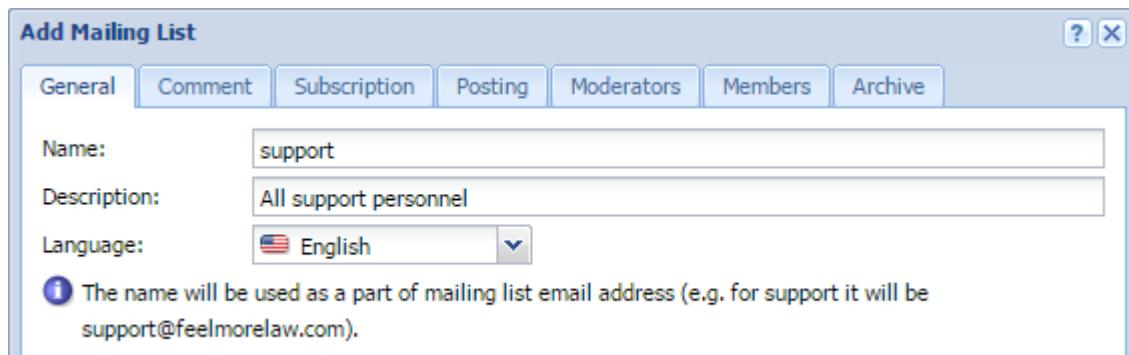
3. Type a name for the mailing list. The mailing list name must not:

- 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.

NOTE

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



5. (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 semi-colons (;). 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.

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

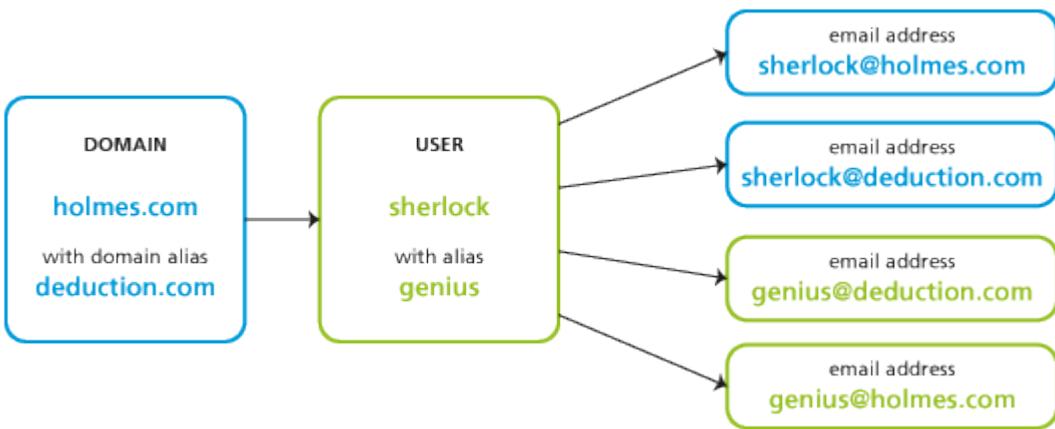
If any problem regarding mailing lists occurs, consult the [Debug log](#) (right-click the Debug log area and enable **Mailing List Processing** in **Messages**).

4.4.5 Creating 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:



Screenshot 15: Map of aliases for a single user account

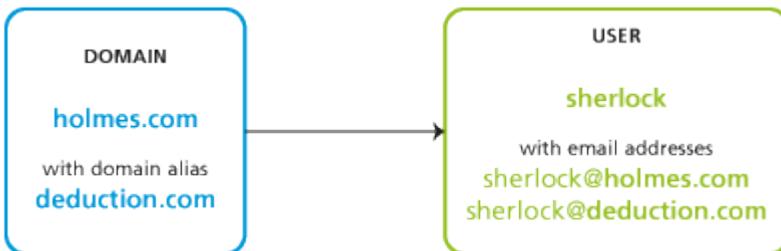
Domain aliases

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

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

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

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



Screenshot 16: Domain aliases

NOTE

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.

IMPORTANT

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).

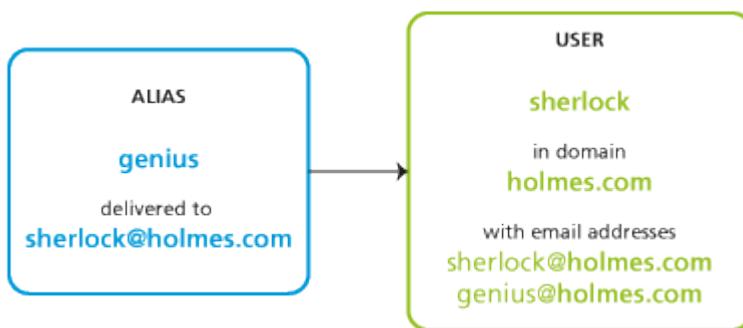
Aliases can be linked to:

- » a user
- » a group
- » an existing alias

NOTE

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):



Screenshot 17: Username aliases

If users have username aliases defined, they can select from which addresses they want to send their messages. For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1331

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 from the menu

NOTE

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

5. Confirm and save.

Example:

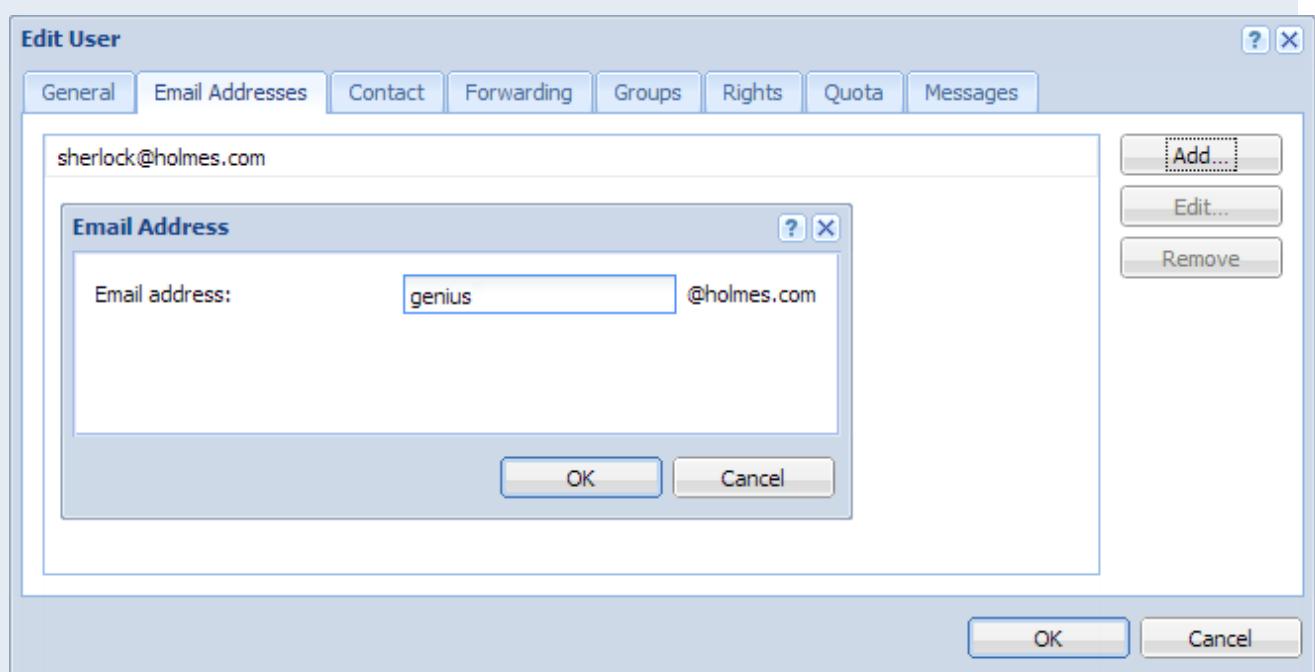
Mr Sherlock Holmes has an account with username **sherlock** in domain **holmes.com** (therefore, his email address is **sherlock@holmes.com**).

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

He orders Dr Watson to create an alias in section **Accounts > Aliases**. The alias is **genius** and is delivered to email address **sherlock@holmes.com**.

From now on, all messages sent to **genius@holmes.com** will be delivered to **sherlock@holmes.com**

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



Screenshot 18: Domain aliases

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

Special scenarios

Alias for messages to be stored in a public folder

Mr Holmes wants messages sent to **info@holmes.com** to be stored 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

NOTE

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

Alias as a protection against wrong spelling — one character

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

Alias as a protection against wrong spelling — numerous characters

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

Checking aliases

In Kerio Connect you can verify all the aliases.

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

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

4.4.6 Configuring resources in Kerio Connect

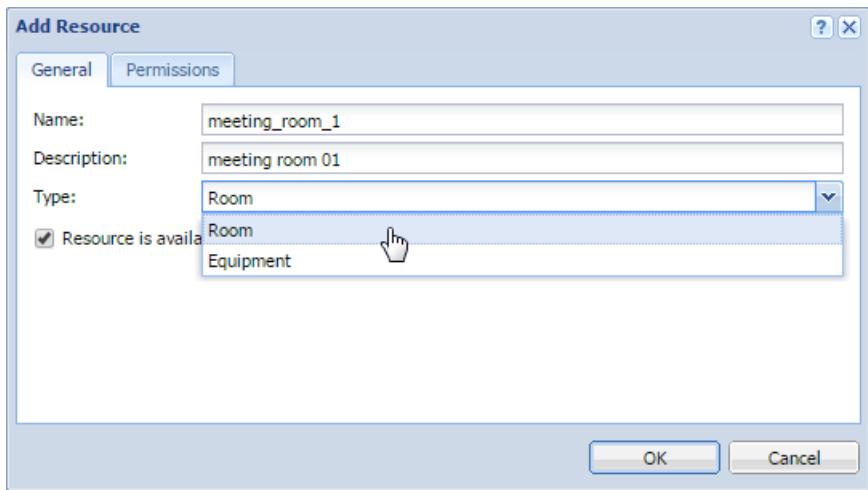
Resources are meeting rooms and other facilities, such as conference rooms, cars, parking lots.

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



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:

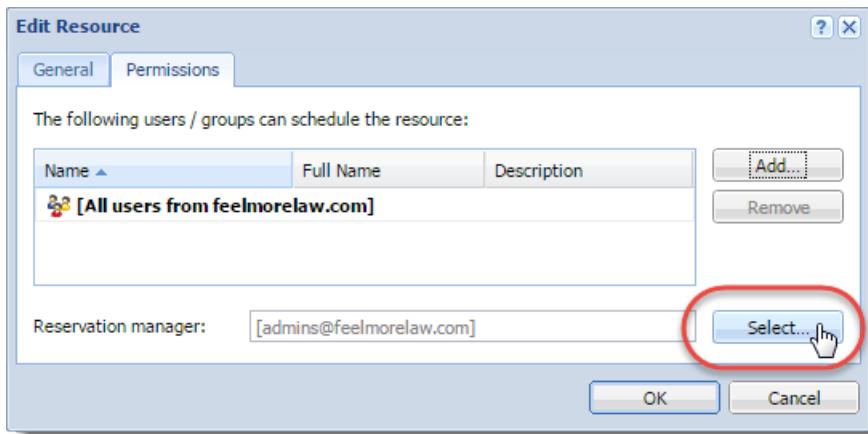
- » Add events directly to the resource calendars, and edit them
- » Delete any event in the resource calendar

NOTE

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**



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

For more information go to http://go.gfi.com/?pageid=connect_help#cshid=1852

Troubleshooting

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

4.4.7 Renaming user account

The following article describes the steps required to change a user's account name in the **Kerio Connect** server. For a variety of reasons, such as a name change after becoming married, it may be necessary to change the account name of a user. The user will have to use the new account name when logging in from any client and the default email address for the user will change to the new address (such as newname@company.com).

IMPORTANT

It is highly recommended that you create a full backup before you apply any changes. You can make a backup using the Backup feature in **Kerio Connect** server, or by copying `mailserver.cfg`, `users.cfg` and the store directory. Please review this section of our manual for instructions on creating a full backup.

NOTE

This process requires that you stop the **Kerio Connect** service for a period of time.

1. Stop **Kerio Connect** service
2. Rename the user's account directory in the store folder to the new account name. Navigate to the directory where user's mail is stored. The store location can be found in the Admin Console in the **Configuration > Advanced Options > Store Directory** screen. If **Kerio Connect** is installed on **MacOS X** or **Linux**, you will have to log in to the **Kerio**

Connect machine as user "root". From the store location, navigate into the domain directory, e.g., mail/-company.com. Find the user's directory (e.g., j.doe) and rename it to the new account name (e.g., j.smith).

3. Start **Kerio Connect** server

4. Add the new user and delete the old user in the Administration Console (choose the option to NOT delete the user's mail). Click on Apply.

If the user uses a **Kerio Outlook Connector**, or a mobile device with **ActiveSync** account, create a new profile for the user in **MS Outlook** in **Entourage** or other email clients, change the login information in the Account Settings and restart the client.

Because of the complexity of changing the folder sharing and subscribing files, it is recommended that you instruct your users to re-share any folders they had shared with this user and re-subscribe to any folders of this user.

If it is desirable to have future incoming mail that is sent to the old account to go to the new account, create an alias which will deliver any mail addressed to the old email address (such as oldname@company.com) to the new address (such as newname@company.com).

IMPORTANT

All calendar events created before user mailbox rename will not be available for editing or deletion.

4.4.8 How do I create a catch-all email address?

1. Log into the Web Admin
2. Click on the "Aliases" section, which is under "Accounts"
3. Click on the Add button
4. Enter an asterisk "*" in the Alias field (no quotes, just the asterisk)
5. In the Description field it is recommended that you enter something to the effect of "Catch-All Email Address"
6. Set the Deliver to field to Email address
7. In the Email address field either enter an email address, or click the Select button to choose a local user
8. Click OK and then click the Apply button at the bottom

Now if an email is sent to a non-existent email address it will be delivered to the email address specified.

4.4.9 How do I move a user to a different domain?

This topic discusses the steps required to move a user from one domain to another in the Kerio MailServer. It is assumed that the old domain name is called **domain.old** and the new domain name is **domain.new**.

It is recommended that you create a full backup before you apply any changes. You can make a backup using the Backup feature in Kerio MailServer, or by copying mailserver.cfg , users.cfg and the store directory. For more information, refer to [Configuring backup in Kerio Connect](#) (page 165).

Note

This process requires that you stop the MailServer for a period of time.

1. Login to the administration console and create the new user in the new domain.new domain, using the same settings that were previously created for the user.
2. Stop the Kerio MailServer.

3. Navigate to the domain.old directory in your store folder. Perform a "MOVE" of the user folder and place it into the domain.new folder.
4. In the users folder open the sub.fld file in a plain text editor, and replace any instance of domain.old with domain.new. Save and close the file. Repeat this process for the folder.map file if the file exists.
5. Now we need to update the permissions for the Public Folders. There are two possibilities, depending if you have a single set of Public Folders for all domains, or individual Public Folders for each domain:
 - Single Public Folder: Navigate to the mail/#public directory and in the acl.fld file replace all instances of domain.old with domain.new
 - Individual Public Folders: Do the same as above, but each domain folder will have an acl.fld file, so you need to modify that file in each of the #public folders.
6. Start the Kerio MailServer.
7. Delete the old user account in the domain.old domain.
8. Now have the user login to their account on the domain.new domain to ensure that they are able to view all of their data.

4.4.10 How do I re-index a user's folder if it has become corrupt?

Learn to manually re-index a folder that has a corrupted index file. This is usually done after consultation with technical support.

IMPORTANT

This is valid for Kerio Connect 7.2.4 and older only. Since Kerio Connect 7.3.0 re-indexing is done automatically by a background process.

In some situations, Kerio Connect will automatically repair the index file, otherwise this procedure must be done manually.

1. The user must log out of all mail sessions - Outlook, WebMail, etc. It is also REQUIRED that the Kerio Connect service be stopped.
2. Access the user's directory from the server in **/store/mail/domain/user/folder_name/**.
3. In this directory you will find the index.fld file. Rename this file to index.bad. Please note that the file extension must be renamed specifically to .bad.

The next time the user accesses their folder, Kerio Connect will rebuild the index file. If they have a large folder they will experience a slight delay while the file is being rebuilt.

NOTE

Each folder contains its own index.fld file. One of the most common cause of inconsistencies in the index.fld file is local anti-virus software that has not been configured to exclude the scanning of the mailserver and store directories. We strongly recommend using the built-in Sophos antivirus or one of the supported AV plug-ins included with Kerio Connect to scan messages for viruses.

4.4.11 Is there a convenient way for a list moderator or administrator to mass subscribe people?

Learn how to add multiple a mass group of people to a mailing list. After creating a mailing list in Kerio Connect, a members file is created in the store directory.

Default locations:

Mac: /usr/local/kerio/mailserver/store/lists/[domain name]/[list name]

Linux: /opt/kerio/mailserver/store/lists/[domain name]/[list name]

Windows: C:\Program Files\Kerio\MailServer\store\lists\[domain name]\[list name]

This file can be directly modified through a text editor or some type of custom script. The members file is in the following format: `sally@domain.com; Sally Smith` or `john@anotherdomain.com; John Doe`

It is the email address followed by a semi colon, followed by the subscribers name followed by a carriage return. You can then add the email addresses through the file instead of the Admin Console.

4.4.12 Resource calendars hide the event subject. Can this behavior be modified?

This article describes the Resource calendar options and its default behavior. The default behavior to hide the event subject can be changed.

Resource calendars are shared to all users of their corresponding email domain. This means that if an event is scheduled in a resource calendar, all other users in that domain can see the event. For security reasons, the details of the event are hidden to all users. Only the name of the organizer and the scheduled time are provided with the event. In some cases, you may want to change this behavior so that all users have access to the details of the event. For example, you may have a company calendar called 'trade_shows', which you've set up as a resource, and you want that all details of the events added to this calendar are available to all users.

To modify the default behavior, you'll need to edit the **mailserver.cfg** configuration file, located in the installation directory of your Kerio Connect server.

1. Stop Kerio Connect server.

2. Using a text editor, open the **mailserver.cfg** file and search for the "Resource" tag. You'll notice a series of list items, which correspond to each resource you've created on the server. Within each resource item, you will see a value labeled "**ClearEventSubject**". The value is set to 1 by default. Change this value to 0, then save the file.

```
<list name="Resource">
<listitem>
<variable name="Name">test_resource</variable>
<variable name="Domain">support2.test.lab</variable>
<variable name="Description">Resource description</variable>
<variable name="Type">0</variable>
<variable name="IsAvailable">1</variable>
<variable name="ClearEventSubject">1</variable>
<variable name="AllowMultipleReservation">0</variable>
<variable name="Manager">Admin@support.test.lab</variable>
<variable name="Guid">4e2656d0-1536-4f11-83af-dd8c0ca9ddda</variable>
<variable name="ResourceUsers">authuser@support2.test.lab</variable>
</listitem>
</list>
```

3. Start Kerio Connect server.

NOTE

This change is applied to new events only. All events created before the change has the subject information already hidden or removed.

4.5 Directory service

This section provides information how to connect to different types of directory services.

4.5.1 Connecting Kerio Connect to directory service	293
4.5.2 Kerio Active Directory Extension	298
4.5.3 Kerio Open Directory Extension	298
4.5.4 How do I configure KMS on a child Active Directory domain?	299
4.5.5 How do I get the LDAP server in Kerio Connect to work with Microsoft Outlook?	300
4.5.6 How to configure LDAP access in Evolution	302
4.5.7 How to map users from a specific Organizational Unit (ou) only	303
4.5.8 Migrating user accounts from local database to directory service	304
4.5.9 Kerberos Authentication with OSX 10.7 against an OpenDirectory Server	305
4.5.10 Mapping different name from Active Directory	307
4.5.11 Mapping users/groups from an OpenLDAP or Generic LDAP server	309
4.5.12 What ports should be open on my Active Directory controller for synchronization with Kerio Connect/MailServer?	323
4.5.13 Accessing LDAP with LinkSys SPA942	323

4.5.1 Connecting Kerio Connect to directory service

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.

NOTE

- » 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:

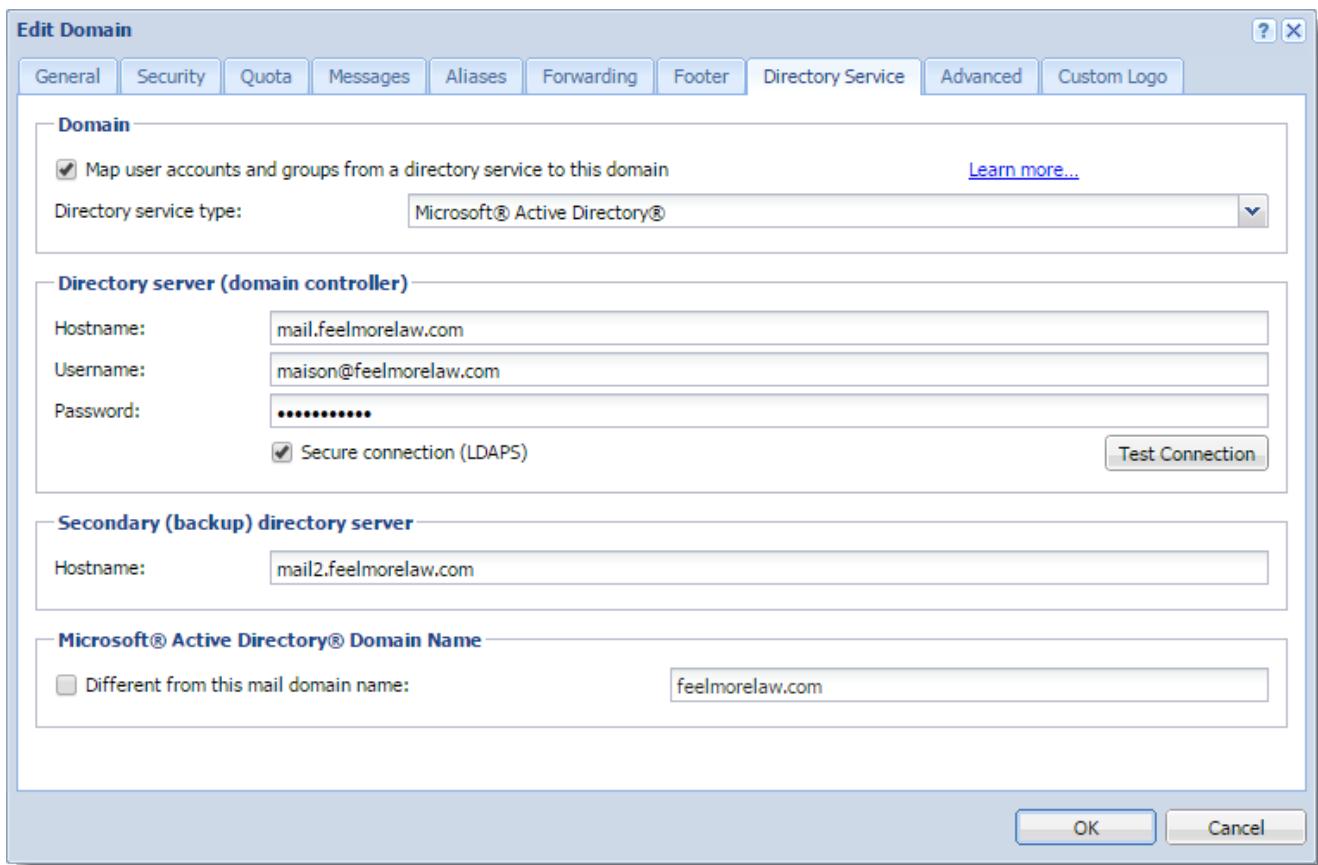
- » Microsoft Active Directory
- » Apple Open Directory

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.

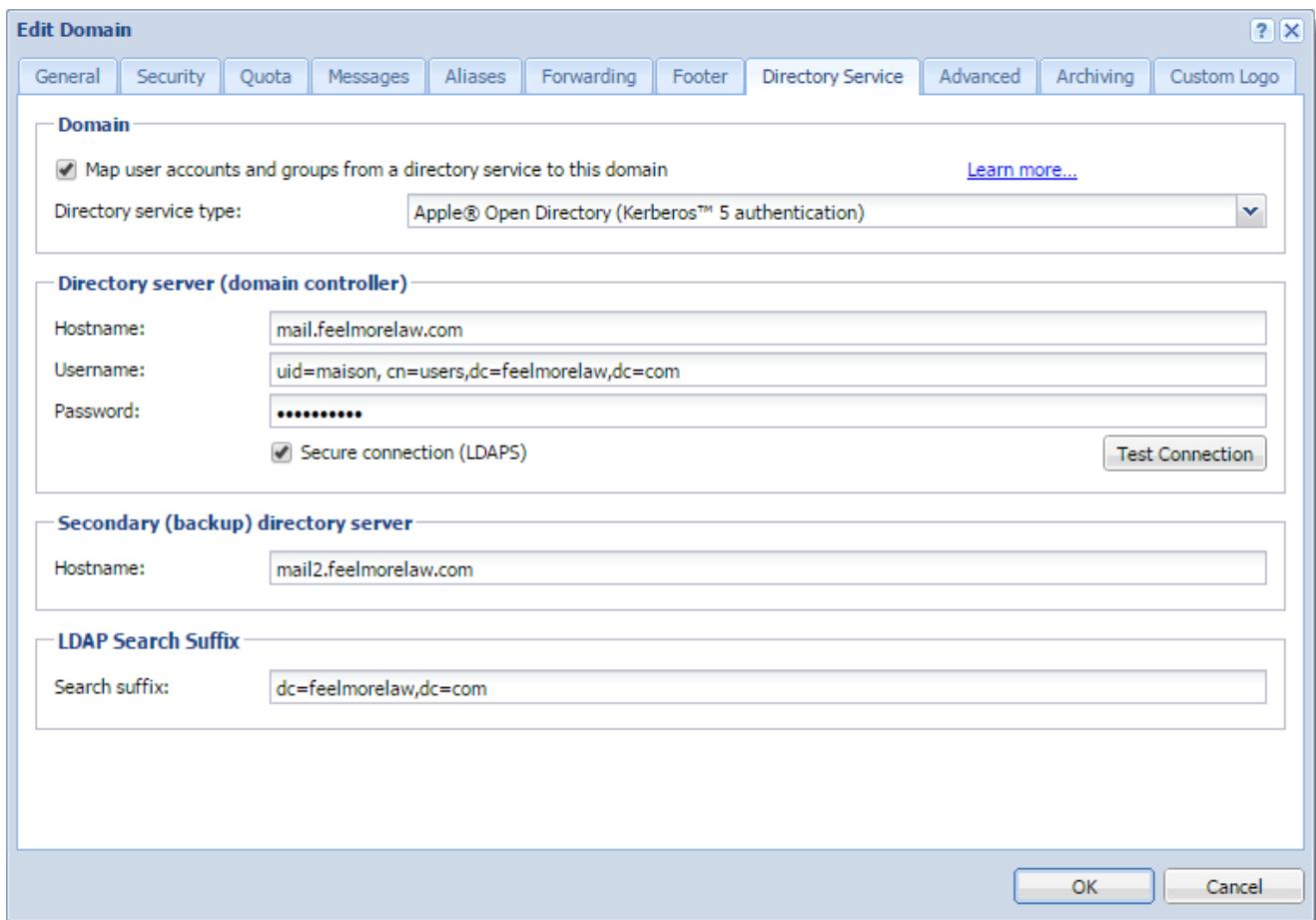
Now you can [map users](#) to Kerio Connect.



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.

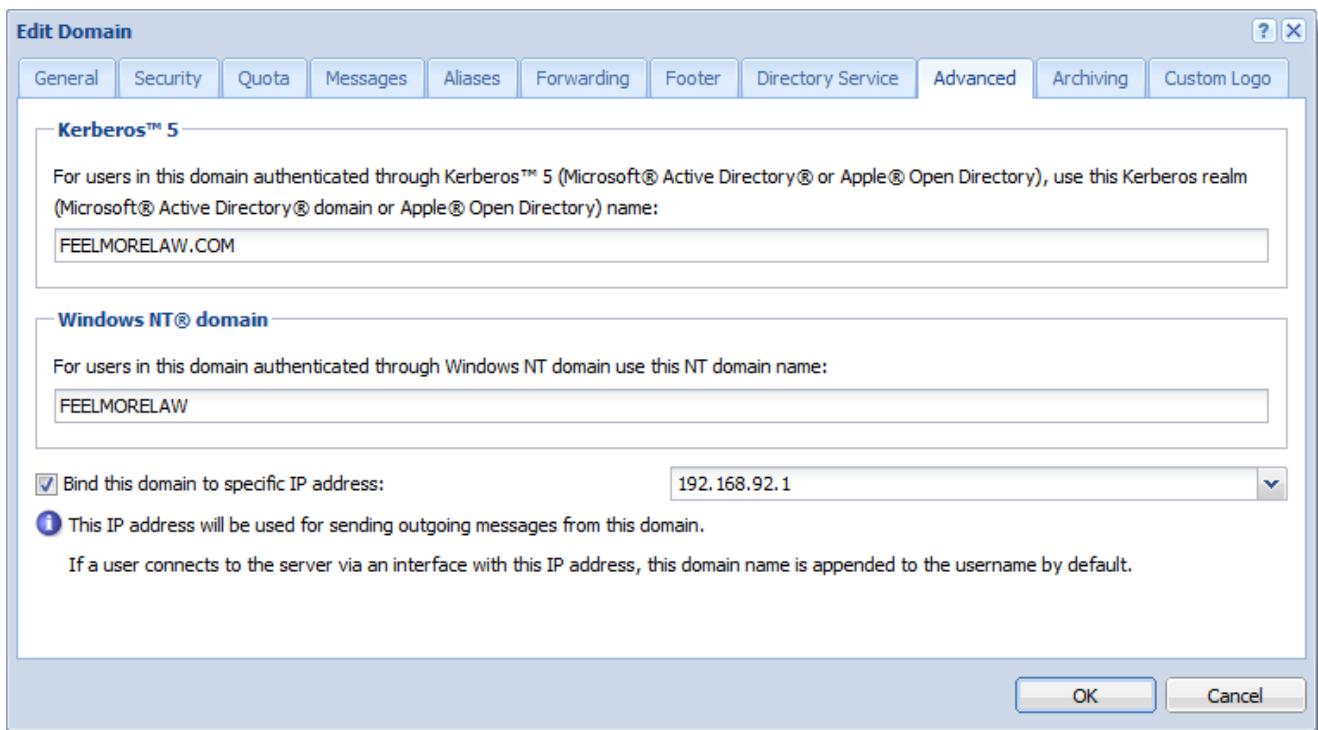
Now you can [map users](#) to Kerio Connect.



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 more information, refer to [Authenticating users through PAM](#) (page 204).
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**



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 more information, refer to [Mapping accounts from a directory service](#) (page 271).

Migrating user accounts from local database to directory service

For more information, refer to [Migrating user accounts from local database to directory service](#) (page 304).

Troubleshooting

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

4.5.2 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.

IMPORTANT

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](#).

IMPORTANT

Usernames must be in ASCII or users will not be able to login to their accounts.

Troubleshooting

If you encounter any problems during KADE installation, view/save the log during the installation process (View Log/Save Log File).

4.5.3 Kerio Open Directory Extension

How to use Kerio Open Directory Extension

When 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.

IMPORTANT

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.

NOTE

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).

4.5.4 How do I configure KMS on a child Active Directory domain?

Step 1 - Configure Active Directory

Ensure that the entire Active Directory structure is configured properly, including setting up internal DNS properly and setting up appropriate trusts between the parent and child domains.

Step 2 - Install Kerio Active Directory Extensions

The Kerio Active Directory Extensions (KADE) only need to be installed on the schema master, which is normally the parent domain controller. The Kerio Active Directory Extensions can be [downloaded here](#). For more information, refer to [Kerio Active Directory Extension](#) (page 298).

Step 3 - Join KMS Machine To Domain

Because of trust relationships that are setup between the parent and the child domains, you can technically join the KMS machine to either the parent domain or any child domain. Please contact your operating system vendor for more information on joining a computer to an Active Directory domain.

Step 4 - Configure Domains Within KMS

Now you need to configure your mail domains inside of KMS and set each of them to map to the appropriate Active Directory domain name. For more information, refer to [Connecting Kerio Connect to directory service](#) (page 293). Please note that on the Advanced tab you will need to modify the Kerberos 5 Realm field to be the Active Directory domain name you are mapping to. So if you are mapping to a child domain, you will need to enter the full child domain name in that field.

Step 5 - Testing/Troubleshooting

Now that everything is configured you should test to make sure that users are able to login sucessfully. The easiest way to verify that authentication is working is to login as a user from each domain in Webmail. Please remember that any user not in the primary mail domain will need to use the full email address in the username field. If you are unable to login as a user this usually indicates a possible configuration issue either in Active Directory or within KMS. The best place to look is the Warning log.

Example Error Messages In Warning Log

```
» [29/Nov/2005 16:26:18] Kerberos 5 auth: user user@CHILD.ADDOMAIN.TEST  
not authenticated, error code c000005e [29/Nov/2005 16:26:18] Win Error:  
1311 - There are currently no logon servers available to service the  
logon request. [29/Nov/2005 16:26:18] HTTP/Webmail: Invalid password for  
user user@maildomain.net. Attempt from IP address 10.0.0.180.
```

One cause of this is that the Kerberos 5 setting in the Advanced tab when editing the domain is not set properly. This needs to be set to the actual Active Directory domain. In this example you will notice that the warning log gives the full user info (user@CHILD.ADDOMAIN.TEST) which tells you what the Kerberos 5 setting is. The "user" is actually in the parent domain, ADDOMAIN.TEST, but for this example I specified the wrong Active Directory domain in order to generate this error message. This same error message will also be displayed if the machine that is running KMS is not joined to the domain. Ensure that the machine is properly joined to the Active Directory domain. Again it does not matter which Active Directory it is joined to.

```
» [29/Nov/2005 16:24:53] HTTP/Webmail: User user@subdomain.maildomain.net  
doesn't exist. Attempt from IP address 10.0.0.180
```

This indicates that the user used the wrong mail domain in the username field. Please ensure that the user is specifying the correct mail domain when logging into the server.

4.5.5 How do I get the LDAP server in Kerio Connect to work with Microsoft Outlook?

LDAP is an acronym for Lightweight Directory Access Protocol. LDAP is used by Kerio Connect as a way of searching through your Contacts folders in your Email Client, like Outlook or Entourage.

The LDAP server in Kerio Connect will only search in any contact folders you can view in Outlook or WebMail. You can also add public and shared contact folders directly in Oulook using the Outlook Connector.

Before you can add a public or shared contact folder to your list, you will need to create it. By default, each email domain comes with a public contact folder named "Public Contacts" which all users on that domain may read. If you have multiple domains, you have the option to make the public folders global for all domains.

If you are using the Kerio Outlook Connector, you do not need to add an LDAP address book, and you may skip this article. A default Outlook Address Book is created which uses the MAPI protocol, and provides the same search features. Under Outlook 2000, you may need to create this address book. Please see "Add or Remove an Address Book" in Microsoft Outlook Help.

Creating A Public Contact Folder

Creating a public folder requires several actions within the Web Administration, and your email client; either WebMail or Outlook may be used. Folders created in WebMail are viewable in Outlook, and vice versa.

Creating a user with Public Folder administrative rights

1. Log into the Kerio Connect Web Administration Console with a user account that has read/write rights.
2. Within the Web Administration Console, go to Configuration > Users.
3. Create a new user for public folder administration, or edit a pre-existing user.
4. On the "Rights" tab, the "This user has administrator rights to public folders" should be checked.

How to create the public folder and share it - WebMail

1. Log into WebMail with the Public Folder administrator user.
2. Within WebMail, right-click on the "Public Contacts" folder and select "New subfolder".
3. Create a new folder of type "Contacts" and supply an appropriate folder name.
4. By default, all users will be able to read this folder. To change permissions on the folder, right-click and select "Share folder."

How to create the public folder and share it - Outlook

1. Log into Outlook (with the Outlook Connector) as the Public Folder administrator user.
2. Select the Public Folder group and right-click. Select "New Folder".
3. Create a folder of type "Contacts" and supply an appropriate folder name.
4. By default, all users will be able to read this folder. To change permissions on the folder, right-click and select "Share folder."

If you need to import local users into a public contact folder, use the Export feature in the Users section of the Web Administration Console.

Setting Up Outlook To Use An LDAP Directory

1. Start Outlook.
2. Click on the Tools Menu and then Email Accounts.
3. Select "Add a new directory or address book" and click "Next."
4. Select "Internet Directory (LDAP)" and click "Next."
5. Type the IP address or the domain name of the Kerio Connect server in the "Server Name:" field.
6. Check the box "This server requires me to log on."
7. In the "User Name" and "Password" fields type the user name and password for the contact folder you will be searching.
8. Proceed accordingly:

- If you are using the default LDAP port of 389, click the "Next" button.
- If you are using the Secure LDAP port, click the "More Settings" button. Then check the box named "Use Secure Socket Layer" on the "Connection" tab and click the "OK" button. Then click the "Next" button.
- If you are using an alternate port number for the LDAP server, click the "More Settings" button and fill in the appropriate port number. Click the "OK" button, then click the "Next" button.

9. If you are setting up a directory service for the first time then you should receive a pop-up window stating you will have to restart Outlook before the Directory Service will start. Click "OK" to close this pop-up window.

10. Click on the "Finish" button.

11. Exit and restart Outlook.

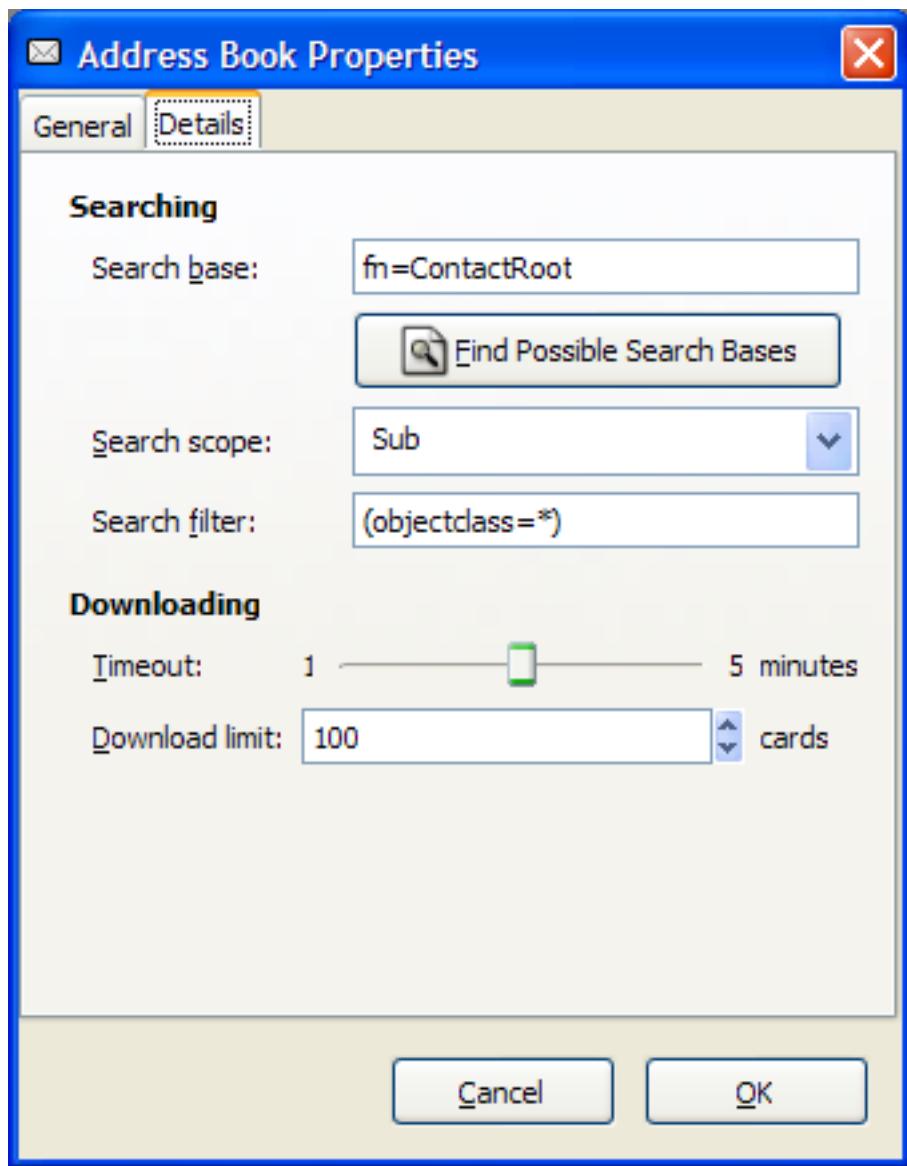
To begin using the LDAP server of Kerio Connect, compose a new email. In the To: or Cc: line, type a few letters of the name or email address you wish to search for and hold down the CTRL key and the letter K on the keyboard. The To: or Cc: line should either fill in with the email address matching your query or you should receive a pop-up window containing the email addresses that match your query.

4.5.6 How to configure LDAP access in Evolution

It is necessary to update Evolution to the current release for LDAP access to Kerio MailServer.

In the account properties for a new address book in Evolution, you will need to specify the authentication (Login method) as 'Using distinguished name (DN)'. The login will be your primary email address. When querying the address book for the first time, you will be asked to supply a password.

On the details page you must supply a Search filter of (objectclass=*), and define the Search scope as 'Sub'. The default search base is fn=ContactRoot, which will instruct Kerio MailServer to search in all private, shared, and public address books.



4.5.7 How to map users from a specific Organizational Unit (ou) only

There are two or more domains on Kerio Connect server mapping users from the same directory service. Both email domains on Kerio Connect server contains same users. There is a need to differ between users according to email domain to which the user belongs.

The LDAP database can use containers to differ between objects. These containers are commonly used to differ between groups, organizations, or departments for example.

Active Directory use following description of such container, which is also the most common container used for such purpose - [Organizational units](#). According to previous description each email domain on Kerio Connect can map users only from a specific container.

Organizational Unit is a full name of the LDAP object. To use organizational units with the Kerio Connect domain mapping you need its Distinguished Name (DN). DN name for this unit is ou=... .

Kerio Connect map users from the default LDAP location by default. This location is defined by the DN name in following format:

dc=domain, dc=com

So by default the Kerio Connect map all users from all containers in the Active Directory as this is the top level structure of the Active Directory tree.

To differ between additional Active Directory / LDAP containers

1. Configure Active Directory mapping according to our manual.
2. Stop Kerio Connect service.
3. Open configuration file mailserver.cfg, which is located in installation directory.
4. Locate following part of configuration file: <list name="Ldap">
5. In this section of the configuration file locate your domain definition - in our example

```
<listitem>
<variable name="Domain">demo.domain.com</variable>
<variable name="ServerName">192.168.65.5</variable>
<variable name="ServerPort">389</variable>
<variable name="BindDn">Administrator@test.lab</variable>
<variable name="BindPassword">DE3:f4cc0ffcf...1d0</variable>
<variable name="MapFile">ads.map</variable>
<variable name="Filter"></variable>
<variable name="UserBaseDn">dc=domain,dc=com</variable>
<variable name="GroupBaseDn">dc=domain,dc=com</variable>
<variable name="Description"></variable>
<variable name="Enabled">1</variable>
<variable name="PrimaryRefreshInt">30</variable>
<variable name="LdapNetworkTimeout">10</variable>
<variable name="SecureConnection">0</variable>
</listitem>
```

6. Change the UserBaseDN and GroupBasedDN search locations according to your path. In our example we change the location to Support department for example.

```
<variable name="UserBaseDn">ou=Support,dc=domain,dc=com</variable>
<variable name="GroupBaseDn">ou=Support,dc=domain,dc=com</variable>
```

7. Save the configuration file.

8. Start Kerio Connect service.

4.5.8 Migrating user accounts from local database to directory service

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:

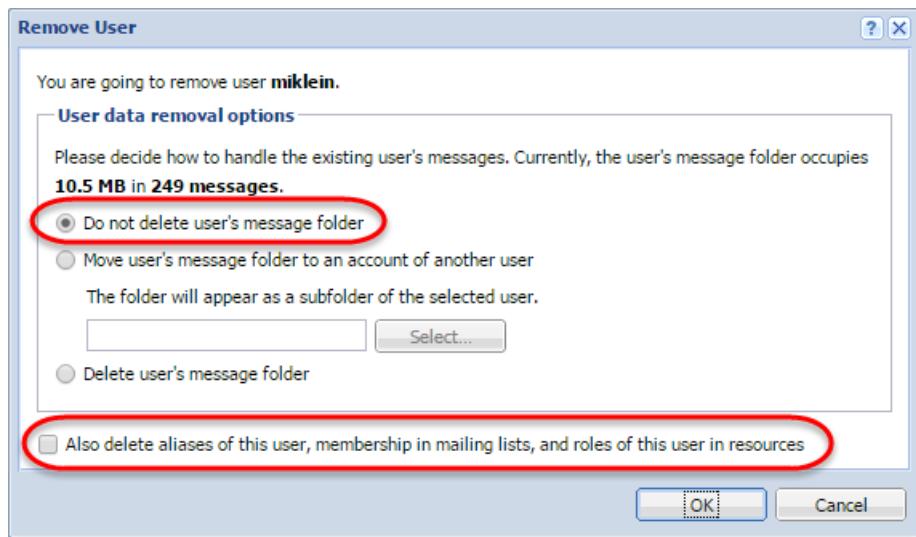
1. Remove the local accounts from Kerio Connect.
2. Connect your domain to a directory service.
3. Create new accounts in the directory service with identical usernames as before.

Migrating users

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

NOTE

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. For more information, refer to [Connecting Kerio Connect to directory service](#) (page 293).
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. For more information, refer to [Mapping accounts from a directory service](#) (page 271).

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. For more information, refer to [Managing logs in Kerio Connect](#) (page 215).

4.5.9 Kerberos Authentication with OSX 10.7 against an OpenDirectory Server

You see authentication errors after you bind an OSX 10.7 machine with Kerio Connect to an OD-Server using Kerberos authentication. This applies despite a successful test of the OD connection.

Starting with 10.7, Apple changed many things in the Kerberos environment. For the purpose of this article, we focus on the file `edu.mit.Kerberos`. This was automatically created in previous versions of the OSX server, when you bind an OSX machine to an OpenDirectory server. The default location is in `/Library/Preferences` - However, this will no longer be created in Lion Server, when you bind the Kerio machine to the OD-Server. Due to the way in which Kerio Connect integrates with an OD server, Kerio Connect still relies on that file.

Solution

You have to create this file manually with a text editor of your choice and save it as a plain text file in `/Library/Preferences`

1. Open eg [TextWrangler \(free of charge\)](#)

2. Copy & Paste the following in the automatically opened "New Document" window (or download the demo file at the end of this article and change it to your needs)

```
[libdefaults]
default_realm = COMPANY.COM
ticket_lifetime = 600
dns_fallback = no

[realms]
COMPANY.COM = {
    kdc = server.company.com. :88
    admin_server = server.company.com.
}
```

3. Replace `COMPANY.COM` with the realm of your OD-Server, replace `server.company.com` with the DNS name of your OD-Server.

4. Save this file as a plain text file in `/Library/Preferences` of the Kerio Connect server and name it `edu.mit.Kerberos`.

5. Restart your server.

Using the `kinit` utility, it is possible to test whether Kerio Connect is able to authenticate against Kerberos. Simply open the prompt line and use the following command: `kinit -S host/server_name@KERBEROS_REALM user_name@REALM`

For example: `kinit -S host/od.company.com@COMPANY.COM jdoe@COMPANY.COM`

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

Now, simply change configuration in Kerio Connect: In the "Domains" section in the Kerio Connect Web administration interface, specify the correct parameters on the "Directory Service" and the "Advanced" tabs (the Apple Open Directory realm must be specified in the Kerberos 5 entry)

IMPORTANT

The Kerberos realm specified on the Advanced tab must be identical to the name of the Kerberos realm specified in the file `/Library/Preferences/edu.mit.Kerberos`. In particular, it must match the `default_realm` value in this file. As a result, the line may read: `default_realm = COMPANY.COM` In the Kerio Connect administration interface, the Apple Open Directory authentication type must be set for user accounts.

Attachments:

» [edu_mit_kerberos.zip](#)

4.5.10 Mapping different name from Active Directory

IMPORTANT

This solution is done at customers own risk. Even if it works and it is tested solution, we cannot guarantee its compatibility across all released versions in the future. We strongly recommend that you backup all modified configuration files in case a future upgrade overwrites them. Tested for Kerio Connect 8.4 and newer.

The AD mapping is based on a special mapping file named ads.map which is located in the installation directory of Kerio Connect in folder **ldapmap**. We map the short (pre Windows 2000) name by default, because it is the most commonly used name by Active Directory users.

It is possible to slightly modify this mapping file to map another property from Active Directory as a user name in **Kerio Connect**. The following text briefly describes the solution and discusses possible aspects of it as the following solution is not directly supported by Technical Support.

This solution maps a different attribute from the Active Directory structure. The attribute is named **userPrincipalName** (User Logon Name in Active Directory settings) and has following format: **user.name@domain.name**. The attribute Kerio Connect maps by default is named sAMAccountName (**User Logon Name** (pre-Windows 2000) in Active Directory settings) and has following format: shortname (it is used as DOMAIN shortname). Both attributes have a different format. However both attributes can be used for authentication in Active Directory as they are aliases for the same username. Users can use the **sAMAccountName** attribute for the authentication to the Active Directory domain (eg. to their computer), and userPrincipalName attribute as Kerio Connect username and email address (the attribute has an email address type format).

There are two possibilities for how the mapped attribute is represented in Kerio Connect. The first possibility is attribute mapping (it is the information displayed in the administration console of Kerio Connect - read operation). This is done using so called map file and the map file can be easily modified according to our needs. The second possible representation of a mapped attribute is the access to the LDAP server of Active Directory (search operation). The search is done to retrieve user attributes or, for example, when new email is received by your Kerio Connect server.

In this solution we are going to modify the userPrincipalName in the map file, it is important both operations (search and read, from Active Directory LDAP server) works properly. The following example shows one more complication. It is the difference between the Active Directory domain name and the Kerio Connect's email domain name:

userPrincipalName attribute is: `name . surname@domain . com`.

The attribute mapped by Kerio Connect would be the username part: `name . surname`.

Kerio Connect would ask for: `name . surname@email . domain . com`

If the Active Directory domain name differs from the email domain name, the user would not be found in the LDAP server of the Active Directory. The mapping is split into two parts as described above. The search and the read operations. It is important to properly define the search operation in the mapping file according to your Active Directory domain name settings.

Active Directory name is the same as the email domain name

Replace the following part in the mapping files ads.map and gal_ads.map:

```
<variable>  
<name>Name</name>  
<value><attribute>sAMAccountName</attribute></value>  
</variable>
```

with the following text:

```

<variable>
<name>Name</name>
<value><attribute regex=".*)@(.*)" result="\1">userPrincipalName</attribute></value>
<search name="userPrincipalName">${Name}@${Domain}</search>
</variable>

```

Active Directory name is different to the email domain name

In this case, you need to specify the correct Active Directory name in the mapping files ads.map and gal_ads.map according to the following example:

```

<variable>
<name>Name</name>
<value><attribute regex=".*)@(.*)" result="\1">userPrincipalName</attribute></value>
<search name="userPrincipalName">${Name}@active.directory.name</search >
</variable>

```

IMPORTANT

The map file is used for all domain mappings defined in **Kerio Connect**. If you need to specify more email domains and you need to use multiple different mappings, per domain map files need to be used as described below.

Per domain map files

It is possible to change the map file **Kerio Connect** uses for each email domain in the configuration file. The following steps are an example for the email domain test.lab and for the custom map file named ads-custom.map.

1. Create a custom map file for each domain (the filename is not important, in our example lets use ads-custom.map)
2. Stop the **Kerio Connect** engine
3. Open the **mailserver.cfg** configuration file in a text editor
4. Locate following section:

```

<list name="Ldap">
<listitem>
<variable name="Domain">test.lab</variable>
<variable name="ServerName">test.kerio.local</variable>
<variable name="ServerPort">389</variable>
<variable name="BindDn">test@kerio.local</variable>
<variable
name="BindPassword">D3S:225a4a0449dd6ea9b49a33b85fa29b2a82eb363e4a62714b
</variable>
<variable name="MapFile">ads-custom.map</variable>
.....

```

5. Modify the MapFile attribute according to the file created for this specific domain, in our example it is `ads-customer.map`.
6. Start **Kerio Connect** server

4.5.11 Mapping users/groups from an OpenLDAP or Generic LDAP server

This article describes how to setup basic OpenLDAP integration with Kerio Connect server.

IMPORTANT

Please note this is not directly supported by Technical Support and you are using this feature at your own risk!!! We recommend to consider if this is really required scenario and we recommend to use some supported solution for not experienced users like the Active Directory integration or the Open Directory integration.

What should you know before you start reading this article

Before you start read the following article for information on:

- » How to edit files under linux, for example using vi.
- » Basic knowledge about linux systems, for example how to install files.
- » Idea about the directory structure you want to implement.
- » This solution describes mapping of users and groups to **Kerio Connect** server.
- » This example use non-secured LDAP binding.
- » Authentication mechanism used in this scenario sends plain text passwords over the network, so it is recommended to have both - OpenLDAP server and Kerio Connect server on the same machine.
- » Example is for SuSe Linux 10.0 or Debian, but it would work for other distributions as well.

LDAP browser might be helpful for editing and for further analysis, such as [JExplorer](#). Following login can be used throughout this example to log into the OpenLDAP server:

- » **Host:** IP Address of the LDAP server
- » **Protocol:** LDAP v3
- » **Base DN:** dc=example,dc=com
- » **Level:** User+Password
- » **User DN:** cn=Manager,dc=example,dc=com
- » **Password:** password

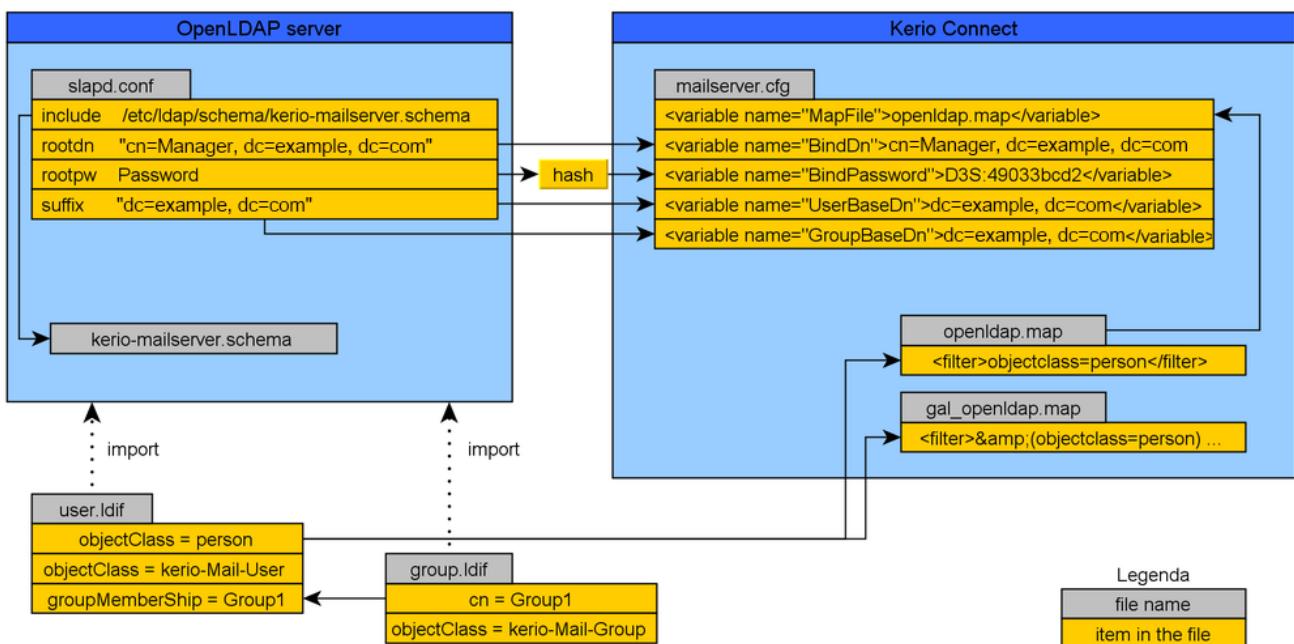
System requirements

- » Supported Linux distribution.
- » Following packages are required in addition:
 - openldap2 - OpenLDAP server package
 - nss-ldap - optional module for user search in OpenLDAP required by some authentication mechanisms
 - pam_ldap - optional module required by PAM module for the user authentication against LDAP

- » **Kerio Connect** installation, it is recommended to install it on the same machine as the OpenLDAP server is due to security reasons.
- » Files in attachment section may be useful during the setup and getting the solution to work.

Overview

Following image is a basic connection map between the OpenLDAP server and **Kerio Connect** server described in this article.



OpenLDAP server installation and configuration

In case you haven't installed the OpenLDAP server yet, install it. You can do it easily using the Yast configuration interface on Suse linux or using following command on Debian linux:

```
apt-get install ldap-utils slapd
```

Install the Kerio Connect server to some local machine or to the same machine as the OpenLDAP server is installed on.

IMPORTANT

In case you will install the Kerio Connect server to the same machine as the OpenLDAP server is installed, you need to modify port number for the built-in LDAP server in Kerio Connect server. Otherwise port conflict appears and the LDAP server may not start properly.

After the installation of OpenLDAP server, default configuration is created. It will be used in this example. But you can modify default configuration according to your needs. The configuration is stored in a file `/etc/openldap/slapd.conf`. There are few fields you will need to configure. In this example let's assume our domain is "my-domain.com", the slapd.conf file will look like following:

```
database dbm
suffix "dc=my-domain, dc=com"
rootdn "cn=Manager, dc=my-domain, dc=com"
rootpw secret
```

```

directory /var/lib/ldap
index objectClass,uid,uidNumber,gidNumber,memberUid eq
index cn,mail,surname,givenname eq,subinitial

```

It contains more information but only these are important in this part of the configuration. Following table describes meaning of each configuration option:

slapd.conf

Database	Database type
suffix	The base distinguished name of the LDAP directory schema
rootdn	Built-in directory manager's name, it is not displayed in the directory structure
rootpw	Built-in directory manager's password, it is not displayed in the directory structure
directory	The directory where is stored the LDAP database
index	Which attributes will be used for indexing

The managers password is stored unencrypted by default. It can be replaced with encrypted password if needed. The hash of the password can be obtained using the following command:

```
/root/ldapconf # slappasswd -h {SHA}
```

New password:

Re-enter new password:

```
{SHA}e4YJDouLxNrSgL/D3m7ZG49EriuICmP8
```

or, using different hash if required:

```
/root/ldapconf # slappasswd -h {MD5}
```

New password:

Re-enter new password:

```
{MD5}c4gYerDyeue6NSgL/D3m7ghGsh9rhtu==
```

Before we will continue, start the OpenLDAP server to double check everything is configured properly:

```
/etc/init.d/ldap start (Suse linux)
```

It is also possible to adjust access lists (ACL) in the `slapd.conf` file. It is not necessary by default and we will not do it in this example. Currently we have OpenLDAP server running. We can double check the server is running properly by performing a simple query:

```

linux:/etc/openldap # ldapsearch -x -b '' -s base '(objectClass=*)' namingContexts
# extended LDIF
#
# LDAPv3
#
# base <> with scope base
# filter: (objectClass=*)
# requesting: namingContexts
#
#
dn:

```

```
namingContexts: dc=my-domain,dc=com
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
linux:/etc/openldap #
```

If there is similar output displayed, the OpenLDAP server is running properly. If you want to start OpenLDAP server automatically during the system startup execute following command:

```
linux:/etc/openldap # chkconfig ldap on (Suse linux)
```

Adding new user/group to OpenLDAP server

This step describes how to add a new users or create a new groups in OpenLDAP server. This is still only OpenLDAP configuration and should be known before we will continue in further configuration steps. The example uses simple objectClass'es which may vary accross LDAP implementations. In case you already use some users/group definition proceed to [next step](#).

Objects can be easily imported to the OpenLDAP directory using LDIF file. The LDIF file is a text file in a format containing data to import/modify/remove objects. This article will not describe the structure of this file, but you can use example files provided in this article. To import a test user account download the [user.ldif](#) file and execute following command or use your LDAP browser to import the LDIF file:

```
linux:/etc/openldap #linux:/etc/openldap # ldapadd -f user.ldif -h 127.0.0.1 -D "cn=Manager,
dc=my-domain,dc=com" -x -W
Enter LDAP Password:
adding new entry "uid=test_user,dc=my-domain,dc=com"
linux:/etc/openldap #
```

The password is requested interactively (-W option), but you can provide it by -w [password] parameter. This password is LDAP administrators password provided in the slapd.conf file. The -f [filename] parameter specifies the LDIF file to import and the -h [IPaddress/hostname] specifies the IP address or a hostname of the LDAP server (in our example both Kerio Connect and OpenLDAP are installed on the same computer, so localhost address is used).

user.ldif file example:

```
dn: uid=test_user,dc=my-domain,dc=com
uid: test_user
sn: User
cn: Test User
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: top
loginShell: /bin/bash
homeDirectory: /home/testuser
```

```
uidNumber: 1001  
gidNumber: 1001
```

Almost the same applies to groups, but the format is slightly different. See example LDIF file named **group.ldif** for more information. To add a group to your OpenLDAP server download the **group.ldif** file and execute following command:

```
linux:/etc/openldap #linux:/etc/openldap # ldapadd -f group.ldif -h 127.0.0.1 -D "cn=Manager
```

```
,dc=my-domain,dc=com" -x -W
```

Enter LDAP Password:

```
adding new entry "uid=Group1,dc=my-domain,dc=com"
```

```
linux:/etc/openldap #
```

group.ldif file example:

```
dn: cn=Group1,dc=my-domain,dc=com  
cn: Group1  
objectClass: top  
objectClass: groupOfNames  
objectClass: posixGroup  
member: uid=test_user,dc=my-domain,dc=com  
gidNumber: 100  
memberUid: test_user
```

There are two independent group definitions - **objectClasses** - in the **group.ldif** file. The **groupOfNames** class and **posixGroup** class. It is not necessary to use both of them, even both are used in this example. Choose one which fits your needs. According to choosed group specify users using the **member** attribute - in case of **groupOfNames** objectClass definition. Or using the **memberUID** attribute - in case of **posixGroup** objectClass definition.

Kerio Connect configuration - directory mapping

Once the OpenLDAP server is configured and new user/group is created, it is possible to bind the OpenLDAP with Kerio Connect server.

IMPORTANT

It is recommended to have a test user and test group in OpenLDAP server before all changes are applied to your existing user accounts. It is also recommended to make a backup copy of the OpenLDAP server configuration and its database.

- » Create a new email domain in Kerio Connect. In Directory Services tab choose the Open Directory service. This service is closest to the OpenLDAP definition and can be used as a reference. Fill in all necessary information in all dialogs according to the example below. Finally test the connection if everything is correct and if it is possible to do LDAP bind against the OpenLDAP server.
- » Extend the OpenLDAP schema for the Kerio Connect's properties. It will not affect any existing user, but it will be possible to add some additional attributes to each user/group definition. These attributes are used only by Kerio Connect to store its own attributes. In case you already have your custom attributes you want to match against the Kerio Connect server, it is possible to use them instead of Kerio ones and adjust the map file which will be described later in this article.

- " To extend the OpenLDAP schema download schema extension file **kerio-mailserver.schema** from Attachments section. Copy schema extension file to **/etc/openldap/schema/** directory.
 - Edit the **/etc/openldap/slapd.conf** file (using the vi editor for example) and add new line to appropriate section of the config file (the section with other includes): `include /etc/openldap/schema/kerio-mailserver.schema`
- » Restart the OpenLDAP server by executing following command: `/etc/init.d/ldap restart`
- » We used the Apple Open Directory mapping as a reference configuration, but there are differences in the OpenLDAP and Open Directory implementation. According to these different implementations we need to adjust Kerio Connect's configuration file **mailserver.cfg**.
- a. Stop Kerio Connect service
 - b. Open **mailserver.cfg** file located in the installation directory of **Kerio Connect**.
 - c. Locate your domain definition in following section of the configuration file: `<list name="Ldap">`
 - d. According to the example below for test domain `example.com` modify the **UserBaseDN** and **GroupBaseDN** search path to appropriate search path in your OpenLDAP implementation. In this example it is "`dc=my-domain,dc=com`" which is default domain after the OpenLDAP installation. But it can be different in case you have some containers for user accounts (for example), or if you use different domain name of course. Also create a copy of the **apple.map** file and save it as **openldap.map** file which we will use for our OpenLDAP mapping. The configuration of **openldap.map** file will be described later in this article.

The **openldap.map** file example is available in Attachment section and it contains all necessary modifications. You can use this file instead.

```

<listitem>
<variable name="Domain">example.com</variable>
<variable name="ServerName">127.0.0.1</variable>
<variable name="ServerPort">389</variable>
<variable name="BindDn">cn=Manager,dc=my-domain,dc=com</variable>
<variable name="BindPassword">DE3:716f95b639c...15</variable>
<variable name="MapFile">openldap.map</variable>
<variable name="Filter"></variable>
<variable name="UserBaseDn">dc=my-domain,dc=com</variable>
<variable name="GroupBaseDn">dc=my-domain,dc=com</variable>
<variable name="Description"></variable>
<variable name="Enabled">1</variable>
<variable name="PrimaryRefreshInt">30</variable>
<variable name="LdapNetworkTimeout">10</variable>
<variable name="SecureConnection">0</variable>
</listitem>

```

- » Start Kerio Connect engine.
- » You should not see any error message when you try to access Users or Groups in Domain Settings tree. You will not see any user yet, because users don't have any **Kerio Connect** properties yet. However this test may prove the LDAP

connection is working properly and **Kerio Connect** extensions were installed properly. In case you receive error message saying the Directory Extensions were not installed properly, check steps above if you specified correct search patch and the include was accepted by the OpenLDAP server.

Extending user definitions in OpenLDAP for the Kerio Connect properties

At this point the OpenLDAP server is configured and Kerio Connect server is configured to connect to the OpenLDAP directory.

But there is still no user mapped from the OpenLDAP directory to kerio Connect. It is because there is no **Kerio Connect** user enabled in your actual OpenLDAP directory. Each user which should have **Kerio Connect** account have to be extended for **Kerio Connect** properties. Follow these steps to extend user's attributes and configure correct user mapping to create a Kerio Connect account for such user:

1. The OpenLDAP user have to be extended for **Kerio Connect** attributes. We can divide it to two groups. First group contains necessary attributes (objectClass definition), second one contains optional attributes. You can modify existing **user.ldif** file according to your needs or you can use an example **kerio-user.ldif** file as a reference one. These modifications can be easily applied by executing following command on your OpenLDAP server:

```
linux:/etc/openldap # ldapmodify -f kerio_user.ldif -h 127.0.0.1 -x -D  
"cn=Manager,dc=  
my-domain,dc=com" -W  
Enter LDAP Password:  
modifying entry "uid=test_user,dc=my-domain,dc=com"  
linux:/etc/openldap #
```

The **kerio_user.ldif** file example...

```
dn: uid=test_user,dc=my-domain,dc=com  
uid: test_user  
sn: User  
cn: Test User  
objectClass: person  
objectClass: organizationalPerson  
objectClass: posixAccount  
objectClass: top  
objectClass: kerio-Mail-User  
loginShell: /bin/bash  
homeDirectory: /home/testuser  
uidNumber: 1001  
gidNumber: 1001
```

Necessary attributes/objectClasses	Description
objectClass: kerio-Mail-User	This option will extend the user attributes set for the Kerio Connect ones. It allows to add optional attributes like the Message Quota, ... It does not activate the account, account needs to be activated using the optional kerio-Mail-Active attribute.

Optional Kerio Connect attributes	Description
kerio-Mail-Active	It activates the Kerio Connect account. 0 - not active 1 - active
kerio-Mail-AccountEnabled	It can enable/disable the account.
kerio-Mail-AdminRights	Admin rights.
kerio-Mail-Authorization	The authorization properties.
kerio-Mail-Address	User's email address.
kerio-Mail-ForwardMode	Forward mode.
kerio-Mail-ForwardAddress	Address to which email should be forwarded in case forward mode is enabled.
kerio-Mail-QuotaStorage	The user's storage quota.
kerio-Mail-QuotaMessage	The max. number of emails user's quota.
kerio-Mail-MaxOutgoingMessageSize	Maximal outgoing message size.
kerio-Mail-WebReplyToAddress	Reply-to address used in webmail interface.

Example minimal attribute set:

Example attribute sets	Description
objectClass: kerio-Mail-User kerio-Mail-Active: 1	The user can have Kerio Connect account. The account is activated (can receive emails).

2. Now it should be possible to activate (Add) new user from the Administration console of **Kerio Connect**. Activated user can not be used because there is no user-group mapping and there is no authentication method specified. To create **Kerio Connect** group in OpenLDAP and to create user-group mapping read [next chapter](#).

Extending group definitions in OpenLDAP for the Kerio Connect properties

OpenLDAP uses different mapping for users and groups than OpenDirectory or ActiveDirectory. Usually other directory services use two directional mapping when each group definition contains users which belongs to the group, and vice versa the user contains the information to which group belongs. This scenario is used in Active Directory or Open Directory.

OpenLDAP uses only one way mapping when group contains its members. But the information in user definition to which group the user belongs is missing. Because of this limitation it is required to create such mapping manually. We can split group integration into two parts. Extending the schema for custom **groupMembership** attribute and to mapping the OpenLDAP group to **Kerio Connect**. Follow next steps to extend the schema for custom **groupMembership** attribute. In addition we are adding **apple-generateduid** attribute which is required since Kerio MailServer 6.7. for web based administration. This attribute is used to uniquely identify user or a group. So it is required to add it to group definition as well (use the same approach as for the user definition in this example). The apple-generatedid is automatically updated by **Kerio Connect** so it is not necessary to define it manually.

1. Open the OpenLDAP schema file defining the user definition - **/etc/openldap/schema/rfc2307bis.schema** in this example. You can modify any schema used for user definition in case you use different OpenLDAP implementation. If you already have such mapping, skip extending the schema for the **groupMembership** attribute and proceed to part describing the group mapping to **Kerio Connect**.

2. Locate last attribute definition in this file.

```
attributetype ( 1.3.6.1.1.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
```

```

SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount' SUP top AUXILIARY
DESC 'Abstraction of an account with POSIX attributes'
MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
MAY ( userPassword $ loginShell $ gecos $ groupMemberShip $
description ) )

```

3. Once you find last attribute definition change it according to following example.

```

attributetype ( 1.3.6.1.1.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
attributetype ( 1.3.6.1.1.1.34 NAME 'groupMemberShip'
EQUALITY caseExactIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetype (1.3.6.1.1.1.35
NAME ( 'apple-generateduid' )
DESC 'generated unique ID'
EQUALITY caseExactMatch
SUBSTR caseExactSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount' SUP top AUXILIARY
DESC 'Abstraction of an account with POSIX attributes'
MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
MAY ( userPassword $ loginShell $ gecos $ groupMemberShip $ apple-generateduid $
description ) )

```

4. Restart the OpenLDAP server to apply changes.

The user definition is now extended for new attributes describing the group to which the user belongs, what is native for OpenLDAP implementations. However we use apple-kerberos.map file. OpenDirectory use different user to group mapping as well as Active Directory. We need to extend also user definition in the map file to properly search Open LDAP for new **groupMembership** attribute mapping:

1. We used Apple Open Directory server mapping as a reference configuration and we created **openldap.map** file based on **apple.map** file. Hence we need to adjust the **openldap.map** file which is used for this mapping. This file is located in **../installation_directory/ldapmap** folder. Locate this file and open it via some text editor.

2. Locate User definition section at the beginning of this file. See this example from original **apple.map** file.

```

<map table="User">
...
<variable>

```

```

<name>Groups</name>
<value><attribute>cn</attribute></value>
</variable>
...
</map>

```

3. Change the directory map file according to following example to alter the user to group mapping in **Kerio Connect**.

4. Example of user to group mapping using the GroupMemebrShip attribute from our example...

```

<map table="Users">
...
<variable>
<name>Groups</name>
<value><GroupMemberShip></value>
</variable>
...
</map>

```

5. Restart the **Kerio Connect** engine to apply changes.

6. You can download complete map file from Attachment section - [openldap.map](#).

Following steps maps our OpenLDAP group to **Kerio Connect** and we will add the test_user into this new group.

The OpenLDAP group has to be extended for **Kerio Connect** attributes as well as the OpenLDAP user. We can divide attributes to two groups. First group contains necessary attributes (objectClass definition), second one contains optional attributes. You can modify existing **group.ldif** file according to your needs or you can use an example **kerio-group.ldif** file as a reference one (it contains all required attributes). These modifications can be easily applied by executing following command on your OpenLDAP server:

```

linux:/etc/openldap # ldapmodify -f kerio_group.ldif -h 127.0.0.1 -x -D
"cn=Manager,dc=my-do
main,dc=com" -W
Enter LDAP Password:
modifying entry "cn=Group1,dc=my-domain,dc=com"
linux:/etc/openldap #

```

The **kerio_group.ldif** file example:

```

dn: cn=Group1,dc=my-domain,dc=com
cn: Group1
objectClass: top
objectClass: groupOfNames
objectClass: posixGroup
objectClass: kerio-Mail-Group
member: uid=test_user,dc=my-domain,dc=com
gidNumber: 100
memberUid: test_user

```

Necessary attributes/objectClasses	Description
objectClass: kerio-Mail-Group	This option will extend the user attributes set for the Kerio Connect ones. It allows to add optional attributes like the Message Quota, ... It does not activate the account, account needs to be activated using the optional kerio-Mail-Active attribute.

Optional Kerio Connect attributes	Description
kerio-Mail-Active	It activates the Kerio Connect group account. 0 - not active 1 - active
kerio-Mail-AdminRights	Admin rights.
kerio-Mail-Authorization	The directory where is stored the LDAP database
kerio-Mail-Address	Which attributes will be used for indexing

Examples minimal definition:

Example attribute sets	Description
objectClass: kerio-Mail-Group kerio-Mail-Active: 1	The user can have Kerio Connect account. The account is activated (can receive emails).

In this point we have created **Kerio Connect** group in OpenLDAP server. So we can adjust the map file to map the OpenLDAP group definition with **Kerio Connect**.

To create appropriate mapping follow these steps:

1. We used Apple Open Directory server mapping as a reference configuration. Hence we need to adjust the **apple.map** file which is used for this mapping. This file is located in **../installation_directory/ldapmap** folder. Locate this file and open it via some text editor.
2. Locate Group definition section at the bottom of this file. See this example from original **apple.map** file.

```
<map table="Group">
<filter>objectclass=apple-group</filter>
<active-attribute>kerio-Mail-Active</active-attribute>
<variable>
<name>Name</name>
<value><attribute>cn</attribute></value>
</variable>
<variable>
<name>MailAddress</name>
<value><attribute>kerio-Mail-Address</attribute></value>
</variable>
<variable>
<name>Rights</name>
<value><attribute>kerio-Mail-AdminRights</attribute></value>
</variable>
<variable>
<name>Authorization</name>
```

```

<value><attribute>kerio-Mail-Authorization</attribute></value>
</variable>
<variable>
<name>Description</name>
<value><attribute>apple-group-realname</attribute></value>
</variable>
</map>
</mapfile>

```

3. Change the group map file according to your group definition in OpenLDAP. We used three group objectClass definitions in our OpenLDAP group - `groupOfNames`, `posixGroup`, `kerio-MailGroup`. Choose one from this list and use it as a filter. So only OpenLDAP items with the specified objectClass will be searched as **Kerio Connect** groups. All other attributes are optional and may stay unchanged (instead of last one which use apple attribute, change it to some attribute describing your OpenLDAP group - in this example it is **description** attribute).

4. Example of group definitions...

```

<map table="Group">
<filter>objectclass=groupOfNames</filter>
<active-attribute>kerio-Mail-Active</active-attribute>
<variable>
<name>Name</name>
<value><attribute>cn</attribute></value>
</variable>
<variable>
<name>MailAddress</name>
<value><attribute>kerio-Mail-Address</attribute></value>
</variable>
<variable>
<name>Rights</name>
<value><attribute>kerio-Mail-AdminRights</attribute></value>
</variable>
<variable>
<name>Authorization</name>
<value><attribute>kerio-Mail-Authorization</attribute></value>
</variable>
<variable>
<name>Description</name>
<value><attribute>description</attribute></value>
</variable>
</map>

```

5. Restart the **Kerio Connect** engine to apply changes.

It would be possible to see OpenLDAP group in Kerio Connect's Administration console. Next chapter describes how you can add users into groups.

Adding users to groups

If all previous configuration steps were successfully passed, it should be possible to see users from the OpenLDAP database in Kerio Connect Administration console and it should be possible to see also groups defined in your OpenLDAP server in it. Following text describes how to add a user into a group using the OpenLDAP directory definitions.

As was described in Group mapping section OpenLDAP uses one direction of mapping of users. Because of this we have created new special attribute named `groupMemeberShip` which can be used by **Kerio Connect** to locate group to which user belongs. So adding a user to some group means adding this attribute to user definition in OpenLDAP server.

See following example how to add our `test_user` to a `Group1`. Exactly it means extending the user definition for `groupMemeberShip` attribute.

1. Edit the `kerio_user.ldif` file, or your custom user definition file.
2. Add attribute `groupMemeberShip` to definition file as is shown on following example or use the LDAP browser to extend the user definition for a new attribute `groupMemberShip`:

```
dn: uid=test_user,dc=my-domain,dc=com
uid: test_user
sn: User
cn: Test User
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: top
objectClass: kerio-Mail-User
loginShell: /bin/bash
homeDirectory: /home/testuser
uidNumber: 1001
gidNumber: 1001
groupMemberShip: Group1
```

3. Now the user belongs to a group named `Group1`.

Authentication

We set up the OpenLDAP account and the OpenLDAP group and we performed correct mapping. But the user still can't authenticate. This is because of the incorrect authentication type used for a user. The authentication type is set in the `apple.map` file. Default value is Kerberos authentication in Apple OpenDirectory.

1. The authentication type is set in the map file (**openldap.map**) and is set to 3 by default. See possible authentication methods:

- 0 - Internal database authentication
- 1 - NT domain authentication.
- 2 - LinuxPAM authentication method.

- 3 - Kerberos authentication. Requires Kerberos server.
- 4 - Apple Password Server authentication method.
- 5 - Authentication against LDAP server. It is used in this example.

NOTE

All methods are well described and this article is not related to authentication problem. However we will describe one authentication method which is not common and which is close to the OpenLDAP server. This authentication method (5 - Authentication against LDAP server) is simple authentication method, which tries to authenticate user to LDAP server. If it is successful the user is also authenticated in **Kerio Connect**.

2. This method send passwords in plain text format to the LDAP server so it is not secure to send it over the network. Hence it is highly recommended to have **Kerio Connect** on the same machine as your OpenLDAP server or in the same isolated network. The second disadvantage of this solution is that the user cannot change his password. We recommend to use different authentication method if it is possible hence it is more secure, and it may also supports password updates. If it is necessary to use this authentication type follow these instructions to enable it.

3. Stop **Kerio Connect** engine.

4. Modify the **openldap.map** file according to following example:

```
<variable>
<name>Auth_type</name>
<value>5</value>
</variable>
```

5. Modify or add additional map attribute (in **openldap.map** file in user definition section) according to the following example:

```
<variable>
<name>LdapDN</name>
<value><dn /></value>
</variable>
```

6. Start **Kerio Connect** engine. Now you should be able to authenticate against the OpenLDAP server.

NOTE

Notice that a new user created in OpenLDAP does not have a password. To create password for the OpenLDAP user use following command:

```
linux:/etc/openldap # ldappasswd -S -D "cn=Manager,dc=my-domain,dc=com" -h
127.0.0.1 -x -W "
uid=test_user,dc=my-domain,dc=com"
New password:
Re-enter new password:
Enter LDAP Password:
Result: Success (0)
linux:/etc/openldap #
```

Attachments:

- » mailserver.cfg
- » kerio-mailserver.schema
- » openldap.map
- » slapd.conf
- » user.ldif
- » group.ldif
- » schema2.png
- » kerio_user.ldif
- » kerio_group.ldif

4.5.12 What ports should be open on my Active Directory controller for synchronization with Kerio Connect/MailServer?

Kerio Connect/MailServer needs to access the following services to communicate properly with Active Directory:

- » LDAP - by default TCP port 389
- » kerberos-sec - by default TCP/UDP port 88
- » kpassword5 - by default TCP/UDP port 464

4.5.13 Accessing LDAP with LinkSys SPA942

To access the LDAP contacts on my Kerio MailServer from my LinkSys SPA942 desktop phone.

This phone has a web interface that you can use to adjust the LDAP settings in order to access the Public contacts.

The following settings will allow you to access the Public Contacts using the Directory option from the phone.

LDAP Dir Enable: YES

LDAP Corp Dir Name: The name you wish to appear on your phones Directory e.g. Global Contacts

LDAP Server: IPaddress or Domain Name of Kerio MailServer

LDAP Auth Method: SIMPLE

LDAP Client DN: valid Kerio username e.g. administrator

LDAP Username: valid Kerio username e.g. administrator

LDAP Password: password of the specified account

LDAP Search Base: fn=ContactRoot

LDAP Last Name Filter: sn:(sn=*\$VALUE*)

LDAP First Name Filter: cn:(cn=*\$VALUE*)

LDAP Display Attrs: a=cn;a=sn;a=mobile;n=Mobile;t=p;a=telephoneNumber;n=Phone;t=p;

4.6 Security

This section helps you secure your Kerio Connect server.

4.6.1 Securing Kerio Connect	324
4.6.2 Configuring anti-spoofing in Kerio Connect	328
4.6.3 Password policy in Kerio Connect	329
4.6.4 Authenticating messages with DKIM	332
4.6.5 Configuring DNS for DKIM	334
4.6.6 Configuring SSL/TLS in Kerio Connect	338
4.6.7 PCI DSS Compliance	341
4.6.8 Antispam	342
4.6.9 Antivirus	369
4.6.10 SSL certificates	377

4.6.1 Securing Kerio Connect

You can secure your Kerio Connect by:

- » [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](#)
- » [Encrypting data](#)

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

Service (default port)	Incoming connection
LDAP (389)	deny
LDAPS (636)	allow
HTTP (80, 4040, 8800)	deny
HTTPS (443, 4040, 8843)	allow

Password policy

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

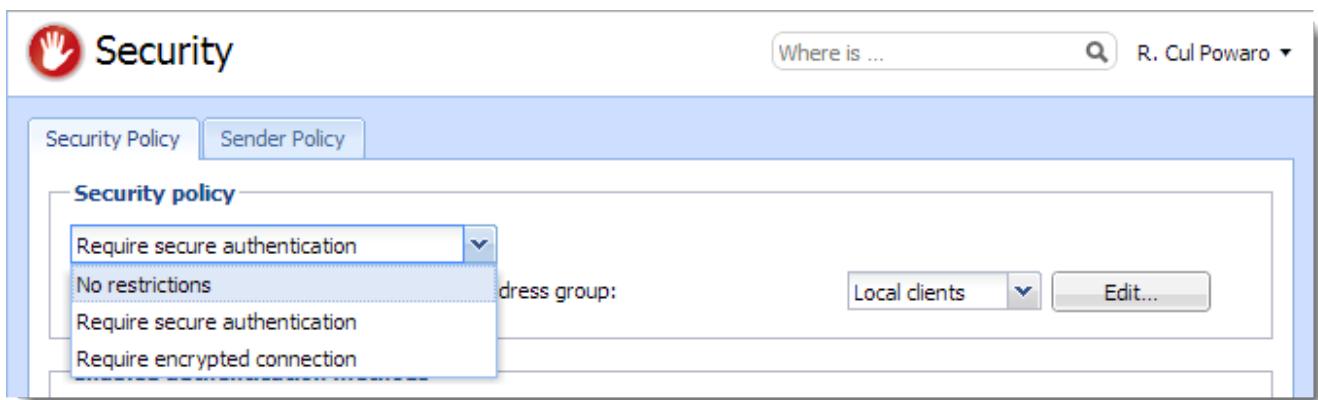
Configuring a secure connection to Kerio Connect

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).

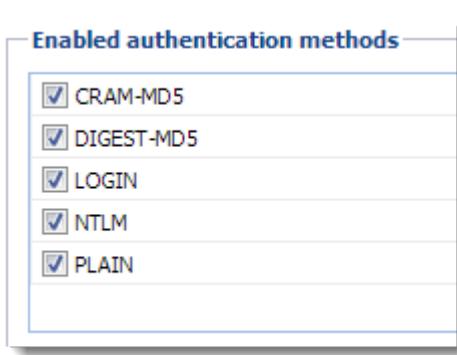


Securing user authentication

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.

NOTE

If users' passwords are saved in the SHA format:

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

Data Encryption

NOTE

- » This feature is only available for users running Kerio Connect v9.2.7 and above on Linux.
- » Data Encryption is not supported on external or removable disks and, on multi-volume data storage.
- » The initial encryption and decryption process takes considerable amount of time to complete based on the size of the email data. It is recommended to not interrupt the process as this will result in a corrupted email store. Email delivery is also unavailable during this time.

Enabling Encryption

You can configure Kerio Connect to encrypt user settings, logs, system configuration, and messages saved to the disk.

IMPORTANT

Encryption is bound to a specific storage device, so if you plan to change the hardware you must first disable encryption. Also, encryption results in more resources being utilized so performance maybe impacted.

1. In the Kerio Connect administration interface, go to **Configuration > Advanced Options > Store Directory**.
2. Go to the **Data Encryption** section.

Data Encryption

Enable Encryption to ensure that Kerio Connect will encrypt all data prior writing it to the disk. Please note that encryption results in more resources being utilized and hence performance could be affected. Encryption also locks the data to this particular device, hence change to the device hardware could result in the data being inaccessible.

Disabled. Data encryption is disabled.

Password:

Confirm password:

Enable

Screenshot 19: The data encryption tab

3. Key-in the **Password** and re-enter to confirm the same.

IMPORTANT

Once encryption is enabled, the password cannot be changed. Remember this password, as you would require it to decrypt data.

4. Click **Encrypt** and confirm the action.

Disabling Encryption

To decrypt: data and disable encryption:

1. In the Kerio Connect administration interface, go to **Configuration > Advanced Options > Store Directory**.
2. Go to the **Data Encryption** section.

Data Encryption

Enable Encryption to ensure that Kerio Connect will encrypt all data prior writing it to the disk. Please note that encryption results in more resources being utilized and hence performance could be affected. Encryption also locks the data to this particular device, hence change to the device hardware could result in the data being inaccessible.

Enabled. Data is encrypted.

Disable

Screenshot 20: The data encryption tab

3. Click **Decrypt**.
4. Key-in the **Password** set while encrypting and confirm the action.

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](#).

NOTE

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

4.6.2 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.

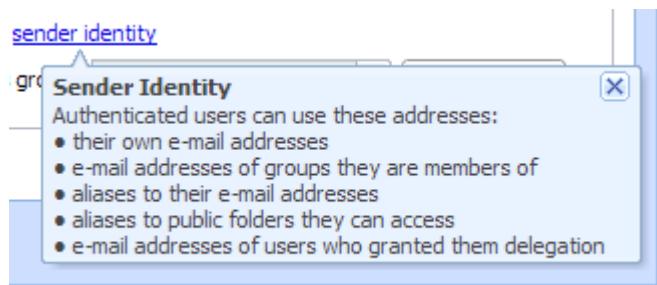
First, configure anti-spoofing for your server. Then, enable anti-spoofing for each domain.

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**.

NOTE

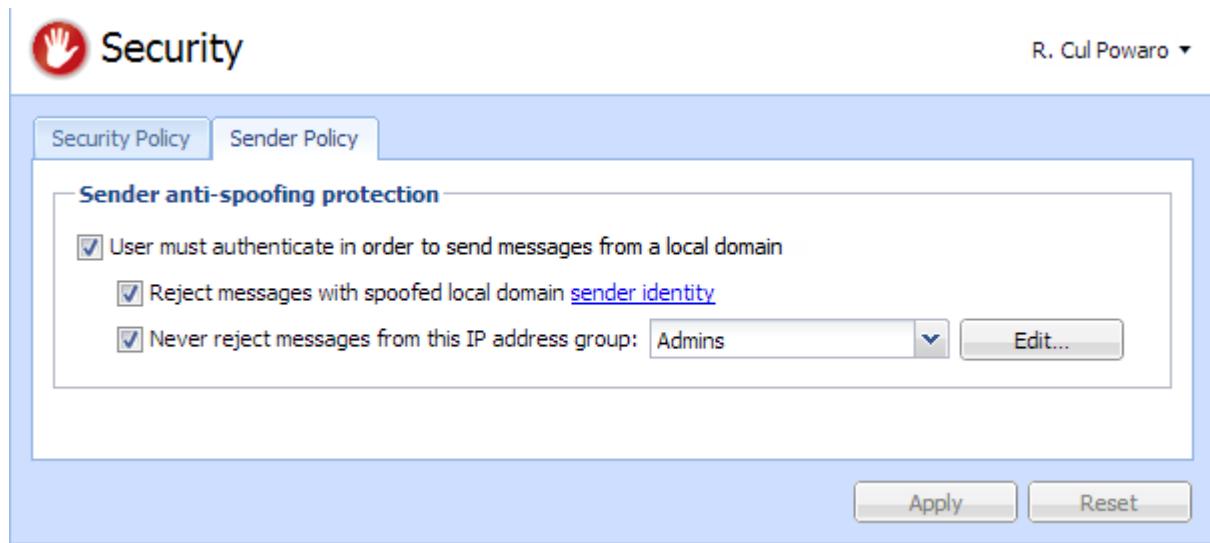
See the [Security log](#) for information about the rejected messages.

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.

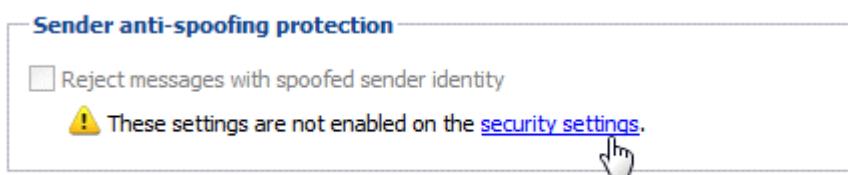
6. Click **Apply**.



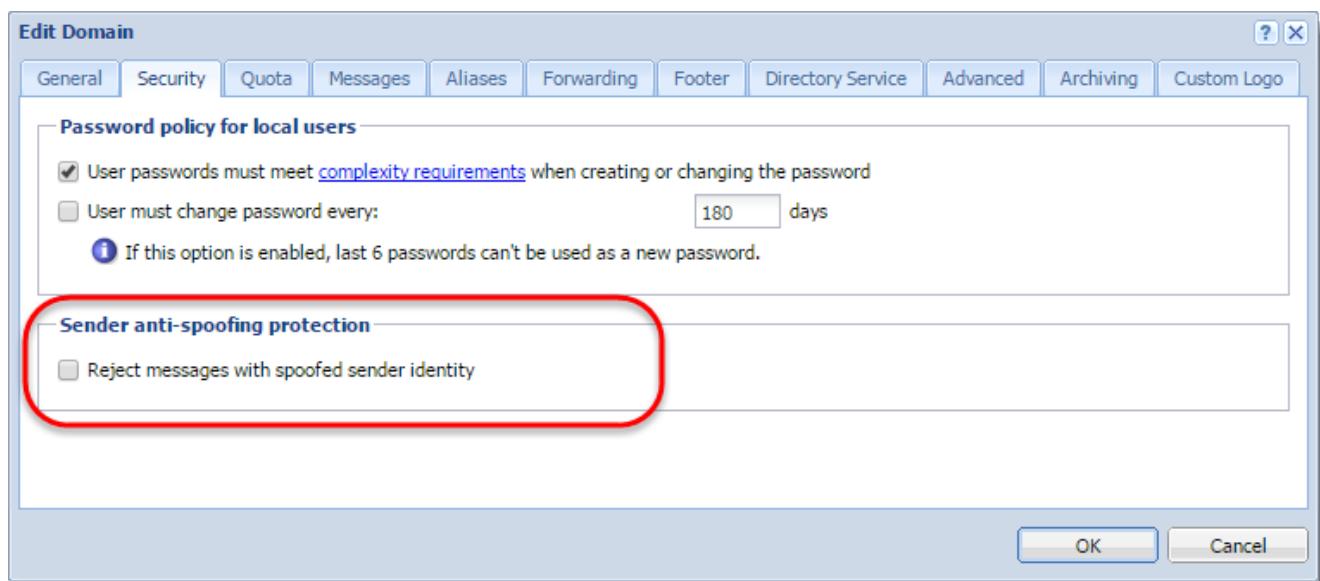
For more information about other security features in Kerio Connect, read [Securing Kerio Connect](#).

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.



4. Click **OK**



4.6.3 Password policy in Kerio Connect

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:

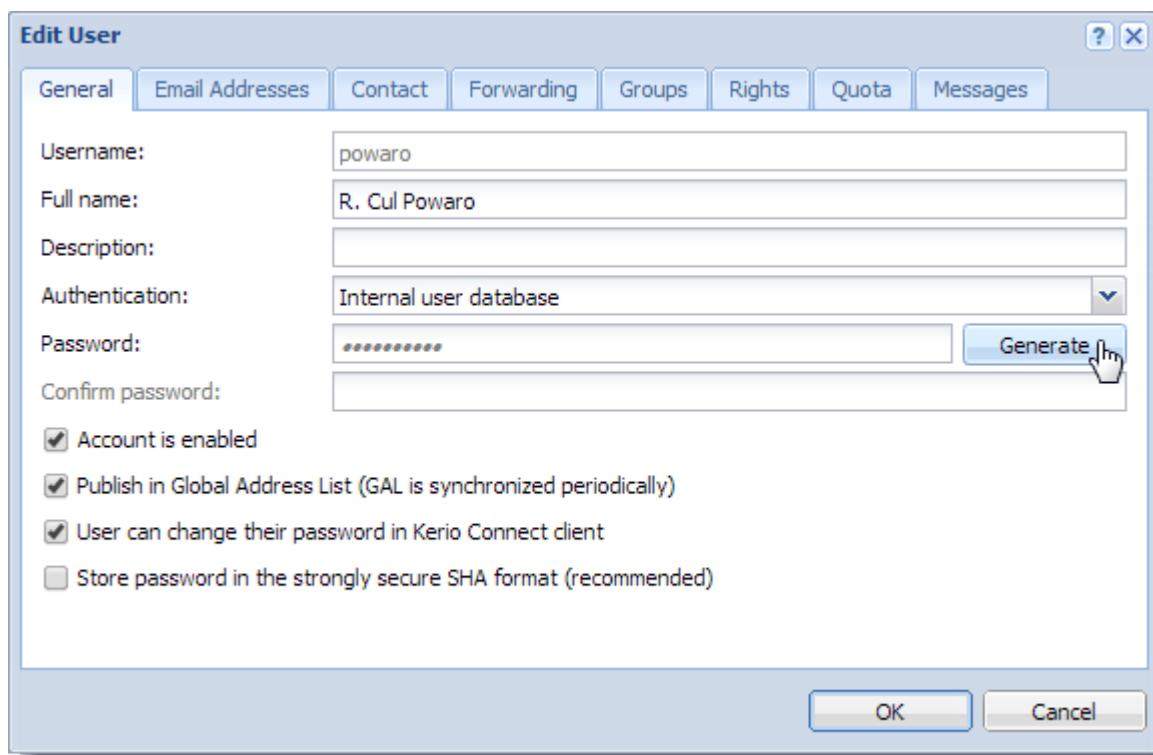
- Lowercase letters
- Uppercase letters
- Numbers
- Special characters

Users should change their password often.

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**.



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.

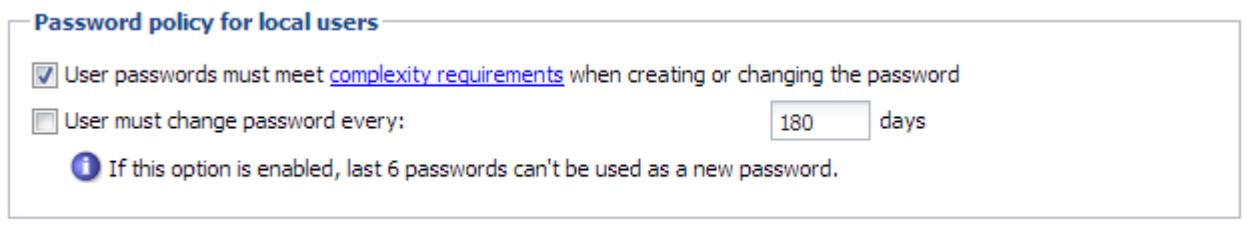
Complex password:

- » 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.

NOTE

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**

NOTE

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).

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

Protecting against password guessing attacks

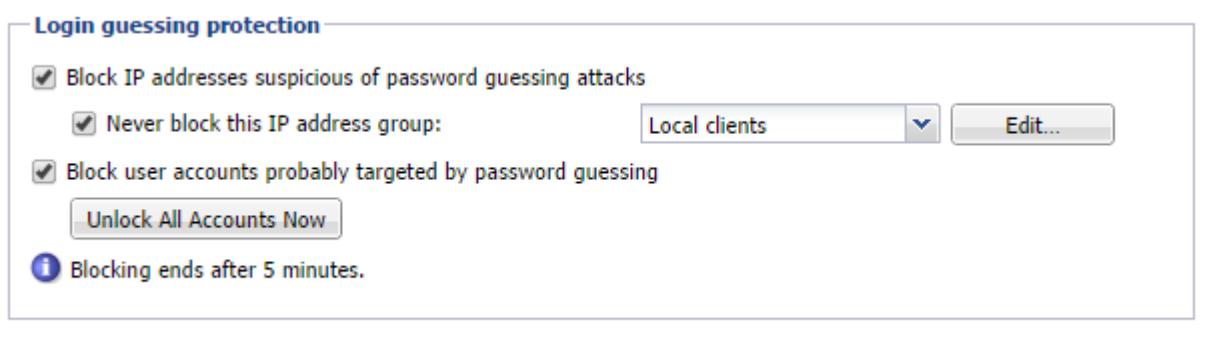
Kerio Connect can block IP addresses suspicious of password guessing attacks (ten unsuccessful attempts in one minute).

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

NOTE

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](#).

4.6.4 Authenticating messages with 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.

Edit Domain

General	Security	Quota	Messages	Aliases	Forwarding	Footer	Directory Service	Advanced	Archiving	Custom Logo
Domain: feelmorelaw.com Rename										
Description: Feel More Law Inc.										
User count										
Number of users in the domain: 10										
<input checked="" type="checkbox"/> Limit maximum number of users in the domain: <input type="text" value="50"/>										
DomainKeys Identified Mail (DKIM)										
<input checked="" type="checkbox"/> Sign outgoing messages from this domain with DKIM signature. Learn more...										
! DKIM public key for feelmorelaw.com is wrong. <input type="button" value="Show public key..."/>										
Chat										
<input checked="" type="checkbox"/> Enable chat in Kerio Connect Client.										
<input type="button" value="OK"/> <input type="button" value="Cancel"/>										

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

@ Domains

Internet hostname: mail.feelmorelaw.com

Name	Description	Aliases	Forward to Host	Quota	DKIM enabled
@ feelmorelaw.com (primary)	Feel More Law Inc.			41 %	Yes
@ company.com	Domain of other company	company.cz	mail1.company.com	12 %	No
@ dedukce.cz					Yes
@ feelmorelaw.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).

For more information, refer to [Configuring DNS for DKIM](#) (page 334).

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.

4.6.5 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), for example: mail._domainkey.feelmorelaw.com.
- » **TXT value**, forexample: v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDf10chtL4siFYCrSPxw43fqc4z
Oo3N+I1220oK2Cp+NzW9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn
AB3DGAQ6+/7UVXF9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb bcBh-
thrnETKoCg8wOwIDAQAB

NOTE

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).

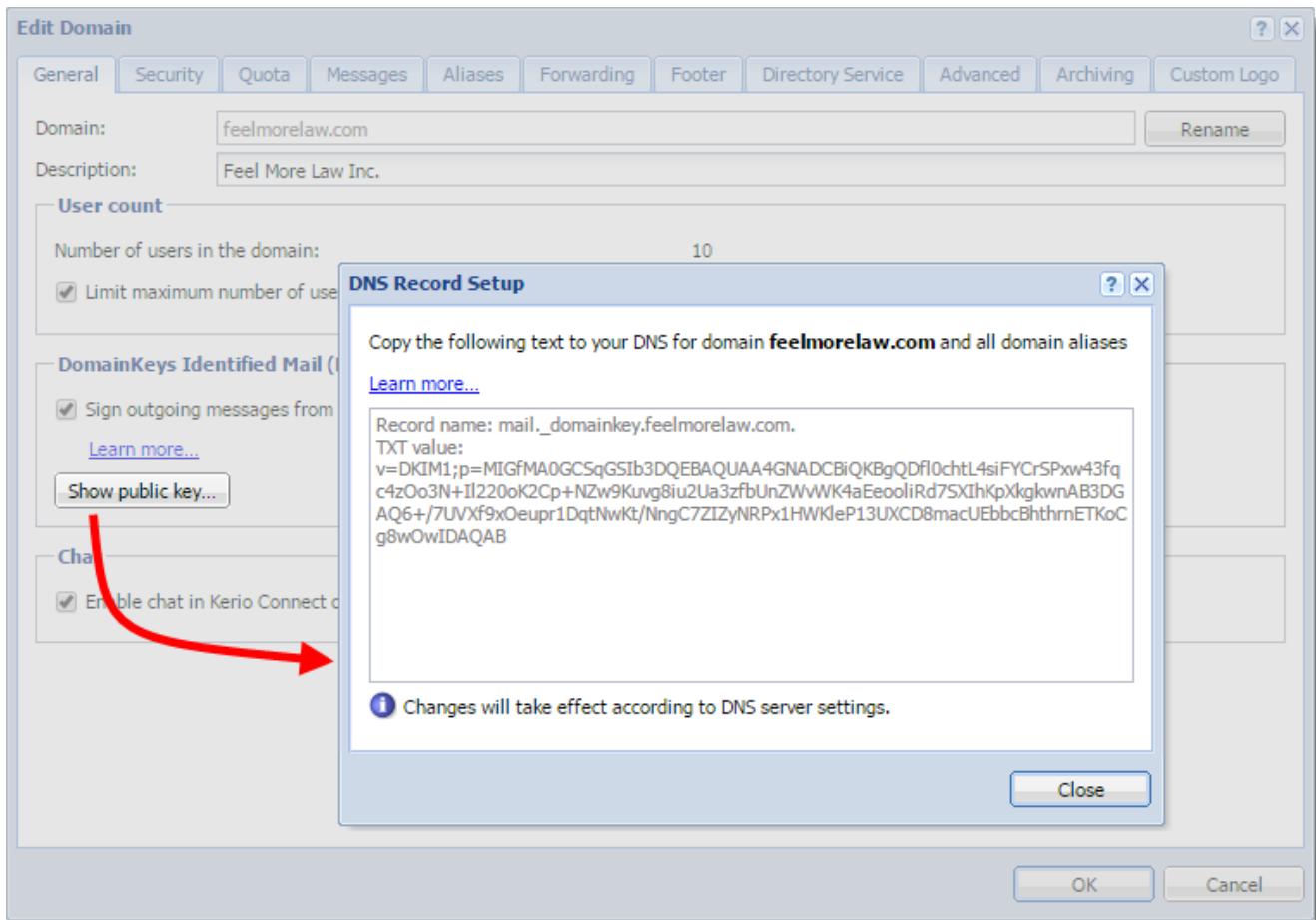
The DKIM public key in Kerio Connect is 2048-bit. Some providers may restrict the length of the key (the TXT value) — read section [Creating a short DKIM public key](#) to get detailed information.

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



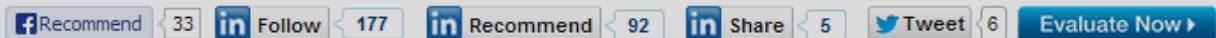
Creating a short DKIM public key

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



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

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

feelmorelaw.com	Domain name of the "From:" header address, not the SMTP "MAIL FROM". (e.g., port25.com)
mail	DomainKey Selector (e.g., key1)
<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.

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

CREATE KEYS

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

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDpnmlWPJXpRmTT2PL4AxYgp0cz
D0ojoWP8qn1XMLCW/FdmjnkuWwehRqH6ubFh7exI1xn4iXay8Qtv213e3m5yZPn
w7LYodRJBe5hPoP5PHMVe3BlfcyrUzJmXb3rb99d5UMXANhAJTu0tLM9JILN0s+i
kn3QM1IUmAyRCg2XAwIDAQAB
```

-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----

```
MIICWwIBAAKBgQDpnmlWPJXpRmTT2PL4AxYgp0czD0ojoWP8qn1XMLCW/Fdmjn
uWwehRqH6ubFh7exI1xn4iXay8Qtv213e3m5yZPnw7LYodRJBe5hPoP5PHMVe3Bl
fcyrUzJmXb3rb99d5UMXANhAJTu0tLM9JILN0s+ikn3QM1IUmAyRCg2XAwIDAQAB
AoGAU9LTiP0GISRz6xtt2pVo7B+fiU/8HxKF5+d/FGAbNZe93AMJgMsTQ0QpB9m+
IeQXggSZFGETifsREgUcpwFz5AkCpJG/RlgJuRJVNi+sM9qMXtW3MoOBHHFUNIaZ
rL9JsJ0gaoNWlp7rpN0iOhanMx3o4uF00w5ZbpkzP0pM7zkCQQD8nFLUV603KmXM
REUEAdnBdfMSFsnrO4PfMK5i8NDEXb/vsUBXeXqtwOu3nqvD0KmatYcM7+RIPzN8
izbR11jNAkEA7MDTSNhQNY38f0mUffomkSO6W/Huk/5lpswUNR1/XBz6EbBYs2
DyvGp96RTYV0R0y7mN7cJqA+XdX372jvDwJAM9urrWfqaV7M0yhYwBZFK7q/YcFH
5oCrS9BknG8vjIBqfLx4pvYlUMxAF8v9Gw/lIZu0g/tjc/7PNQwnTtOxKQJAQBm1
Gtpk8nkFIxGwWA/trLtmBGBL7sKYWnYBHBjt9QbFAsJL3qRibpkboDfSF3qykNt1
r24njQ211RIpnth6YQJAE5+LE13rwPoFdG8Z9zXIly8iTclLQglFms8uNT8zldci
F58+8n3Gj+v8XPXvT8e95I8vDuyBIjocwhPrucAIQQ==
```

-----END RSA PRIVATE KEY-----

Adding a new private key to Kerio Connect

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

NOTE

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 domain's configuration. You can now create the DNS DKIM record with the new public key.

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

BIND DNS server

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

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

Example:

```
TXT ("v=DKIM1;"  
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFl0chtL4siFYCrSPxw43fqc4z"  
"Oo3N+I1220oK2Cp+NZw9Kuvg8iu2Ua3zfbUnZWvWK4aEeooliRd7SXIhKpXkgkwn"  
"AB3DGAQ6+/7UVXf9xOeupr1DqtNwKt/NngC7ZIZyNRPx1HWKleP13UXCD8macUEb"  
"bcBhthrnETKoCg8wOwIDAQAB")
```

4.6.6 Configuring SSL/TLS in Kerio Connect

NOTE

New in Kerio Connect 8.5!

Kerio Connect allows you to enable or disable specific security protocols and cipher sets 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. For more information, refer to [Configuration files](#) (page 15).
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. For more information, refer to [Configuration files](#) (page 15).
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 ciphers

It is recommended to use only strong ciphers suites to ensure compliance with various compliance standards.

Here is a list of strong ciphers available:

Strong ciphers (Recommended)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

Here is a list of weak ciphers. These ciphers are not recommended for compliance:

Weak Ciphers
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

List of variables

Kerio Connect uses eight variables for the SSL/TLS protocols configuration.

AllowEphemeralDH

NOTE

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).

NOTE

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

NOTE

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.

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.

SSL Dont Insert Empty Fragments

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 cipher set to use regardless of the client preferences.

4.6.7 PCI DSS Compliance

Payment Card Industry Data Security Standard (PCI DSS) is a proprietary security standard required by some banks in order to allow the company to process and store data about credit cards and payments.

To be in compliance with PCI DSS, some 3rd party security companies can verify the compliance. Usually, they run Nessus scanner and report any potential vulnerabilities or insecure issues.

The administrator can configure Kerio Connect to use supported cipher suits to ensure PCI DSS compliance. For more information, refer to [Configuring SSL/TLS in Kerio Connect](#) (page 338).

Kerio Connect and PCI

NOTE

Always upgrade to the latest version of Kerio Connect for the best security!

If you run Kerio Connect and have difficulties to be granted the compliance, try the following:

The list of known incompatibilities

Vulnerability to the TLS CBC attack

Solution: In Kerio Connect 8.0.0 and newer, set the `SSL Dont Insert Empty Fragments` configuration value to 0 in the `mailserver.cfg` configuration file. Users with Kerio Outlook Connector (Offline edition) 8.0.2 and older on Windows XP systems may not be able to connect to the server or synchronize the data.

Vulnerability to the SSL BEAST attack

Solution: In Kerio Connect 8.0.1 to 8.4.2, set the `DisableRC4SHA` configuration value to 0 in the `mailserver.cfg` configuration file.

RC4 cipher may be considered by some other security scans as insecure due to the known attack vectors to this algorithm. Some US government organizations and agencies must follow FIPS-140-2 standard, which forbids RC4 ciphers.

In Kerio Connect version 8.3.0 to 8.4.0, set also the `PREFERECDHCIPHER` configuration value to 0 in the `mailserver.cfg` configuration file.

Vulnerability to the POODLE and CVE-3566 attack

Solution: In Kerio Connect 8.3.3 and older, set the `DISABLESSLV3` configuration value to 1 in the `mailserver.cfg` configuration file.

SSLv3 is also disabled if `DISABLETLSV1` is set to 1.

Kerio Connect 8.3.4 and newer is not vulnerable to POODLE and CVE-3566.

IMPORTANT

If you disable TLSv1, some SMTP servers may not be able to deliver messages to your server.

How to test SSL vulnerabilities

To test SSL vulnerabilities, use an online test, for example, at <https://www.ssllabs.com/ssltest/>

4.6.8 Antispam

This section helps you protect your Kerio Connect server against spam.

- » [Configuring the anti-spam filter](#)
- » [Kerio Anti-spam filter](#)
- » [Configuring greylisting](#)
- » [Blocking messages from certain servers](#)
- » [Creating custom rules for spam control in Kerio Connect](#)
- » [Configuring Caller ID and SPF in Kerio Connect](#)
- » [Creating an SPF or Caller ID record](#)
- » [Bayesian self-learning in Kerio Connect](#)
- » [Optimizing the anti-spam filter](#)
- » [How do I exclude an email address from a blacklist?](#)
- » [How to reset the Spam Assassin plugin and Bayes database](#)
- » [How do I configure my Anti-Spam gateway to automatically gather valid addresses from Kerio Connect?](#)

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, refer to [Kerio Anti-spam filter](#) (page 345).

NOTE

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 more information, refer to [Blocking messages from certain servers](#) (page 351).
- » **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 more information, refer to [Configuring Caller ID and SPF in Kerio Connect](#) (page 357).
- » **Greylisting** — The greylisting method delivers only messages from known senders. For more information, refer to [Configuring greylisting](#) (page 349).
- » **Delayed response to SMTP greeting (Spam Repellent)** — You can set a delayed SMTP greeting that prevents delivery of messages sent from spam servers.

NOTE

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](#)

NOTE

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 message reaches the block score, Kerio Connect discards the message.

NOTE

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.

 **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:

Block score:

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

Reached Tag score limit action

Prefix the message's Subject with the text:

Reached Block score limit action

Send bounce message to sender

Forward the message to the quarantine address:

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

NOTE

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](#)

Kerio Anti-spam filter

NOTE

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.

NOTE

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

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.

NOTE

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

NOTE

Changed in Kerio Connect 9.2!

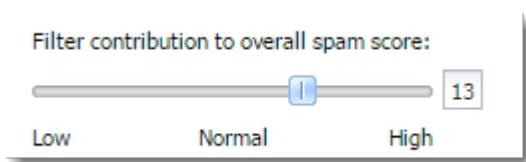
Kerio Connect calculates the Kerio Anti-spam score using a special algorithm and adds the score to the overall [spam rating](#).

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.



NOTE

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

NOTE

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.

NOTE

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**.

NOTE

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.

Kerio Anti-spam configuration

Enable Kerio Anti-spam advanced filter
Anti-spam advanced filter creates a secure connection to [Bitdefender's online scanning service](#) to analyse email content.

Filter contribution to overall spam score:
[Slider] 13
Low Normal High

Allow signatures and metadata to be utilized for enhancing the online scanning service

Apache SpamAssassin configuration

Use spam learning Bayesian filter
 Check every incoming message in Spam URI Realtime Blocklist (SURBL) database

Bayesian filter statistics

Filter status: Disabled

Messages learned as spam: -

Messages learned as not spam: -

Apply **Reset**

NOTE

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

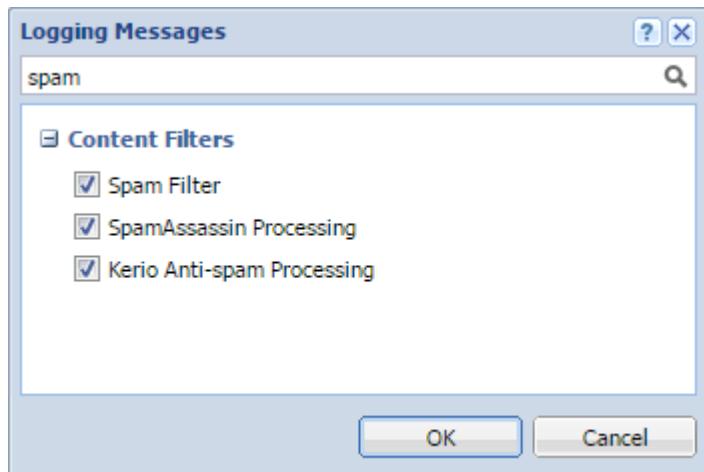
If you are upgrading from a previous version, restart Kerio Connect after you enable Kerio Anti-spam.

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.

NOTE

After debugging, clear those options. Otherwise, the logging may slow down server performance.



Configuring greylisting

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).

NOTE

To learn more about greylisting, consult greylisting.org.

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.

NOTE

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.

NOTE

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.

NOTE

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

5. Click **Apply**.

The screenshot shows the 'Spam Filter' interface with the 'Greylisting' tab selected. The top navigation bar includes links for 'Spam Rating', 'Blacklists', 'Custom Rules', 'SpamAssassin', 'Caller ID', 'SPF', 'Greylisting' (which is active), and 'Spam Repellent'. A user icon for 'Shimon Ski' is in the top right. The main content area has a header 'Greylisting configuration' with a note about its purpose: 'Greylisting limits amount of received spam by temporarily blocking emails sent by unknown senders or IP addresses.' Below this is a privacy note: 'Privacy note: When greylisting is enabled, IP address of each host delivering an email is presented to the Kerio Greylisting Service over a secure channel.' A link 'Learn more...' is provided. A section titled 'Greylisting configuration' contains several settings: a checked checkbox for 'Check incoming messages by Kerio Greylisting Service', an unchecked checkbox for 'Do not apply greylisting on connections from:' followed by a dropdown menu set to 'Admins' with a 'Edit...' button, and a note that 'IP addresses reserved for private networks are whitelisted by default.' A 'Test Connection' button is also present. Another section titled 'Greylisting statistics' displays two metrics: 'Messages accepted by greylisting: 0' and 'Messages temporarily rejected: 0'. At the bottom are 'Apply' and 'Reset' buttons.

Screenshot 21: 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 do 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

The screenshot shows the 'Spam Filter' configuration interface. At the top, there are tabs for 'Spam Rating', 'Blacklists', 'Custom Rules', 'SpamAssassin', 'Caller ID', 'SPF', 'Greylisting', and 'Spam Repellent'. The 'Blacklists' tab is selected.

Custom whitelist of IP addresses:

- Use IP address group:
- Info:** All IP addresses reserved for private networks are always included in this whitelist by default.

Custom blacklist of spammer IP addresses:

- Use IP address group:
- Block the message
- Add spam score to the message:

Internet blacklists:

<input type="checkbox"/>	Name	DNS Suffix	Action	Ask Directly
<input checked="" type="checkbox"/>	SpamCop	bl.spamcop.net	Block	No
<input checked="" type="checkbox"/>	SpamHaus SBL-XBL	zen.spamhaus.org	Block	Yes
<input checked="" type="checkbox"/>	SORBS DNSBL	dnsbl.sorbs.net	Block	No
<input checked="" type="checkbox"/>	SORBS RHSBL	rhsbl.sorbs.net	Block	No
<input checked="" type="checkbox"/>	WPBL - Weighted Private Block List	db.wpbl.info	Increase score by 1.4	No

Screenshot 22: Blacklists tab

Blocking messages from spam servers — Custom blacklists

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

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

6. Click **Apply** in the bottom right corner.

Blocking messages from spam servers — Public databases

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

To use blacklists from **public databases**:

1. Go to section **Configuration > Content Filter > Spam Filter > Blacklists**.
2. In the **Internet blacklists** section, select all the public databases you want to use.
3. Double-click a blacklist and select the option corresponding to the action you want performed when messages arrive that meet the blacklist's criteria:

- Block the messages (this marks them as spam)
- Add [spam score](#) to the message

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

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

1. In the same section, click **Add**.
2. Type the DNS name of the server that handles the of Kerio Connect enquires.
3. Select the option corresponding to the action you want performed when messages arrive that meet the blacklist's criteria:
 - Block the messages (this marks them as spam)
 - Add [spam score](#) to the message
4. Click **Apply** in the bottom right corner.

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

NOTE

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.

Creating custom rules for spam control in Kerio Connect

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**.

The screenshot shows the 'Spam Filter' configuration page. The 'Custom Rules' tab is selected. A table lists four custom rules:

Item	Type	Content	Action	Description	Last Used Before
Mail body	Substring	cialis	Increase score by 9.0	cialis	83 days, 22 hours, 2 minutes
From	Address	someone@wanted.com	Allow	Wanted sender	Unused
From	Domain	spammer.cz	Reject	Denied domain	Unused
Subject	Empty		Increase score by 4.0	Empty subject messages	10 days, 21 hours, 18 minutes

Below the table are buttons: 'Add...', 'Edit...', 'Remove', and 'Remove Unused...'. A 'Search:' input field is also present. To the right of the table are up and down arrow buttons for reordering rules.

Reject messages as soon as possible (during communication through the SMTP protocol)

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:

Info If option "Reject messages as soon as possible" is enabled, some messages cannot be forwarded to quarantine.

Buttons at the bottom: 'Apply' and 'Reset'

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**

NOTE

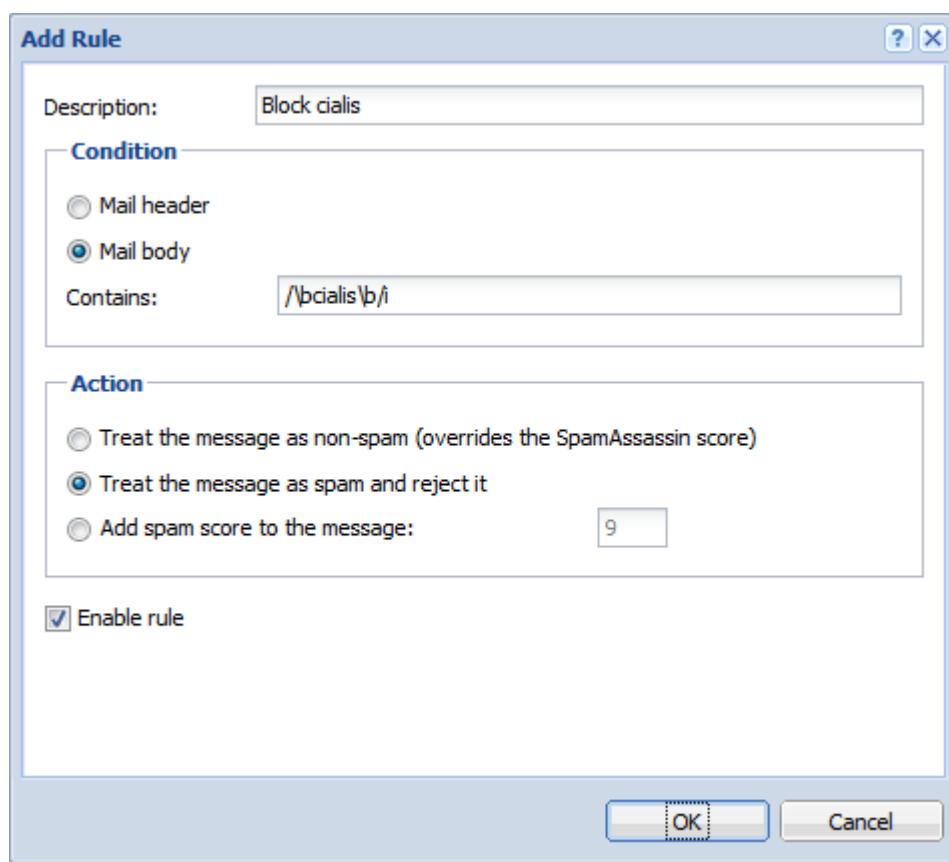
To decrease the load on your server, place the From and To header rules at the top. If Kerio Connect rejects messages using this rule, no other antispam or antivirus tests are performed on these messages.

Example for regular expressions

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

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

1. In **Configuration > Content Filter > Spam Filter > Custom rules**, click **Add**.
2. Select **Mail body** and type the following regular expression: `/\bcialis\b/i`
3. Select **Treat the message as spam and reject it**.
4. Click **OK**

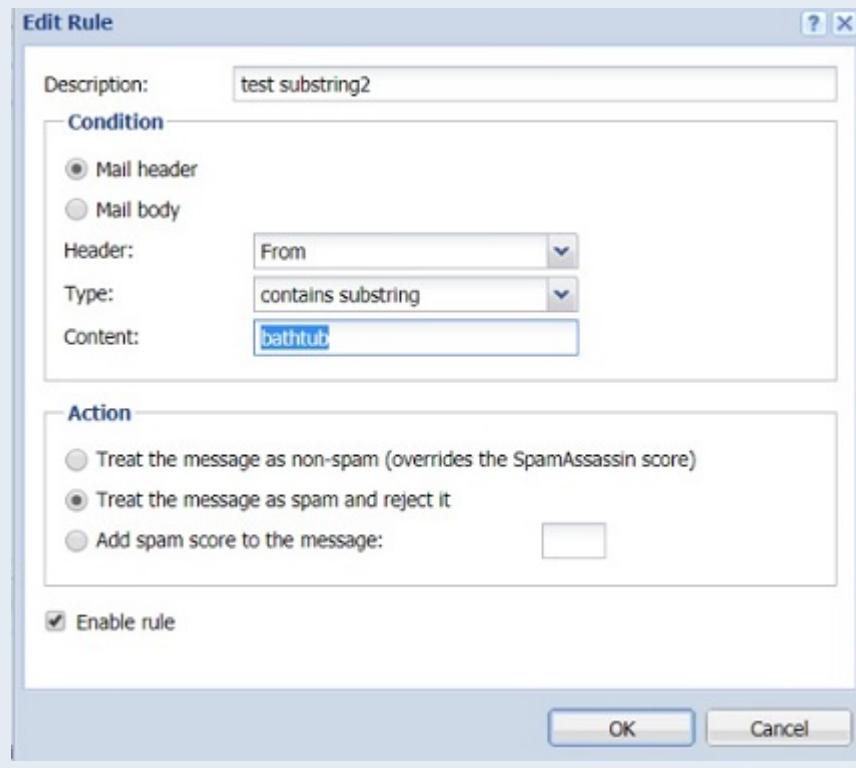
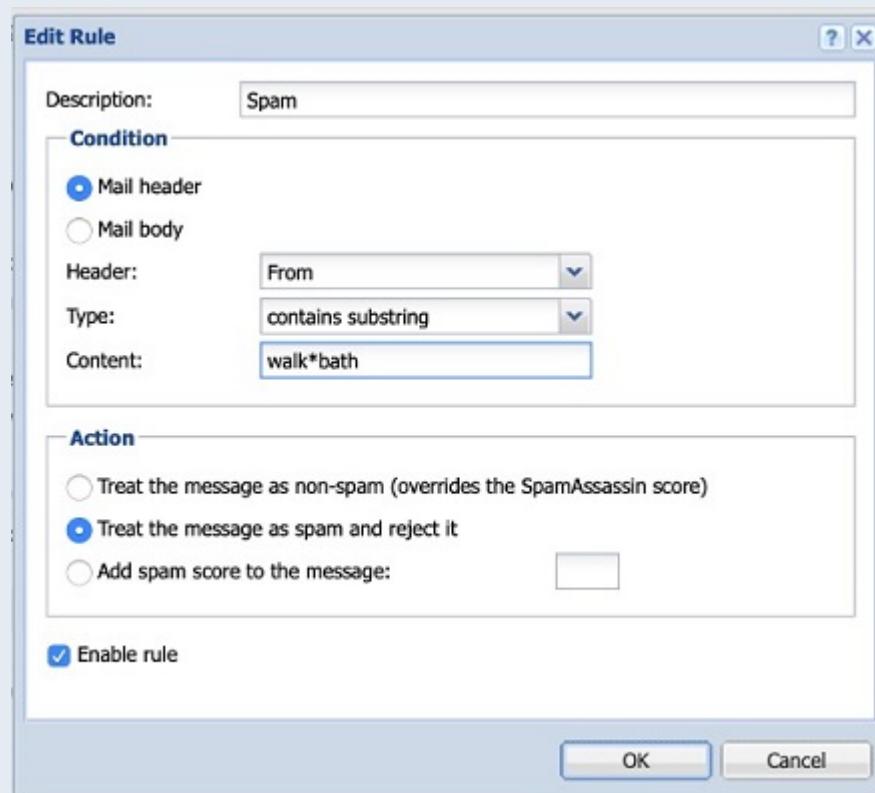


From now on, Kerio Connect rejects all messages that include `cialis` as a single word.

For detailed information on regular expressions, see the [SpamAssassin wiki page](#).

NOTE

Regular expressions combined with * and ? wildcards do not work with **contains substring** (see the screenshot below).



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 options 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:

spam@feelmorelaw.com

i If option "Reject messages as soon as possible" is enabled, some messages cannot be forwarded to quarantine.

NOTE

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.

Configuring Caller ID and SPF in Kerio Connect

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.

IMPORTANT

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.

NOTE

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](#).

The screenshot shows the 'Spam Filter' configuration page in the Kerio Connect admin interface. The 'SPF' tab is active. In the 'Invalid Caller ID action' section, the radio button for 'Log this to the Security log only' is selected. In the 'Other settings' section, two checkboxes are checked: 'Apply this policy also to the testing Caller ID records' and 'Don't check Caller ID from the IP address group:', with 'Admins' selected from a dropdown menu. At the bottom are 'Apply' and 'Reset' buttons.

Screenshot 23: 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.

The screenshot shows the 'Spam Filter' interface in Kerio Connect. The top navigation bar includes links for 'Spam Rating', 'Kerio Anti-spam', 'Blacklists', 'Custom Rules', 'Caller ID', 'SPF', 'Greylisting', and 'Spam Repellent'. The 'SPF' tab is active. A search bar at the top right contains the placeholder 'Where is ...' and a user dropdown showing 'R. Cul Powaro'. Below the tabs, there are two status messages: a checked checkbox for 'Enable SPF check of every incoming message' and an info icon for 'Messages sent from trustworthy relay agents defined in the SMTP relay options are not checked.' Under the 'Negative SPF result action' section, three radio buttons are available: 'Log this to the Security log only' (selected), 'Block the message', and 'Add spam score to the message:' followed by a numeric input field set to '0'. In the 'Other settings' section, a checked checkbox for 'Don't check SPF from the IP address group:' is paired with a dropdown menu set to 'Local clients' and a 'Edit...' button. At the bottom right are 'Apply' and 'Reset' buttons.

Screenshot 24: SPF

Creating an SPF or Caller ID record

You may be receiving spam where the sender information is specified as your domain. In this case, the recommended solution would be to add both an SPF and Caller ID record for your email domain. This will ensure that spammers may not spoof your email domain when sending email to your Kerio Connect. It will also prevent spoofing of your domain for messages sent to other email servers that perform lookups against SPF or Caller ID records.

This example uses the domain "radiusadvertising.com" as an example. The outgoing Kerio Connect for this domain is mail.radiusadvertising.com, which resolves to 63.194.168.220. We want that any email containing 'radiusadvertising.com' in the 'From' header and SMTP envelope should be refused, unless it was sent from 63.194.168.220.

This will require a special DNS configuration called a TXT record. Note that many DNS hosting providers may not support configuration of such records. If you do not host your own DNS, you will need to contact your DNS hosting provider (usually the domain registrar) to find out if they will support configuration of TXT type DNS records. We will use Network Solutions in this example, as they support both SPF and Caller ID type TXT records.

Given an outgoing IP of 63.194.168.220, our SPF and Caller ID records would be created exactly this way:

SPF

```
"v=spf1 mx ip4:63.194.168.220 -all"
```

Caller ID:

```
"<ep xmlns='http://ms.net/1'><out><m> <r>63.194.168.220</r> </m></out></ep>"
```

Note that when configuring the Caller ID record, you must create a special host entry of _ep.yourdomain.com (see the screenshot below).

For your email domain, you may simply replace the IP address from this example, with the outgoing IP address of your Kerio Connect.

In case you have multiple outgoing email servers for your domain, you can add them like this:

NOTE

SPF: ip4:63.194.168.220 ip4:63.194.168.221 ip4:63.194.168.222
Caller ID:<r>63.194.168.220</r> <r>63.194.168.221</r> <r>63.194.168.222</r>

You may verify your records using the following commands:

```
dig txt _ep.radiusadvertising.com +short
```

```
dig txt radiusadvertising.com +short
```

Or you can use the SPF checker located [here](#).

The following images are taken from the DNS editor of Network Solutions

Add/Edit Text(TXT Records) - Currently Managing Domain : radiusadvertising.com.

Warning: Some character sequences will cause your TXT record to be invalid. When entering values for TXT records:

- You do not need to enter double quote(s) at the beginning and end of the TXT record.
- If you need double quotes ("") in the middle of a record, escape them with a single backslash (ie: \").
- No other characters need to be escaped.

[Click here for complete rules and examples](#)

SPF (Sender Policy Framework) records can be entered as TXT record. Need help creating an SPF TXT record? Try using [this site](#) to create a record you can enter in this form.

Host	Domain Name	TTL	Text	Delete
@ (None)	.radiusadvertising.com.	7200	v=spf1 mx ip4:63.194.168.220 -all	<input type="checkbox"/>
_ep	.radiusadvertising.com.	7200	<ep xmlns='http://ms.net/1'><out><	<input type="checkbox"/>
	.radiusadvertising.com.	7200		<input type="checkbox"/>

Text (TXT Records)

SPF (Sender Policy Framework) records can be entered as TXT record.

Host	TTL	Text
@ (None)	7200	v=spf1 mx ip4:63.194.168.220 -all
_ep .radiusadvertising.com.	7200	63.194.168.220

[Add/Edit »](#)

Considerations

Not all DNS hosting providers support configuration of 'txt' type records. The previous example uses Network Solutions. Other providers such as Go Daddy may only support SPF, but not Caller ID as it uses XML data.

If you do not host your own DNS, you will need to contact your DNS hosting provider to confirm that they support configuration of 'TXT' records.

If you have defined an IP address in your records (like in this example) you will need to update this record if the IP address of your mail server changes.

If you have created your own SPF record using the wizard at openspf.org, you will probably have a ~all at the end of the line. You will need to change this to -all in order to force a hard failure, as Kerio Connect will not block a soft fail.

Users outside of your network will not be able to relay email through the outgoing SMTP server of their Internet Service Provider if they are sending email from the email domain configured with an SPF or Caller ID record. External users should always use the Kerio Connect hosting their email domain for sending outgoing email. Some service providers may block SMTP protocol (TCP port 25). In this case you may specify an additional port for the SMTP service.

Bayesian self-learning in Kerio Connect

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**.

Optimizing spam protection in Kerio Connect

Kerio Connect provides multiple features to prevent spam. For a general overview of each feature, refer to [configuring spam control in Kerio Connect](#). This article describes in more detail the anti-spam features and outlines the implications of each feature.

SpamAssassin

Introduction

SpamAssassin provides three layers of spam protection:

- » Rules
- » Bayes
- » SURBLs

SpamAssassin Rules

SpamAssassin includes a preconfigured set of static rules that update with specific releases of Kerio Connect. The rules are located in the SpamAssassin folder of the mailserver directory. Modification to the rules is not recommended.

Kerio Connect passes the content of messages to SpamAssassin. SpamAssassin evaluates the message against its rules and assigns a numeric value to the message. Kerio Connect inserts this value as a score into the headers of the message. There are 3 possible X-Spam headers:

- » X-Spam-Status: - The cumulative score (hits), the threshold value 'required', and all positively evaluated rules with their associated values 'tests'
- » X-Spam-Flag: - YES, or NO to indicate if the message is spam
- » X-Spam-Level: - The cumulative score represented by a count of asterisks. For example, a score of 4.2 would be represented as ****.

SpamAssassin Bayes

The Bayes, or Bayesian filter is a dynamic component of SpamAssassin that works similarly to rules, however its intelligence is not statically pre-defined. This intelligence includes a database of message characteristics that updates continuously. Kerio Connect processes two types of messages into the Bayes database:

- » Self-Learned: Messages that exceed a score of 12, and both the header score and body score are above 3, or messages with a score that is below 0.1.
- » User-Trained: Messages that have been marked by end users of the mail system as either spam or not spam.

The Bayes score is combined with the score assigned by the static rules. The numerical value assigned by the Bayes filter is included in the X-Spam-Status header as 'Bayes'.

SpamAssassin SURBLs (Spam URI Realtime Blocklists)

All messages are scanned for links to Internet locations or URIs (Uniform Resource Identifier). These links are compared to a number of online blocklists. If a URI is located in a blacklist the cumulative spam score is adjusted according to the score that the blacklist assigns for the given URI.

Configuration and management of SpamAssassin

Configuration of SpamAssassin for Kerio Connect is located in the Administration console under **Configuration >**

Content Filter > Spam Filter. By default, SpamAssassin is enabled with the following settings:

- » Messages sent from local users are not scanned.
- » Messages which receive a score of 5 or above will be flagged as spam.
- » Messages which receive a score of 9.5 or above will be discarded.

Messages flagged as spam will be automatically sorted to the 'Junk email' folder, which is a default folder belonging to each user of Kerio Connect. Note that users who access mail using POP3 protocol will not have access to their 'Junk email' folder. These users should log into webmail and disable the automatic 'Junk email' filter from the settings menu.

Adjusting the threshold

The default threshold value of 5 is aggressive enough to block the majority of spam, while maintaining almost no false positives. This value may be decreased to improve the number of detected spam, however it is also possible to encounter more false positives. Before adjusting the threshold, it is recommended to examine the spam score of a sample of spam messages that have managed to pass the spam filter rating, and compare these scores to a sample of legitimate messages.

Managing SpamAssassin Bayes

By default, the Bayes filter is inactive. This is because it needs to establish a sufficient level of intelligence before evaluating email. It is highly recommended for users to train the server using one of the following techniques:

- » Using the 'Spam' or 'Not spam' buttons in webmail to mark messages that have been mistakenly marked by the server.
- » Moving messages between the 'Inbox' and the 'Junk email' folders which have been mistakenly marked by the server.

These actions will be logged in the Spam log, located in the Kerio Connect Administration console. The total number of trained messages will be displayed in the Administration console under **Configuration > Content Filter > Spam Filter > SpamAssassin.** Once the number of trained messages has reached 200, the Bayes filter will become active. This can be verified by checking the X-Spam-Status header for the 'BAYES' score.

Although the Bayes filter can be very effective, it can also be detrimental. It is important for the Administrator to regularly monitor the Bayes score, especially when there is an increase in unrecognized spam. Many spammers will try to poison the Bayes database by sending the server specially crafted emails. Check the Bayes score for a sample of spam email (both recognized and unrecognized) as well as legitimate email. The Bayes score should generally have a negative value for legitimate email, and a positive value for spam email. If the Bayes score seems universally low, it may have become poisoned, and should be reset.

Resetting the Bayes

All components of the Bayes filter are located in the Kerio Connect store directory under /spamassassin/bayes/. To reset the Bayes, simply rename, or delete the bayes folder, then restart Kerio Connect.

Custom Filters

Although custom filter rules are processed independently of SpamAssassin, they are primarily used to either modify or bypass the SpamAssassin score. Because the majority of spam is highly variable and inconsistent, custom rules are more commonly used to whitelist particular senders or entire domains by using the option 'treat the message as non-spam'. With a sufficient whitelist, it suffices to set a slightly more aggressive spam threshold value.

There are some types of custom rules that can be created to reduce spam. For example, where certain standard headers such as 'From' or 'To' are missing.

Blacklists

On a default installation, Kerio Connect includes a small list of well known Internet blacklists, however none of them are enabled. Enabling these blacklists can greatly reduce spam, however some legitimate email may be rejected. It is important to occasionally review the security log to confirm the volume of rejected email from blacklists, and to make sure it is not rejecting legitimate senders. In case you do encounter legitimate senders which are rejected by the blacklist, the IP address can be extracted from the log and added to a whitelisted IP address group.

Note that this feature is only effective when Kerio Connect receives mail directly from the sender's outgoing mail server. In case Kerio Connect receives all mail from a single host, such as an SMTP gateway, it will not be able to appropriately identify the IP address of the originating mail server.

SPF (Sender Policy Framework)

Unfortunately email communication is designed so that spammers are able to use anyone's email address as the sender. The receiving mail server does not have any effective mechanisms for verifying the identity of the sender. Although SPF cannot protect against spoofing of a specific email address, it does allow the receiving mail server to identify a spoofed domain name.

The Domain name architecture allows for configuration of various types of hostname to IP mappings. One of these record types is referred to as TXT. SPF information is defined within a TXT record. During an SMTP conversation, Kerio Connect takes the sender's email domain and queries its authoritative name server for a valid TXT record containing SPF data. If no such record exists, Kerio Connect will allow reception of the email, unless it is rejected by another antispam component. A valid SPF record will contain all IP addresses which are allowed to send email using the sender's domain name. The IP address of the sending mail server is compared to this record. The message will be immediately rejected if the sending mail server's IP address does not exist in the corresponding SPF record.

Because spammers are capable of checking domains for these types of records, they are able to use spoofed addresses from domains which do not have any SPF record. This feature is therefore primarily useful in preventing spoofed email from domains configured locally on the Kerio Connect Spammers will often attempt to use the same email address for both the sender and the recipient. The receiving mail server therefore may be less inclined to consider the message as spam, since the sender address belongs to a local recipient. SPF is most effective at preventing this type of spam attack.

SPF is highly efficient as it does not result in false positives. The drawback to this technology is that it is not trivial to properly format the TXT record, and many DNS hosting providers do not allow configuration of TXT records. There are however companies such as <http://www.zonedit.com/> who provide DNS hosting services and allow configuration of TXT records. You can find more information regarding SPF at <http://www.openspf.org/>, including a simple form to automatically generate the proper TXT format used in your DNS configuration.

Spam Repellent

The majority of Spam is generated by specialized mass mailing applications. The objective of such software is to distribute as much spam as possible in a small amount of time. Successful mail delivery for spammers is therefore a luxury, rather than a necessity. Legitimate mail servers on the other hand are obligated to ensure that every message properly reaches its destination.

The Spam Repellent feature works by introducing an artificial delay to the SMTP greeting. Legitimate mail servers will typically wait at least 2 minutes before closing the connection, while spam engines may wait only a few seconds. A good value is 25 seconds. This simple adjustment will eliminate a significant amount of spam, without causing any loss of legitimate email. The only minor drawback to this setting is that Internet email will take an additional 25 seconds to receive. It is recommended to enable the IP address exclusion so that internal users will not be affected by this setting.

SMTP Security and IP based restrictions

These features are primarily intended to prevent abuse, or misuse of the SMTP server. Because spammers typically try to abuse the SMTP server, these security settings can be effective in preventing inbound spam. By default, none of these features are enabled. Although it is recommended to enable these options, it should be done with caution and a bit of initial attention.

Max. number of messages per hour from one IP address: This feature is most effective in preventing open relay, rather than blocking inbound spam to local recipients. Before enabling this option, it is recommended to examine the mail log. In some network configurations, the Kerio Connect may be receiving the majority of its mail from a single host, such as an SMTP gateway. In this case the IP address of the gateway should be added to an address group which is referred to by the option 'Do not apply these limits to IP address group'. An appropriate value for this option may range anywhere from 20 to 100, depending on the nature of the users of the mail system.

Max. number of concurrent SMTP connections from one IP address: Most legitimate mail senders will only open one or two SMTP connections, depending on how many messages someone is trying to send at once. A appropriate value for this option is 5.

Max. number of unknown recipients (directory harvest attack protection): Spammers will sometimes try to attack a mail server by guessing common types of addresses. The spammer is able to use this technique to create a list of known recipients on a server. By enabling this option, Kerio Connect will refuse any SMTP connections from the offending SMTP client for one hour. A appropriate value for this option is 3.

Block if sender's mail domain was not found in DNS. This option should be enabled. It confirms that the sender's mail address exists as a valid domain. Any legitimate message should contain a valid sender address.

Max. number of recipients in a message: The value of this option is based on the behavior of the users of the mail system. In some circumstances, a user may have a distribution list containing hundreds, or even thousands of recipients. It is the Administrators decision to determine an appropriate maximum value of recipients in a single message. This feature is more effective at preventing unauthorized mail relay, than rejecting inbound spam.

After enabling these options, it is very important to review the security log to ensure that legitimate mail senders are not affected by these features.

Kerio Connect Client AntiSpam Features

End users of the web client have personalized control over the spam filter. By default, all spam is sorted into a folder named 'Junk E-mail'. As mentioned previously, users can adjust the global spam server, or Bayes filter by using the 'Spam' or 'Not Spam' buttons that appear in the toolbar when a message is selected. Non Kerio Connect client users can train the Bayes filter by moving messages between the Inbox and the Junk E-mail folders.

Recommended Settings

The following summary shows the recommended settings in the different tabs of the Spam Filter section in the Kerio Connect Web administration.

Spam rating

- » Rating of messages sent from trustworthy relay agents - disabled. This includes devices in your internal network such as scanners or fax machines. Backup MX server should not be in this IP address group.
- » Tag score 4.5, block score 9.8.

Kerio Anti-spam

- » Enable Kerio Anti-Spam advanced filter. Set its contribution to Normal.
- » We recommend allowing use of signatures and metadata for improving the online scanning service.

Blacklists

Internet blacklist should add between 1 and 3 points depending on their reliability:

- » bl.spamcop.net - add 3 points
- » zen.spamhaus.org - add 2.5 points
- » dnsbl.sorbs.net - add 3.0 points
- » rhsbl.sorbs.net - add 3.0 points
- » db.wpbl.info - add 2.0 points
- » b.barracudacentral.org - add 2.5 points, Ask Directly=Yes
- » bl.spamcannibal.org - add 1.5 points

Please note that using certain DNS blacklists requires registration at the blacklist website and configuring Kerio Connect to ask the blacklist DNS server directly (eg. Barracudacentral).

Custom rules

Use custom rules as you wish. The rules can increase the spam score based on message subject or sender, or instantly block a message. You can also create a whitelist based on various criteria.

- » We do not recommend using too generic words which may produce false positive results. Eg. rule "If Subject contains substring "div"" is too generic and could block legitimate emails.
- » Enable "Reject message as soon as possible" option so From and To custom spam rules are applied during SMTP session and contribute to lower load in spam filter.

Caller-ID

- » Enabled.
- » Block the message.
- » Use exclude list for your backup MX, antispam gateways or relay SMTP servers.

SPF

- » Enabled.
- » Block the message.
- » Use exclude list for your backup MX, antispam gateways or relay SMTP servers.

Greylisting

- » Enabled
- » Use exclude list for your backup MX, antispam gateways or relay SMTP servers.

Spam repellent

- » Enabled, delaying SMTP greeting by 15-25 seconds.
- » Use exclude list for your LAN clients, backup MX, antispam gateways or relay SMTP servers.

How do I exclude an email address from a blacklist?

Kerio Connect can ask online blacklists if a sender's outgoing mail server is listed as a known spam offender. These blacklists greatly reduce spam, however they sometimes reject legitimate email. Kerio Connect allows you to define a custom whitelist of IP addresses to be excluded from the blacklist lookups. Some domains such as hotmail.com or yahoo.com mistakenly end up in blacklists, and there isn't an easy way to exclude all of their IP addresses.

Find out which blacklist is responsible

Kerio Connect reports all rejected emails and connections to the security log. If Kerio Connect is rejecting a message from a legitimate address, it will be reported in this log. You can search this log by right clicking in the window and choose 'find'. Perform an upward search from the bottom of the log for the sender's email address. The matched result will tell you the particular blacklist where this user's outgoing mail server was listed.

Change the action of the blacklist

Once you have identified the blacklist, you will need to change its action. From the Administration console, go to **Configuration > Content Filter > Spam Filter**. Under the Blacklists tab, edit the appropriate blacklist and change the action from 'Block the message' to 'Add spam score to the message'. Assign it a value of 10, which will ensure that any message from senders in this blacklist will be marked as spam, and can be filtered accordingly. Now that these messages are going to be received by Kerio Connect they can be processed by the spam filters, which will allow you to make exceptions based on header information.

Create a spam filter exclusion rule

Spam filter rules are defined in the Spam Rating tab under **Configuration > Content Filter > Spam Filter**. Create a new rule where the message header 'From' contains the email address of the sender who is being rejected by the blacklist. Choose to 'Treat the message as non-spam'.

How to reset the Spam Assassin plugin and Bayes database

Learn how to re-install the Spam Assassin plugin if the plugin is failing to initialize and how to reset the Bayes database if it has become corrupt or no longer effective.

Resetting Spam Assassin Plugin

Resetting the Spam Assassin plugin should only be done if you are getting error messages in the error log that shows the plugin is having trouble to start or initialize. You should have an error message like this in your error log:

IMPORTANT

SpamClient.cpp: Unable to initialize plugin.

To reset the Spam Assassin plug you will need to do the following:

1. Stop Kerio Connect
2. Navigate to the installation folder:

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

3. Once you are in the installation folder go to the '/plugins/spamserver' folder
4. Remove the folder 'spamassassin' and the file 'spamserver'
5. Run a repair install of Kerio Connect (You will need to download a copy of the Kerio Connect installer) - state exceptions
6. Then start Kerio Connect

By doing the above you are removing the old Spam Assassin plugin and installing a fresh copy of the plugin. Once you restart Kerio Connect the plugin will then update to the newest virus definitions from the Sophos servers.

[Resetting Bayes database](#)

Resetting the Bayes database only needs to be done if the database has become corrupted or is outdated. If the database is corrupted you should see error messages in the error log to indicate that. You should see an error message in the error log that says: 'RUNNING EXPIRE'.

To reset the Bayes database you will need to do the following:

1. Stop Kerio Connect
2. Navigate to the 'spamassassin' folder inside your store directory
3. You can verify the location of your store directory in the web administration in Configuration > Advanced Options [store directory tab]
4. Go inside the 'spamassassin' folder and delete the folder called 'Bayes'
5. Run a repair install of Kerio Connect (You will need to download a copy of the Kerio Connect installer)
6. Then start Kerio Connect

Resetting the Bayes database will allow your Kerio Connect to learn what is and is not spam all over again. The downside to resetting the Bayes database is that you will be prone to receiving more spam than usual until spamassassin has learned enough emails as spam/not spam. Once the database has been rebuilt then you should start to see less and less spam getting through Connect.

[How do I configure my Anti-Spam gateway to automatically gather valid addresses from Kerio Connect?](#)

In order to have full control over all incoming and outgoing email, most Anti-Spam gateways implement their own SMTP server, as opposed to transparently filtering the communication, which is a technique used by many firewalls. When acting as its own Mail Transfer Agent, or SMTP server, the Anti-Spam gateway will receive and store messages before forwarding them to the back-end mail server. This behavior however introduces a fundamental problem in that the SMTP gateway will collect all mail for the destination domain, even if the recipient address does not exist on the back-end mail server. It is therefore necessary for the Anti-Spam gateway to know all recipients of the back-end mail server; otherwise it will be responsible for handling the failure notifications of messages addressed to invalid recipients.

There are several techniques that can be used by Anti-Spam gateways in order to quickly and easily learn or obtain the valid recipients of the back-end mail server. One of the more common techniques involves the use of LDAP. LDAP clients may be used to lookup contacts stored in Kerio Connect, however this method is not ideal, as it is not a true reflection of the real list of recipients stored in Kerio Connect. An LDAP lookup to Kerio Connect will take the account of the authenticated user and look in all contact folders which are accessible to that user.

The preferred method for account verification involves an SMTP command called Verify (VRFY). With this command the SMTP gateway can very quickly identify if an address is valid on the receiving mail server. By default, Kerio Connect does

not allow this command as it can be exploited by spammers. This command however can be enabled from the configuration file.

To enable support for the VRFY command, edit the Kerio Connect configuration file (mailserver.cfg). By default, this file can be found in the following location:

- » Mac OSX: /usr/local/kerio/mailserver/
- » Red Hat/SuSE: /opt/kerio/mailserver/
- » Windows: C:\Program Files\Kerio\MailServer\

[Search for the following variable:](#)

```
<variable name="VRFYEnabled">0</variable>
```

And change its value to 1:

```
<variable name="VRFYEnabled">1</variable>
```

Stop **Kerio Connect**, save the changes to this file, then restart the mail server.

When connecting to Kerio Connect, you should now see the following result from an EHLO command. Notice the line, **250 - VRFY**, which is not normally announced by Kerio Connect.

```
EHLO
250-server.local
250-AUTH CRAM-MD5 PLAIN LOGIN DIGEST-MD5
250-SIZE 20971520
250-STARTTLS
250-VRFY
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-PIPELINING
250-ETRN
250-DSN
250 HELP
```

After enabling the VRFY command, you may still receive the following notice that the command is not allowed: "252 2.1.5 Verification not supported." This is because Kerio Connect will only allow the VRFY command to be issued from a trusted IP address. If you do receive this message, then you will also need to add the IP address of the Anti-Spam gateway to an address group that is trusted by your relay policy. This setting is located in the Kerio Connect administration console under SMTP Server > Relay Control. Enable the option to allow relay for users of an IP address group, and select the group which includes the IP of your spam gateway. Be aware that this is allowing anonymous relay from your spam gateway, so make sure that your spam gateway does NOT relay any mail addressed to non-local domains. Otherwise your mail server may quickly become an open relay.

4.6.9 Antivirus

This section helps you protect your Kerio Connect server against viruses, Trojans, and other types of attacks.

- » [Antivirus protection in Kerio Connect](#)
- » [Filtering message attachments in Kerio Connect](#)

- » Antivirus protection in Kerio Connect 9.2.1 and earlier
- » Using an external antivirus with Kerio products

Antivirus protection in Kerio Connect

NOTE

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.

NOTE

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 either **Discard the message** or **Deliver the message with the malicious code removed**.
5. In addition, you can select from two options for forwarding messages. Choose either to **Forward the original message to an administrator address** or **Forward the filtered message to an administrator address**
6. For any message that Kerio Antivirus cannot scan, Kerio Connect can either **Deliver the original message with a warning prefixed** or **Reject the message as if it was a virus**
7. Click **Apply**.

 **Antivirus**

Where is ... R. Cul Powaro ▾

Use the integrated Kerio Antivirus engine

Integrated antivirus engine

Check for update every [hours]: Update Now...
The current virus database was updated before: 2 days, 2 hours, 49 minutes
Last update check was performed before: 1 hour, 4 minutes
Virus database version: 8638436
Scanning engine version: 11.0.1.12



If a virus is found in a message

Discard the message
 Deliver the message with the malicious code removed
 Forward the original message to the administrator address:
 Forward the filtered message to the administrator address:

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

Deliver the original message with a warning prefixed
 Reject the message as if it was a virus (use the settings above)

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

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**

NOTE

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

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.

Attachment Filter

Where is ... R. Cul Powaro ▾

Enable attachment filter

Filter options

- Send the sender a warning informing that the attachment was not delivered
- Forward the original message to:
- Forward the filtered message to:
- Discard zip archive containing files with dangerous extensions (e.g. executable files).
- Info** The blocked attachment will be removed and the message will be delivered to the recipient.

Filter rules

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

Add... Edit... Remove

Apply Reset

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. To discard the ZIP attachments with dangerous files, select the **Discard zip archive containing files with dangerous extensions...** option.

NOTE

New in Kerio Connect 8.5!

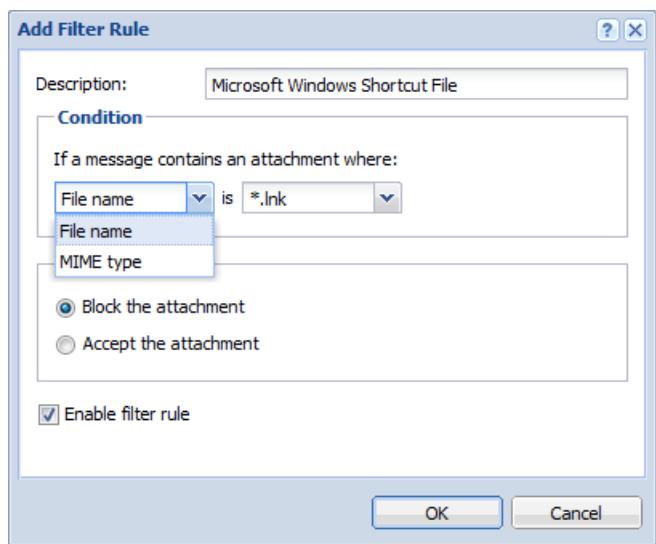
7. Select any of the predefined filter rules. Each rule can allow or block one specific type of attachment.
8. Click **Apply**.

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](#).

Antivirus protection in Kerio Connect 9.2.1 and earlier

NOTE

For Kerio Connect 9.2.2 and newer, see [Antivirus protection in Kerio Connect](#).

Kerio Connect can protect against malicious emails with viruses. Viruses may infect your computer and cause harm to your files or to your computer system.

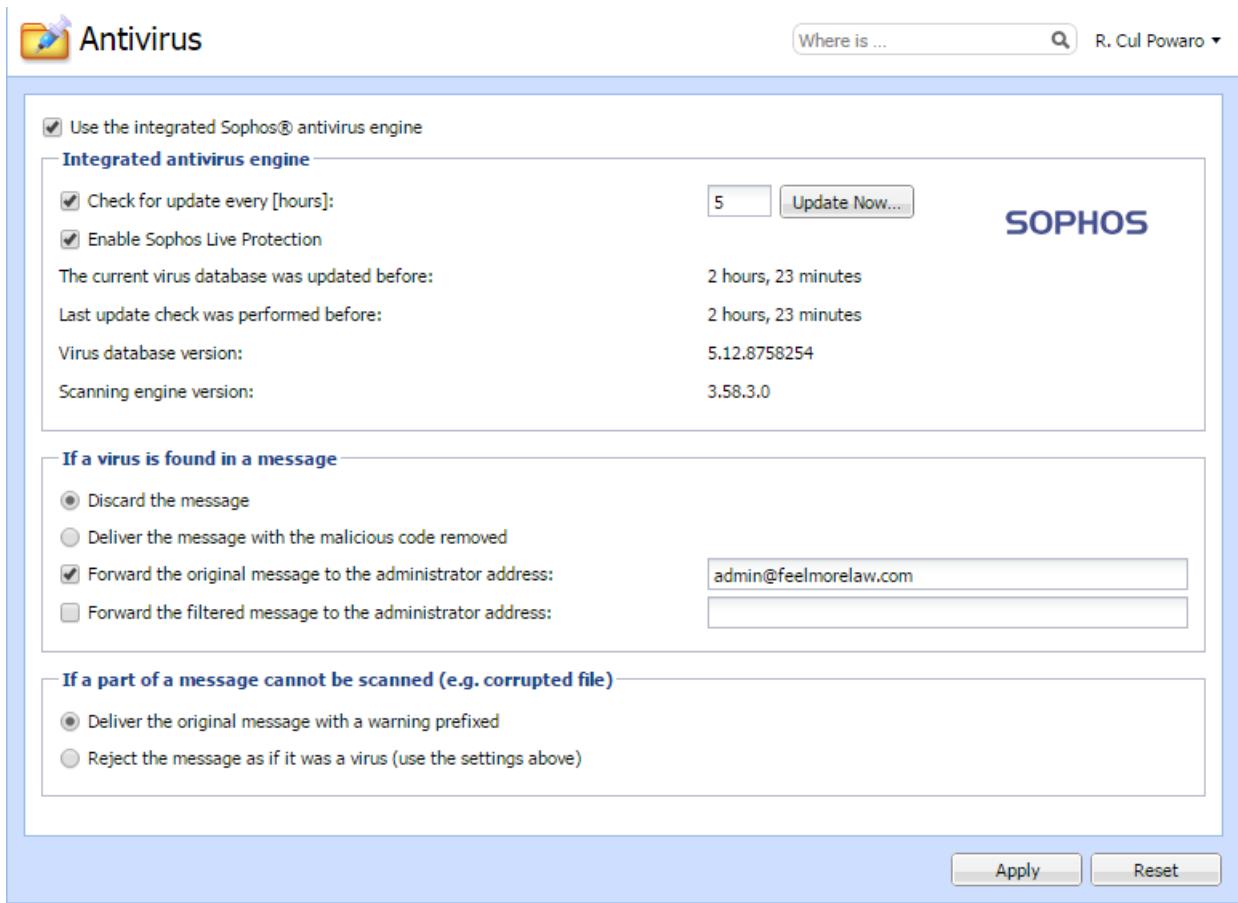
Kerio Connect's internal Sophos antivirus engine protects all email from these harmful viruses.

NOTE

Sophos antivirus is an optional component and is not available for [unregistered trial versions](#). See [Licenses in Kerio Connect](#).

Configuring Sophos in Kerio Connect

1. In the administration interface, go to the **Configuration > Content Filter > Antivirus** section.
2. Select the option **Use the integrated Sophos antivirus engine**.
3. To update the virus database automatically, select **Check for update every [hours]**. Kerio Connect downloads the database files via the HTTP protocol. Provide a persistent connection and allow the communication on your firewall or [proxy server](#).
4. New in Kerio Connect 8.4.2: To allow Kerio Connect to contact Sophos servers for the antivirus check, select **Enable Sophos Live Protection**. This option ensures that the Kerio Connect performs the antivirus check against an always up-to-date cloud database before it downloads the database with the regular update. Note that Kerio Connect sends only a one-way hash of the attachments to the Sophos servers.
5. Select the action for messages that contain a virus. Kerio Connect can:
 - **Discard the message**
 - **Deliver the message with the malicious code removed**
6. 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**
7. For any message that Sophos 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**
8. Click **Apply**.



Configuring the HTTP proxy server

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

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

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

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**

NOTE

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.

Using an external antivirus with Kerio products

Kerio Control and Kerio Connect include Kerio Antivirus that provides an integrated protection against malicious viruses.

However, 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.

4.6.10 SSL certificates

This section contains information about:

- » [Configuring SSL certificates in Kerio Connect](#)
- » [Adding trusted root certificates to the server](#)
- » [How do I configure OS X to use my self-signed SSL certificate?](#)
- » [How do I import a private key which is protected by a pass phrase?](#)
- » [How do I re-issue my SSL certificate?](#)
- » [How do I renew an expired SSL certificate?](#)
- » [How to enable SSLv2 support](#)
- » [Making SSL certificates trusted in Safari](#)
- » [Self-signed certificates in Mozilla Thunderbird](#)
- » [Transferring a signed SSL certificate from Internet Information Server into Kerio Connect](#)

Configuring SSL certificates in Kerio Connect

To secure Kerio Connect by SSL/TLS encryption, you need an 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.

NOTE

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

NOTE

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

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.

NOTES

- » 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.
- » If you have multiple intermediate certificates, add them one by one to the server certificate file.

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 a 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, click on **Import > Import Signed Certificate from CA**.

NOTE

If your certificate authority uses intermediate certificates, follow the steps in [intermediate certificates](#) before importing the certificate.

To obtain your certificate:

1. Go to section **Configuration > SSL Certificates**.
2. Click on **Import > Import Signed Certificate from CA**.
3. To enable the server to use this certificate, select the certificate and click on the **Set as Active** button.

Intermediate certificates

Kerio Connect allows authentication by **intermediate** certificates. To make authentication by these certificates work, follow these steps to add the certificates to Kerio Connect:

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

```
-----BEGIN CERTIFICATE-----
MIIDOjCCAqOgAwIBAgIDPmR/MA0GCSqGSIb3DQEBAUAMFMxCzAJBgNVBAYTA1
MSUwIwYDVQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMR0wGwYDVQ
..... this is a server SSL certificate ...
ukrkDt4cgQxE6JSEprDiP+nShuh9uk4aUCKMg/g3VgEMulkROzFl6zinDg5grz
Qsp0QTEYoqrc3H4Bwt8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDMzCCApygAwIBAgIEAAAATANBgkqhkiG9w0BAQUFADCBxDELMAkGA1UEBh
WkExFTATBgnVBAgTDFdlc3R1cm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
..... this is an intermediate SSL certificate which
signed the server certificate...
5BjLqgQRk82bFiluoG9bNm+E6o3tiUEDywrgrvX60CjbW1+y0CdMaq7dlpszRB
t14EmBxKYw==
-----END CERTIFICATE-----
```

3. Save the settings.

Adding trusted root certificates to the server

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

Function	Method
Add	Use command: <code>sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain ~new-root-certificate.crt</code>
Remove	Use command: <code>sudo security delete-certificate -c "<name of existing certificate>"</code>

Windows

Function	Method
Add	Use command: <code>certutil -addstore -f "ROOT" new-root-certificate.crt</code>
Remove	Use command: <code>certutil -delstore "ROOT" serial-number-hex</code>

Linux (Ubuntu, Debian)

Function	Method
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

NOTE

Restart Kerio Connect to reload the certificates in the 32-bit versions or Debian 7.

Linux (CentOs 6)

Function	Method
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

NOTE

Restart Kerio Connect to reload the certificates in the 32-bit version.

Linux (CentOs 5)

Function	Method
Add	Append your trusted certificate to file /etc/pki/tls/certs/ca-bundle.crt cat foo.crt >>/etc/pki/tls/certs/ca-bundle.crt

NOTE

Restart Kerio Connect to reload the certificates in the 32-bit version.

How do I configure OS X to use my self-signed SSL certificate?

Learn to configure OS X to use your self-signed SSL certificate with Entourage, Safari and Firefox.

Entourage and Safari users

1. Launch the web browser Safari.
2. Type in the fully-qualified domain name you use to access webmail and add /server.cer to the end of the URL. For example: http://mail.kerio.com/server.cer
3. Click on the "Continue" button and a file named servercacert.cer should be automatically downloaded to your desktop.
4. Locate the servercacert.cer file on the desktop and double-click on it. The Keychain Access application should automatically launch.

5. In the Add Certificates pop-up window, set Keychain: to Login and click OK.

6. Double-click on the file named server.cacert.cer again.

7. This time set Keychain: to X509Anchors and click OK

You should now be able to access secure webmail using Safari or use the secure ports in Entourage without being warned that your certificate is untrusted or cannot be verified.

Firefox users should select the option "Accept this certificate permanently" when Firefox provides a pop-up warning that the certificate cannot be verified.

No additional steps should be necessary.

Why is using SSL important?

To encrypt your data for privacy. SSL makes data appear as random gibberish during transfer so a network spy cannot read it.

SSL can fix strange Entourage synchronization problems. Often times, Entourage working over DAV (port 80) can have many different kinds of synchronization problems which appear as folders that will not sync to the server or incorrectly deleted emails, contacts, or calendar events. Many firewalls do packet inspection and can interfere with DAV synchronization. If, however, the packets are encrypted, packet inspection can not interfere. For this reason, SSL can actually fix strange problems in Entourage. Even if you do not have a firewall, it is possible some packet inspection is occurring at remote locations so laptop users can benefit from using SSL.

How do I import a private key which is protected by a pass phrase?

When generating a certificate request, some key generation applications will create a pass phrase associated with the key file. When importing this key file into Kerio MailServer, it will appear successful, however after restarting Kerio MailServer all secure services will be disabled. You may find the following event in the error log:

```
socklib.cpp: Cannot load SSL private key file  
/usr/local/kerio/mailserver/sslcert/server.key: error:0906406D:PEM routines:PEM_def_callback:problems getting password
```

Kerio MailServer does not support password protected keys, however you can use an external utility to convert the key file so that it does not require a pass phrase. On linux/OSX you can run the following command on the key file:

```
openssl rsa -in server.key -out server.key
```

On Windows you can use the sslkeygen utility with the same command.

The private key is located in the following location:

Mac OS X

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

Linux

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

Windows

```
C:\Program Files\Kerio\MailServer\sslcert\
```

You may find multiple private key files located in this directory, (e.g. server.key, server1.key, server2.key). You can identify the correct key file by matching the file name to the active certificate name specified under the 'SSL Certificates' dialog in the Kerio MailServer administration console.

How do I re-issue my SSL certificate?

You need to re-issue an SSL certificate, perhaps because it was not possible to renew with a new .crt file sent by your Certification Authority (CA). Re-issuing a certificate involves creating a new certificate request in KMS and submitting it to the CA. The process of re-issuing an SSL certificate involves the following steps:

1. Generate a new certificate request
2. Import the renewed certificate into Kerio MailServer
3. Install the intermediate certificates (if applicable)
4. Examine the installed certificate to see if it is correctly installed

Generate a new certificate request

Follow the instructions for [generating a new certificate request](#) in the Kerio Administration manual. (Tip: You can use a web browser and view the certificate details of the old certificate. This might make it easier to fill in the certificate request form.)

You will need access to the certificate request you have just generated to re-issue the certificate with your certificate vendor. Choose the certificate request, then select "Show" then "Show Request..." in the buttons below. This can be used to copy/paste the request text into your CA's web forms. When asked for the type of certificate to generate, select Apache Server.

Import the renewed SSL certificate into Kerio MailServer

Once you receive the SSL Certificate from the Certification Authority, in the form of a .crt file, you need to import it into Kerio mail Server using the KMS Admin Console:

1. In the SSL Certificates, section, click on (to highlight) the Request you created earlier.
2. Click on Import > Import Signed Certificate from CA and choose the server SSL Certificate (.crt file) sent to you by the Certification Authority.
3. Click on the new Certificate and then click on the Set as Active button (in the lower right corner).
4. Restart Kerio MailServer

Install the intermediate certificates (if applicable)

If your Certification Authority provides additional files with a .crt extension, so-called intermediate certificates, you can install these into the Kerio MailServer separately. For example, GoDaddy may supply a gd_intermediate.crt or gd_bundle.crt file. Note: the intermediate files may already have been installed when the certificates were first purchased. Check the location in step 2 below to determine if the files are already present. To install the intermediate certificate files in Kerio MailServer:

1. Stop Kerio MailServer.
2. Copy the intermediate certificate sent by the CA into the sslca folder in the Kerio MailServer folder. For example, in Windows, the default location is C:\Program files\Kerio\MailServer\sslca.
3. Start Kerio MailServer.

Examine the installed SSL Certificate to see if it is correctly installed

Open a web browser, enter the URL `https://mail.your-domain.com`, and you should not receive any warning messages. If you receive any warning messages regarding the certificate, the certificate was not correctly installed.

How do I renew an expired SSL certificate?

You have renewed your expired certificate with your certificate provider, and a .crt file has arrived in your email. You need to import it into KMS.

1. In the KMS Administration console, look in Configuration > SSL Certificates. Get the certificate name of the active certificate (Example: server, server1, server2, etc.)
2. On the operating system of KMS, go to the SSL certificate folder for the mailserver. Default locations:
 - Windows: C:\Program Files\Kerio\Mailserver\sslcert
 - Linux: /opt/kerio/mailserver/sslcert (you must be root)
 - Mac OS: /usr/local/kerio/mailserver/sslcert (you must be root)
3. Stop Kerio MailServer.
4. In this folder, you will see files with names like server.crt, server1.crt, etc. Find the name which matches the name from step 1 above. Make a backup of the .crt file with your active certificate name.
5. Copy the new crt file over it and give it the same name as the file from the previous step.
6. Start Kerio MailServer.
7. If all goes well, your certificate should now be updated.
8. If there are any problems, stop Kerio MailServer, put the original certificate back in the sslcert folder, and start Kerio MailServer. Then perform the steps to re-issue your SSL certificate.

How to enable SSLv2 support

Some email clients may not support SSLv3 and may fail to connect to Kerio Connect due to SSL version incompatibility. Because of this it may be required to enable old SSLv2 support in order to support these clients.

This topic contains modification of configuration file so it is needed to restart Kerio Connect service.

1. Stop Kerio Connect service
2. Open configuration file **mailserver.cfg** located in following directory by default:
 - C:\Program Files\Kerio\MailServer on Microsoft Windows system.
 - /opt/kerio/mailserver on Linux based system.
 - /usr/local/kerio/mailserver on Mac OS X based system.

3. Locate following option in the <>Security section of the configuration file:<><variable name="DisableSSLv2">1</variable>

4. Change its value to "0" as follows:<><variable name="DisableSSLv2">0</variable>

5. Save configuration file and start Kerio Connect service

Now is SSLv2 support enabled for Kerio Connect service.

Making SSL certificates trusted in Safari

Kerio Connect Client on Safari requires a trusted SSL certificate to use the **Chat** and **Presence** features. If your server does not use an SSL certificate signed by a trusted Certificate Authority, you can trust the certificate by importing it into your system.



Certificate error

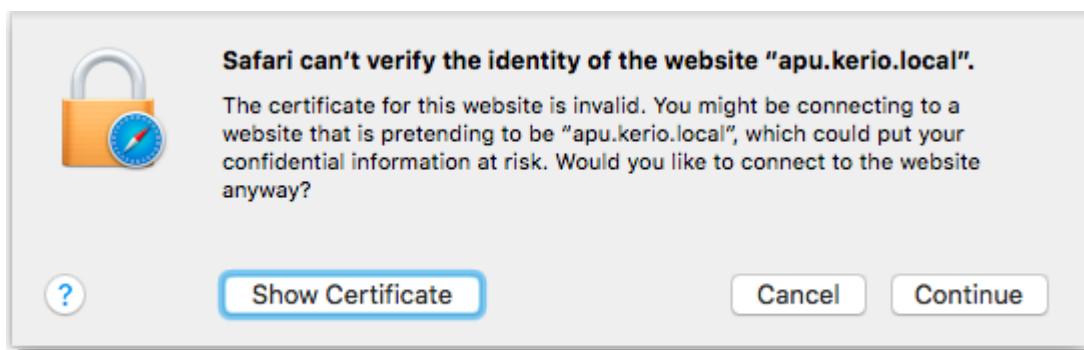
Safari cannot use chat and presence status without a trusted certificate.

[Learn more...](#)

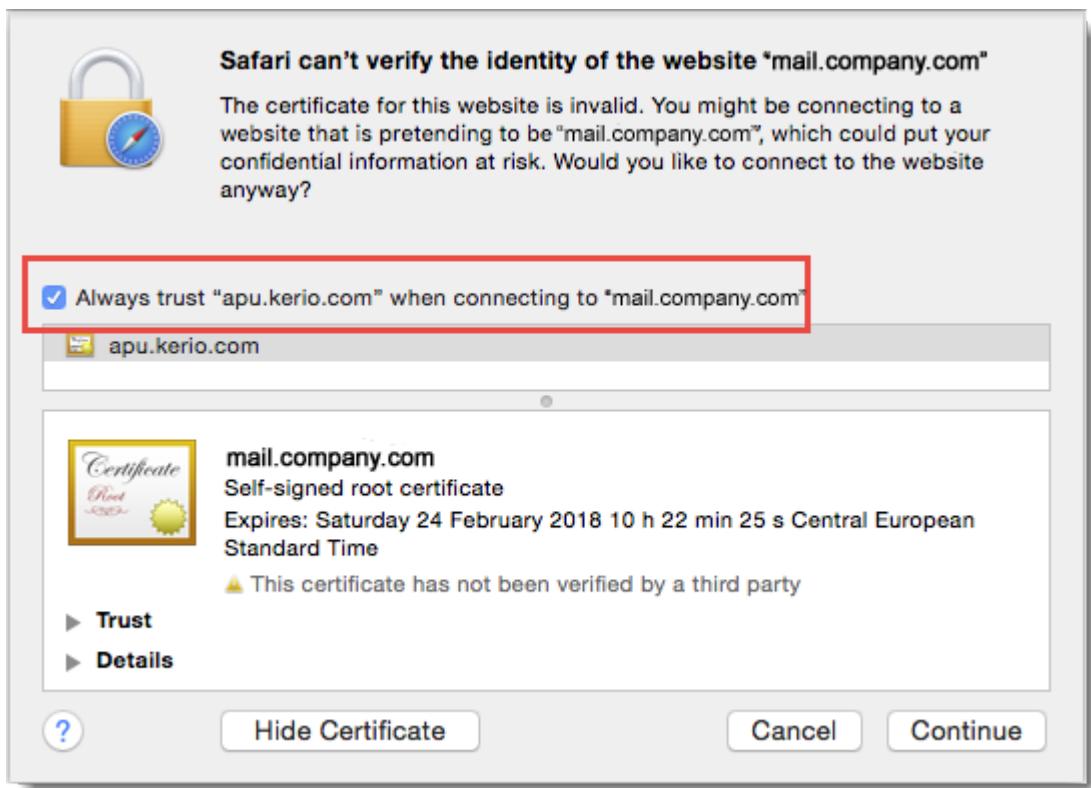
Making SSL certificates trusted in Safari

To import a certificate to your system:

1. Open Safari.
2. Log into Kerio Connect Client. During the login the **Safari can't verify the identity of the website mail.-company.com** dialog box opens.

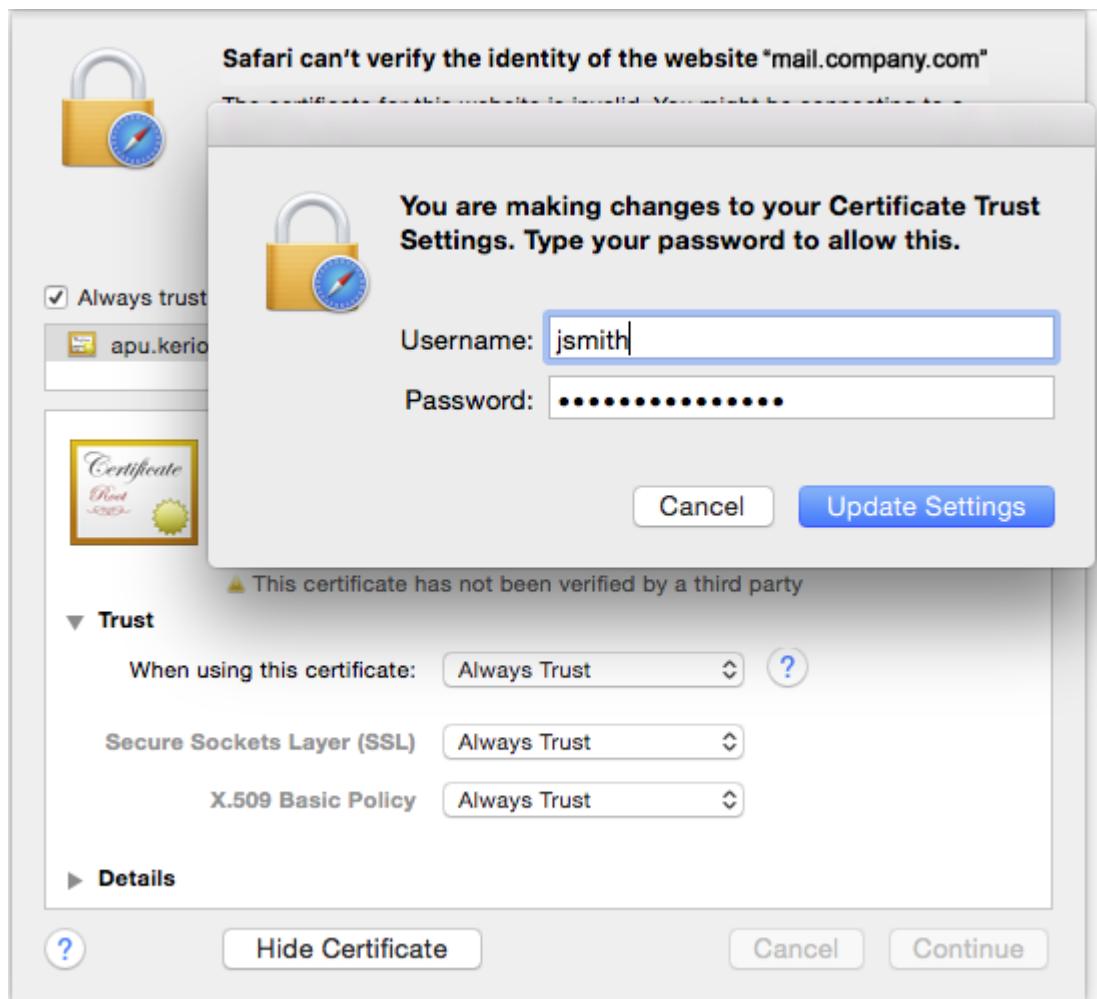


3. Click **Show Certificate**.
4. Select **Always trust mail.company.com when connecting to mail.company.com**.



5. Click **Continue**. A verification dialog box opens.

6. To confirm the SSL certificate as always trusted, type a password of the user with administration rights to the system.



7. Click **Update Settings**. The Kerio Connect Client login dialog opens.

Log into Kerio Connect Client and verify that **Chat** works properly.



Your messenger is set up
Select a contact and enjoy the conversation!

Self-signed certificates in Mozilla Thunderbird

How to set a self-signed certificate in Mozilla Thunderbird as trustworthy

If you use self-signed certificates in Kerio Connect, users with [Mozilla Thunderbird](#) may experience problems with secure authentication from a directory service (LDAPs protocol).

If this is your case, create an exceptions for your self-signed certificate in the application.

1. In Mozilla Thunderbird, go to **Tools > Options > Advanced > tab Certificates**.
2. Click on **View Certificates** and go to tab **Servers**.
3. Click on **Add Exception**.
4. Enter the name of your mail server and click on **Get Certificate**.

IMPORTANT

Do not forget to use the port number of the mail server.

Example: `mail.company.com:636`.

5. Save the exception.

NOTE

We recommend to check the option for permanent storage of the exception.

Your self-signed certificate is now considered as trustworthy by Mozilla Thunderbird.

Server certificate is not available

If your Thunderbird has a problem acquiring the server certificate, follow these steps:

1. In Mozilla Thunderbird, go to **Tools > Options > Composition > tab Addressing**.
2. Check the **Directory Server** option and click on **Edit Directories > Add**.
3. Enter the necessary information a check **Use secure connection (SSL)**. Confirm the dialog.
4. In the list of directory service servers, select the one you have just created a open it.
5. On tab **Offline**, click on **Download Now**.
6. Save the settings.
7. Now you can add the exception as mentioned above.

Transferring a signed SSL certificate from Internet Information Server into Kerio Connect

Transferring a signed SSL certificate from Internet Information Server into Kerio Connect

Export the private key from IIS

1. Open the Internet Information Services administration console located in the Control Panel > Administrative Tools.
2. Select the properties of your website.
3. Select the Directory Security tab
4. Select the button 'View Certificate'.
5. Select the Details tab.
6. Choose the 'Copy to file' button.
7. Choose 'Yes export the private key'.
8. The key will be generated using Personal Information Exchange PKCS#12(.pfx).
9. Specify and confirm a password.
10. Specify a name and save the file to the local disk. In this document we will use the example name example.pfx.

Export the certificate from IIS

1. Refer to the Internet Information Services administration console located in the Control Panel > Administrative tools.
2. Select the properties of your website.
3. Select the Directory Security tab.
4. Choose to 'View Certificate'.
5. Select the Details tab.
6. Choose the 'Copy to file' button.
7. Choose 'No, do not export the private key'.
8. Specify to export the certificate in base-64 encoded X.509 (.CER).
9. Specify a name and save the file to the local disk. In this document we will use the example name example.cer
10. Once the file is created, rename the extension to .crt (e.g. example.crt), as this is the extension format used by Kerio MailServer.

NOTE

The following procedure can only be performed from a Windows computer. The key file can be later copied to another operating system.

Change the key format from PKCS#12 to RSA

1. Download the [SSL Certificate Utility](#).
2. Extract the zip file to some location on the local hard drive. There are four necessary files: ssleay32.dll, libeay32.dll, openssl.cfg and openssl.exe.
3. Move the two files exported from IIS (example.crt and example.pfx) into the folder containing the extracted files.
4. Execute the file openssl.exe.
5. Type the following command: pkcs12 -in example.pfx -nocerts -out example.pem.
6. You will need to supply the password used when you created the Personal Information Exchange file during the export from IIS.
7. After supplying the password, you will then be asked to create and verify a "PEM pass phrase". You will need to supply this pass phrase in order to convert the "PEM file" to a KEY file. This pass phrase will be used only once, and is not relevant after the key file has been created.
8. At this point you will have a new file in the same directory called example.pem.
9. Type the following command: rsa -in example.pem -out example.key.
10. After entering the "PEM pass phrase", the example.key file will be generated. You will no longer need the "PEM pass phrase".

Import the certificate and key files into Kerio MailServer

1. Locate the /sslcert directory. The default location for each supported Operating System is provided below.
 - OS X: **/usr/local/kerio/mailserver**
 - Windows: **C:/program files/kerio/mailserver**
 - Linux: **/opt/kerio/mailserver**
2. Copy the example.crt and example.key files into this directory.
3. Restart Kerio MailServer
4. Connect to Kerio MailServer using the Administration console and go to the Configuration > SSL Certificates dialog.
5. Select the new certificate and choose the option 'Set as active'.
6. Restart Kerio MailServer and the certificate and key should now be used by Kerio MailServer.

4.7 Mail delivery and DNS records

This section contains information about:

4.7.1 Essential DNS Records for Mail Delivery and Spam Protection	391
4.7.2 Scheduling email delivery	393

4.7.3 Configuring POP3 connection	394
4.7.4 Receiving email via ETRN	397
4.7.5 Configuring Autodiscover in Kerio Connect	399
4.7.6 What is an MX record, and how is it created?	401

4.7.1 Essential DNS Records for Mail Delivery and Spam Protection

For proper configuration of a public facing mailserver for proper sending and receiving of mail, it is necessary to configure your public DNS records so that other mailservers can find you to send mail to your users, and so that other mailservers will trust you to receive your mail. There are also DNS records designed to protect you from spam and to help other servers to trust that your server is not a spam host. This article attempts to put all the DNS considerations together into one document for your review.

DNS Hosting Provider

Virtually all DNS Hosting Provider provide a web browser based control interface used to modify your DNS records, and should provide the technical support needed if you get stuck trying to modify any of the DNS records discussed in this article. Some common DNS Hosting providers consist of companies such as GoDaddy, Network Solutions and DynDNS to name three. There are possibly hundreds, so shop around if you have not found one yet. Many companies, including your own ISP might offer DNS hosting on your behalf, but make sure they offer a web based interface which allows you to have some control over your DNS records and make sure they offer good technical support. All of their interfaces are different, but they accomplish the same basic thing; they allow you to publish your hostnames and important DNS records such as the ones mentioned in this article to the Internet.

Hosting Your Own DNS

From within your DNS web hosting portal, it might be possible to configure it to not host your DNS, but instead to point your NS records someplace else. You could point your NS records to another DNS hosting provider or to your own DNS server at your static IP address. This article does not discuss how to do this, but if you are pointing it to your own DNS servers under your direct control, you must have advanced knowledge of the DNS servers you are managing or must have access to the documentation needed to create the DNS records yourself. This article still may prove useful to let you know what kinds of records you need. You still may need additional references to look up how to create them if you are not an expert with the DNS server you are managing. However, this article is aimed primarily at readers who will be using a web based DNS hosting service with its own technical support to help them if they need assistance with their DNS.

Static or Dynamic IP Address

Do everything you can to have a static IP address. It is very difficult to run a business with a dynamic home-user Internet plan. If there is no alternative, it might be possible to use something like DynDNS to do dynamic DNS hosting, but there are drawbacks this article will not cover. This article assumes you have at least one static IP address. For the most part, the web interface will be similar, however, at a dynamic DNS hosting provider.

"A" Record

An "A" record maps a name to an address. You will first need an A record for your mailserver. Your static IP address from your ISP was the first step, of course. For example, you might log into the web portal for the example.com domain and create an "A" record for "mail" for 192.0.2.21. This would create a mail.example.com published on the Internet. However, mailservers still wouldn't know that this is where to send mail. That's what "MX" records are for.

"MX" Record

Your MX record tells other mailservers the name of the server on the Internet to send mail to for your domain. It is a free text field, because it could have any name, including a name that is not part of your domain such as a name of a server from a mail hosting provider or a mail spam filter for example. If you have the Kerio Connect server with A record mail.example.com, you will need to create an MX record that just says "mail.example.com" as its value.

For more information, refer to [What is an MX record, and how is it created? \(page 401\)](#).

"PTR" Record

The PTR record is a reverse lookup which maps the IP address to the name.

Some mailservers will not trust mail coming from your server unless they can do a reverse DNS lookup. This takes two possible forms. Most mailservers care that a PTR record exists at all. Strict mailservers do a forward lookup on the name your mailserver introduces itself as such as mail.example.com, verify it is the IP address that is read off the connection, and do a PTR lookup on that IP address to see if it resolves to the same name.

A very common mailserver that comes to mind is craigslist. AOL is also famous for doing this check, and they have changed their minds from time to time and taken this check off, but it is impossible to predict when they will put the check back on again because they have several times in the past and still do sometimes.

The PTR record is more difficult than the others because it might require more advanced knowledge of DNS. This PTR record discussion here will assume you do not control your own PTR records. This assumes you own only a small number of IP addresses, and you must call your Internet Service Provider (ISP) to ask them to create a PTR record for you. Knowing the A record for mail.example.com, you must create a reverse PTR record. Most ISPs have a DNS Services department which can create a PTR record for you. They will ask the name you want, and what IP address you want assigned to that name. Beware, the person answering the phones often does not know what a PTR record is, and you often must get past that person to make the call work out. First ask for a PTR record and see if they know what to do. Next, ask if they have a DNS services department.

If you must create your own PTR record you will need to do it in your own DNS hosting services web interface. You might need to call them for support. If you host your own DNS, you will need to create a reverse zone which is not covered in this article.

"SPF" Record

SPF gives other mailservers a way to verify that mail claiming to be from your domain is from one of your IP addresses. They do this by checking a special TXT record you put in your DNS records. It is an interesting way to prevent mail spoofing.

For more information, refer to [Creating an SPF or Caller ID record \(page 359\)](#).

"Caller-ID" Record

Caller-ID was an earlier way to do what SPF does today. As with SPF, Caller-ID gives other mailservers a way to verify that mail claiming to be from your domain is from one of your IP addresses. They do this by checking a special TXT record you put in your DNS records. It is an interesting way to prevent mail spoofing. Caller-ID is not nearly as popular as SPF, but does protect you slightly differently than SPF. Because of this, not everyone believes Caller-ID is irrelevant. For more information, refer to [Creating an SPF or Caller ID record \(page 359\)](#).

Recommended Reading

Mail Routing is discussed in RFCs 5321 and 2821.

- » <http://tools.ietf.org/html/rfc5321>
- » <http://tools.ietf.org/html/rfc2821>

Some DNS errors including some useful discussion of PTR records and email security are included in RFC 1912:
<http://tools.ietf.org/html/rfc1912>

SPF is documented in RFC 4408. This RFC is actually an easy read as far as RFCs go.

<http://tools.ietf.org/html/rfc4408>

Caller-ID is an internet draft on the IETF website:

<http://tools.ietf.org/html/draft-atkinson-callerid-00>

4.7.2 Scheduling email delivery

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.

Time	Description	Action(s)
<input checked="" type="checkbox"/> At 00:00	Send and receive mail at midnight	Send mail, Download POP3
<input checked="" type="checkbox"/> Every 10 minutes	Send and receive mail every 10 minutes at working time	Send mail, ETRN Download

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.
4. Specify the **Time condition**. You can schedule tasks to happen:

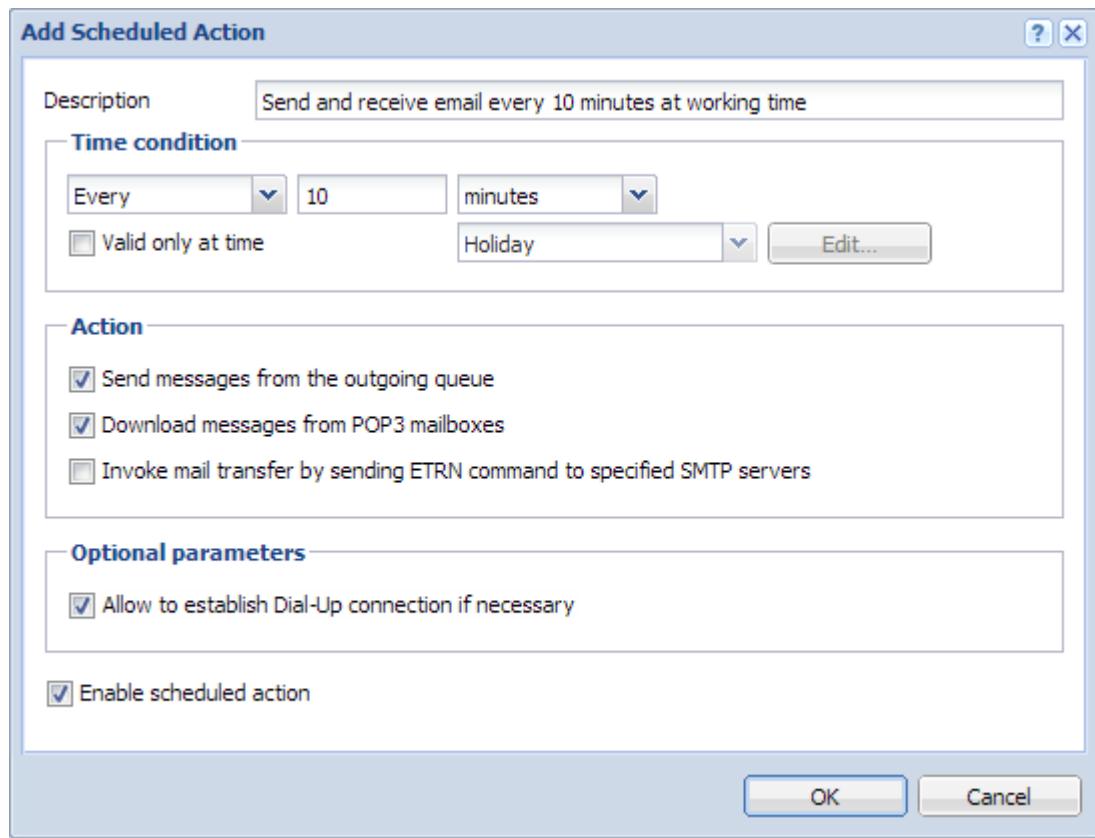
- Every specific number of minutes or hours
- At a specific time every day

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**



4.7.3 Configuring POP3 connection

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

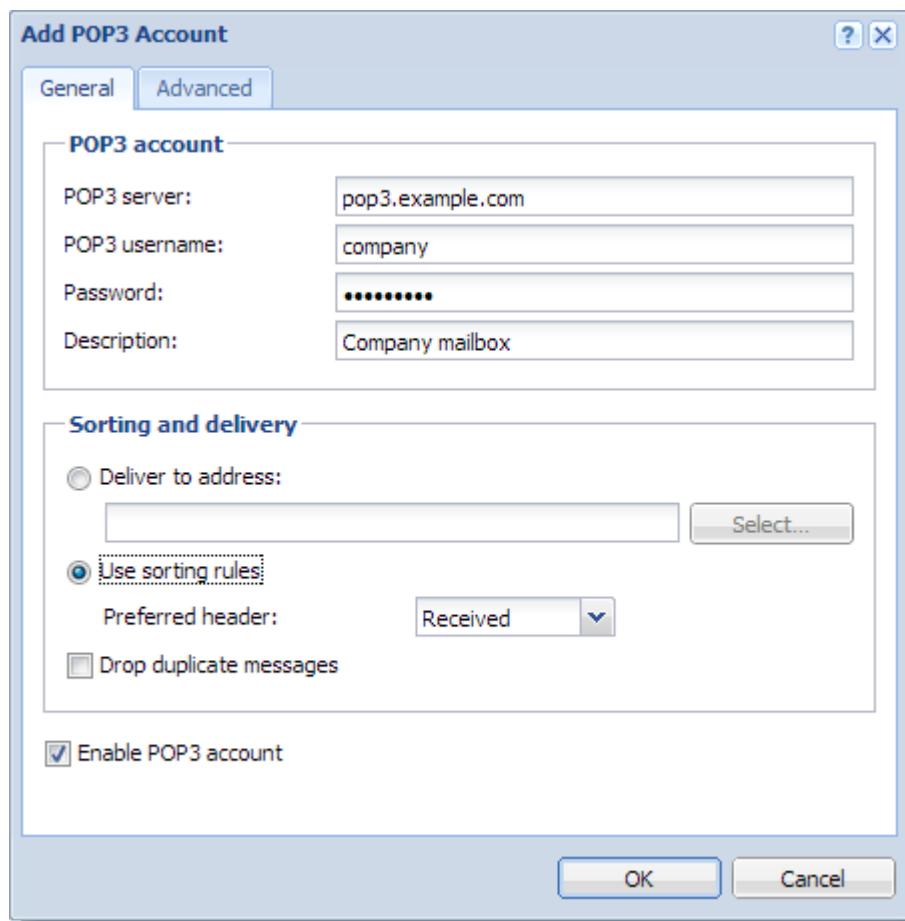
1. In the administration interface, go to **Configuration > Delivery > tab POP3 Download**.
2. In the **Accounts** section, click **Add**.
3. On the **General** tab, type the name of the POP3 server, and username and password of the POP3 account.

NOTE

The password length is max. 119 characters.

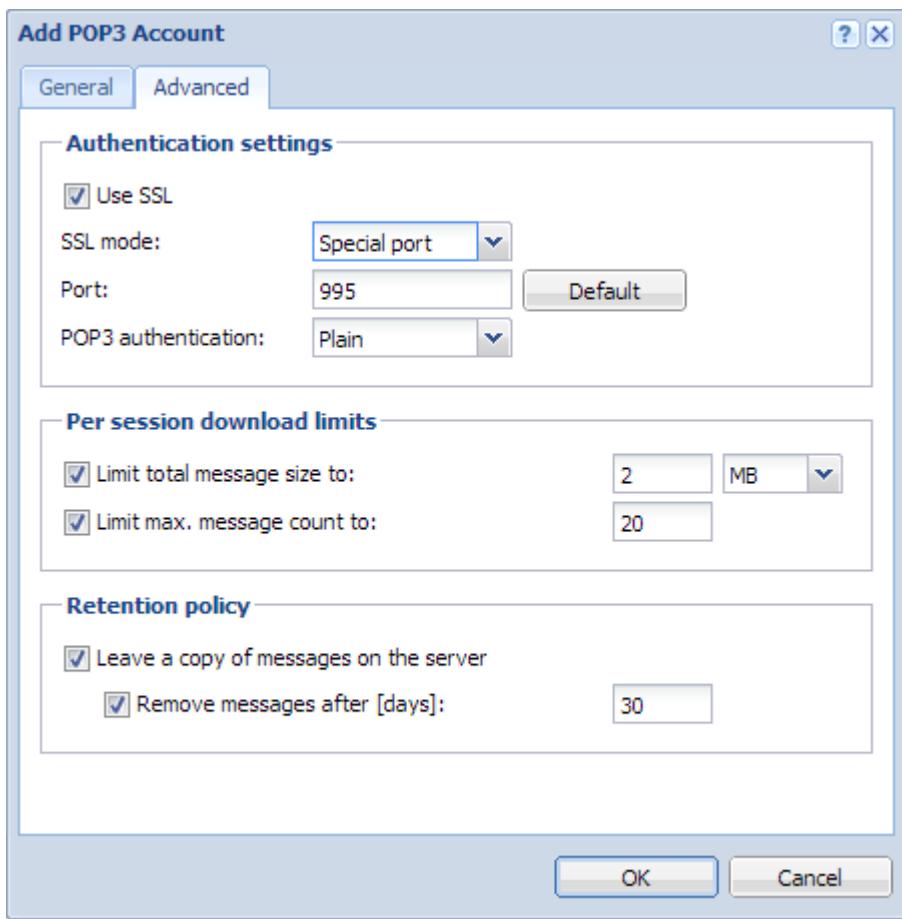
Kerio Connect can:

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



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

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



5. Click **OK**

POP3 Server	POP3 User	Deliver to	Description
<input checked="" type="checkbox"/> pop3.example.com	company	Sort with header "Received"	Company mailbox
<input checked="" type="checkbox"/> pop3.example.com	powaro	To mailbox powaro@feelmorelaw.com	Powaro's private mailbox

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 from the Kerio Connect server.



5. Click **OK**

Sort Address	Deliver to	Description
powaro@feelmorelaw.com	powaro@feelmorelaw.com	R. Cul Powaro
regret@feelmorelaw.com	media@feelmorelaw.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.

4.7.4 Receiving email via ETRN

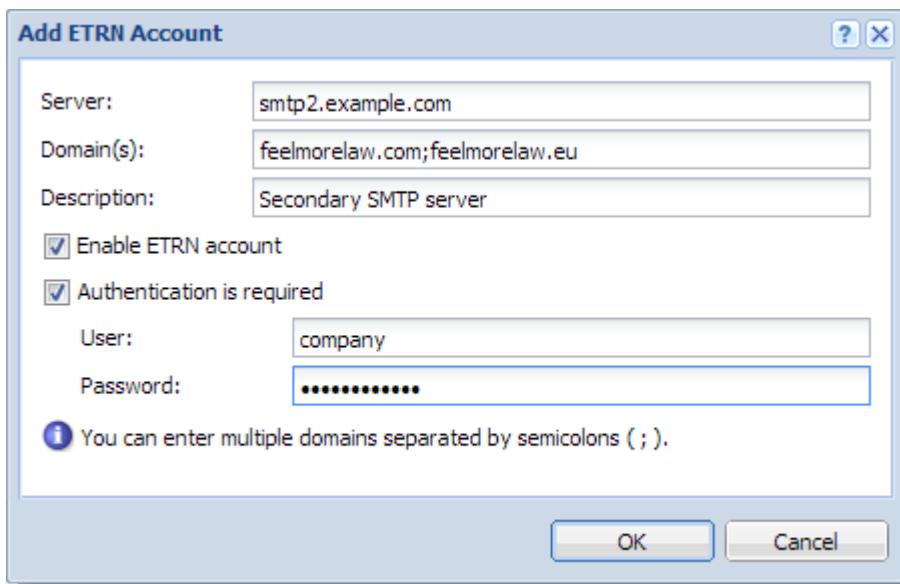
ETRN is a command of SMTP protocol. It serves for requesting emails stored on another SMTP server (usually secondary or tertiary SMTP servers).

Server	Domain(s)	Description
smtp2.example.com	feelmorelaw.com;example.com	Secondary SMTP server
smtp.example3.com	feelmorelaw.com	Tertiary SMTP server

Add... Edit... Remove Options... Download Now

Configuring the ETRN account

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

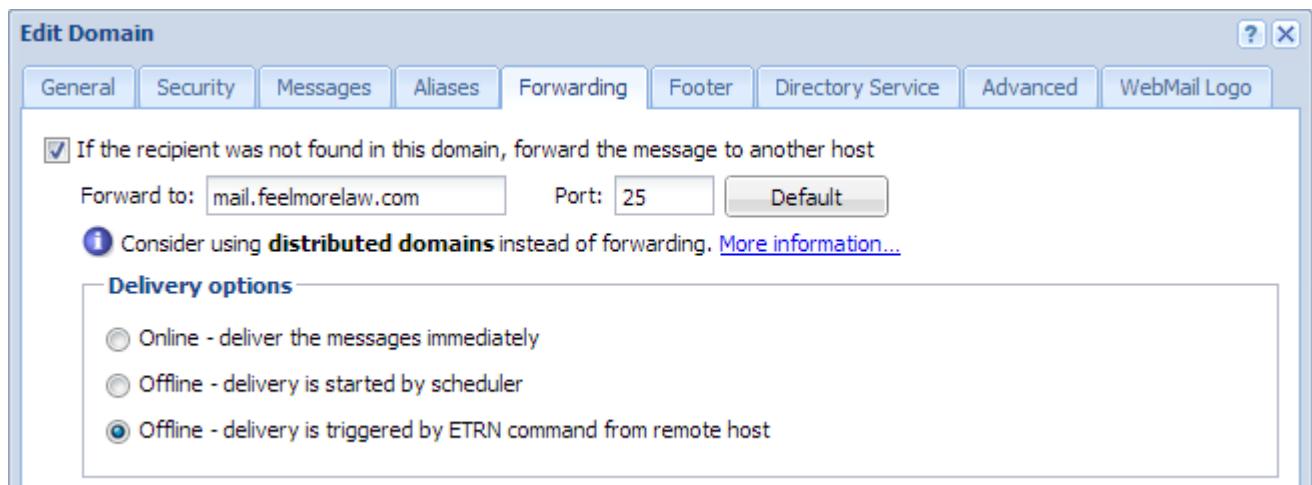


Forwarding email

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

- On your primary server, [enable and schedule sending of the ETRN command](#).
- Go to **Configuration > Domains** and double-click the backup server.

3. On the **Forwarding** tab, select **If the recipient was not found in this domain, forward the message to another host.**
4. Type the primary server hostname and port.
5. Select **Offline - delivery is triggered by ETRN command from remote host.**
6. Click **OK**



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

4.7.5 Configuring Autodiscover in Kerio Connect

Autodiscover simplifies the configuration of desktop applications and mobile devices that support communication using Microsoft Exchange or other web based protocols. By supporting automatic discovery users can setup accounts by themselves as the application requires only to specify an email address and password. The application uses autodiscover to obtain all other parameter associated with the account. Applications supporting Autodiscover include:

- » Kerio Connect Client desktop application
- » Microsoft Outlook
- » macOS applications
- » Most mobile devices implementing Exchange Activesync
- » Spark App for iOS

NOTE

You can also enable automatic configuration for instant messaging applications that use XMPP. For more information, refer to [Configuring DNS for instant messaging](#) (page 184).

Autodiscover uses several methods to locate the responsible server for an email address (refer to the [Microsoft Documentation](#) for full details). After locating the responsible server for an email address, the application opens a secure connection to the mail server to download an XML file containing the connection parameters for the mailbox account.

Requirements

Verify the following in your configuration to ensure proper operation of the Autodiscover process:

- » Secure connectivity (HTTPS) is accessible to your Kerio Connect server from the Internet. For more information, refer to [Securing Kerio Connect](#) (page 324).
- » Your Kerio Connect server's SSL certificate is signed by a trusted certificate authority (CA) such as InstantSSL by Comodo or RapidSSL. For more information, refer to [Configuring SSL certificates in Kerio Connect](#) (page 377).
- » If you have a web server or other type of server that is accessible via HTTPS when connecting to the root level of your domain (e.g., example.com) you must be sure that the SSL certificate presented by that server (usually your web site) matches your root domain name and the certificate is signed by a trusted CA. You can use online tools such as [sslshopper.com](#) to test the accessibility and validity of your server's SSL certificate.
- » You do not have a CNAME or any host record for your domain that resolves "autodiscover".
- » The Internet hostname of your Kerio Connect server matches the name on your SSL certificate. For more information, refer to [Internet hostname](#) (page 249).
- » All users in Kerio Connect have a full name assigned to their account (the full name must not be empty). For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).
- » Your DNS hosting provider supports SRV configuration. See below.

Configuring SRV for Autodiscover

The most reliable method of Autodiscover uses a Service record (SRV). Service records for Autodiscover consist of the following parameters and values:

Parameter	Value
Service	_autodiscover
Protocol	_tcp
Name (your email domain name)	example.com
Priority	0
Weight	5
Port	443
Target (your Kerio Connect server's Internet hostname)	mail.example.com

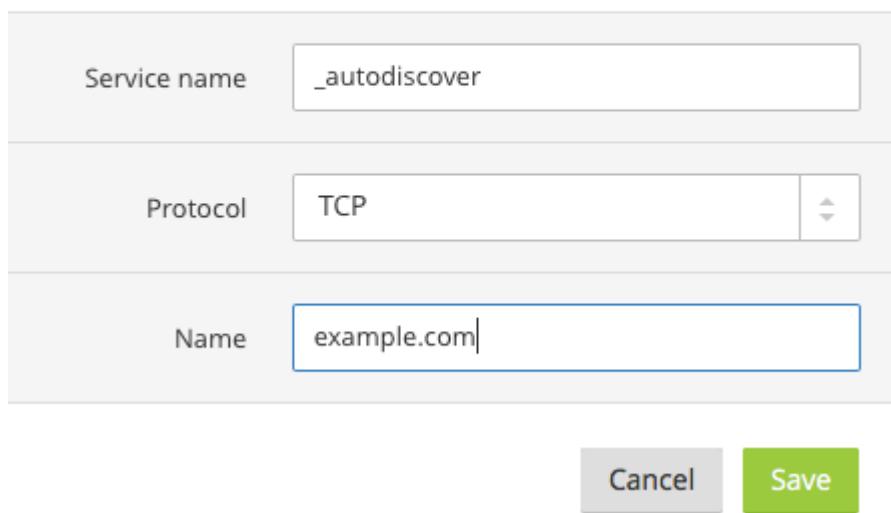
Example configuration using Cloudflare.com DNS manager

Edit Record: SRV name

_autodiscover._tcp.example.com.

Service name	_autodiscover
Protocol	TCP
Name	example.com

Cancel **Save**



Troubleshooting

You can verify your Autodiscover configuration using the [Microsoft Remote Connectivity Analyzer](#).

4.7.6 What is an MX record, and how is it created?

An MX (mail exchange) record is an entry in your DNS zone file which specifies a mail server to handle a domain's email. You must configure an MX record to receive email to your domain.

NOTE

If you are using Kerio Connect as an internal email system, with no communication outside of your domain, it's not necessary to configure an MX record for your domain. You may configure any domain in Kerio Connect, as it does not perform any DNS validation of its local domain names.

Setting Up an MX Record

1. To relay email outside of your locally configured domains, ensure that the underlying operating system properly resolves domain names. This means that a valid domain name server must be configured in the TCP/IP settings of the host operating system.

2. Configure the MX record on the authoritative name server for your domain:

- In most cases, the authoritative name server is the DNS servers managed by your domain registrar – for example, Godaddy or Network Solutions.
- These domain registrars usually provide additional services, including DNS hosting. In this case, you will use a web-based DNS configuration utility to configure your MX record.

- Here are some additional resources for configuring an MX record for Godaddy and Network Solutions.
<http://support.godaddy.com/help/article/7924/adding-or-editing-mx-records?locale=en>, <http://www.networksolutions.com/support/mx-records-mail-servers-2/>
- Since most DNS servers store its information in a cache for a certain period of time, it might take up to 24 hours for the change to get propagated over the internet to DNS servers where the record is stored. Email delivery can be pointed to the secondary email server in the MX record list until the primary server DNS name is changed.

3. Check if a DNS server applied the MX record changes by using nslookup command-line tool:

```
mac-mini: username$ nslookup
> server 8.8.8.8Default server: 8.8.8.8
Address: 8.8.8.8#53
> set q=MX
> kerio.com
Server: 8.8.8.8
Address: 8.8.8.8#53
...
>
```

Checking an MX Record

You can check a DNS MX record using an online test tool (e.g. <http://mxtoolbox.com/>) or by using nslookup command-line tool.

In the following example, three servers can receive emails for the kerio.com email domain. The lowest number means the highest server preference. In this example the primary MX server (the server with highest preference) is mx1.kerio.com:

```
mac-mini: username$ nslookup
> set q=MX
> kerio.com
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
kerio.com mail exchanger = 40 fw-c.kerio.cz.
kerio.com mail exchanger = 10 mx1.kerio.com.
kerio.com mail exchanger = 20 mx2.kerio.com.

Authoritative answers can be found from:
fw-c.kerio.cz internet address = 195.113.184.20
mx1.kerio.com internet address = 195.113.184.2
mx2.kerio.com internet address = 91.121.64.51
>
```

Additional Resources

» http://en.wikipedia.org/wiki/Mx_record - A mail exchanger record (MX record) is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient's domain, and a preference value used to prioritize mail delivery if multiple mail servers are available. The set of MX

records of a domain name specifies how email should be routed with the Simple Mail Transfer Protocol.

- » <http://www.icann.org/registrar-reports/accredited-list.html> - The following companies have been accredited by ICANN to act as registrars in one or more top level domains.
- » <http://www.internic.net/regist.html> - The following companies have been accredited by ICANN to act as registrars in one or more top level domains.

4.8 Services

This section contains information about network protocols and services used by Kerio Connect.

4.8.1 Services in Kerio Connect	403
4.8.2 Configuring the SMTP server	407
4.8.3 Securing the SMTP server	411
4.8.4 Can I run Kerio Connect and IIS web services on the same computer?	412

4.8.1 Services in Kerio Connect

Setting service parameters

You can set parameters for Kerio Connect services in the **Configuration > Services** section.

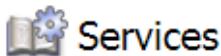
By default, all services are running on their standard ports.

NOTE

For security reasons, enable only the services you know will be used. For more information, refer to [Configuring your firewall](#) (page 324).

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



R. Cul Powaro ▾

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

[Start](#)[Stop](#)[Restart](#)[Edit...](#)

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.

IMPORTANT

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.

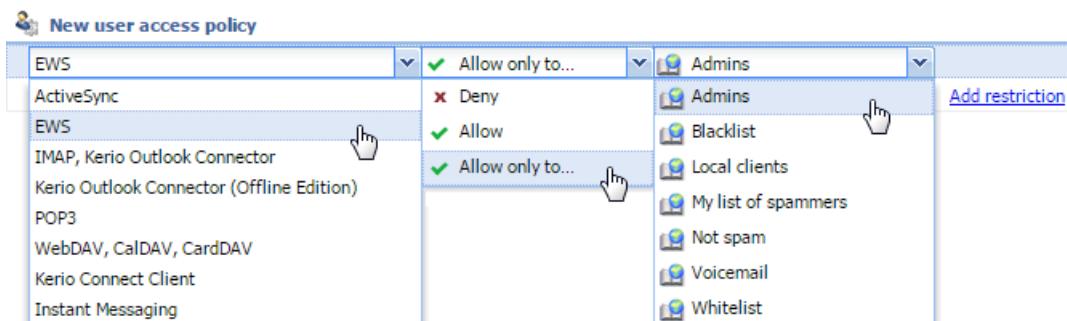
Restricting access to some services

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):

Service type	When to use
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	<ul style="list-style-type: none"> » 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.

4.8.2 Configuring the SMTP server

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.

NOTE

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:

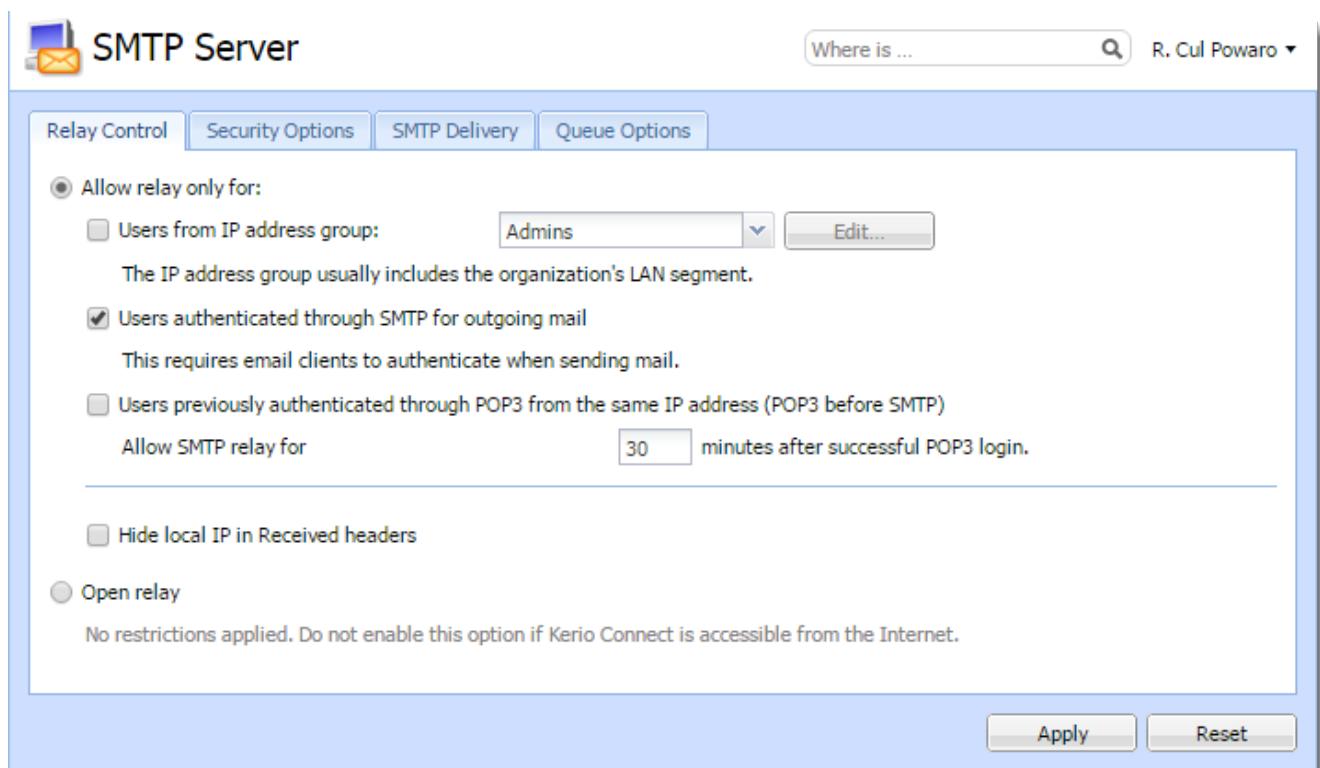
1. In the administration interface, go to the **Configuration > SMTP Server > Relay Control** section.
2. Select the **Allow relay only for** option.
3. To specify a group of IP addresses from which users can send outgoing messages, select the **Users from IP address group** option and the IP address 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.

NOTE

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.

5. 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.

6. Click **Apply**.



Screenshot 25: SMTP server

Sending outgoing messages through multiple servers

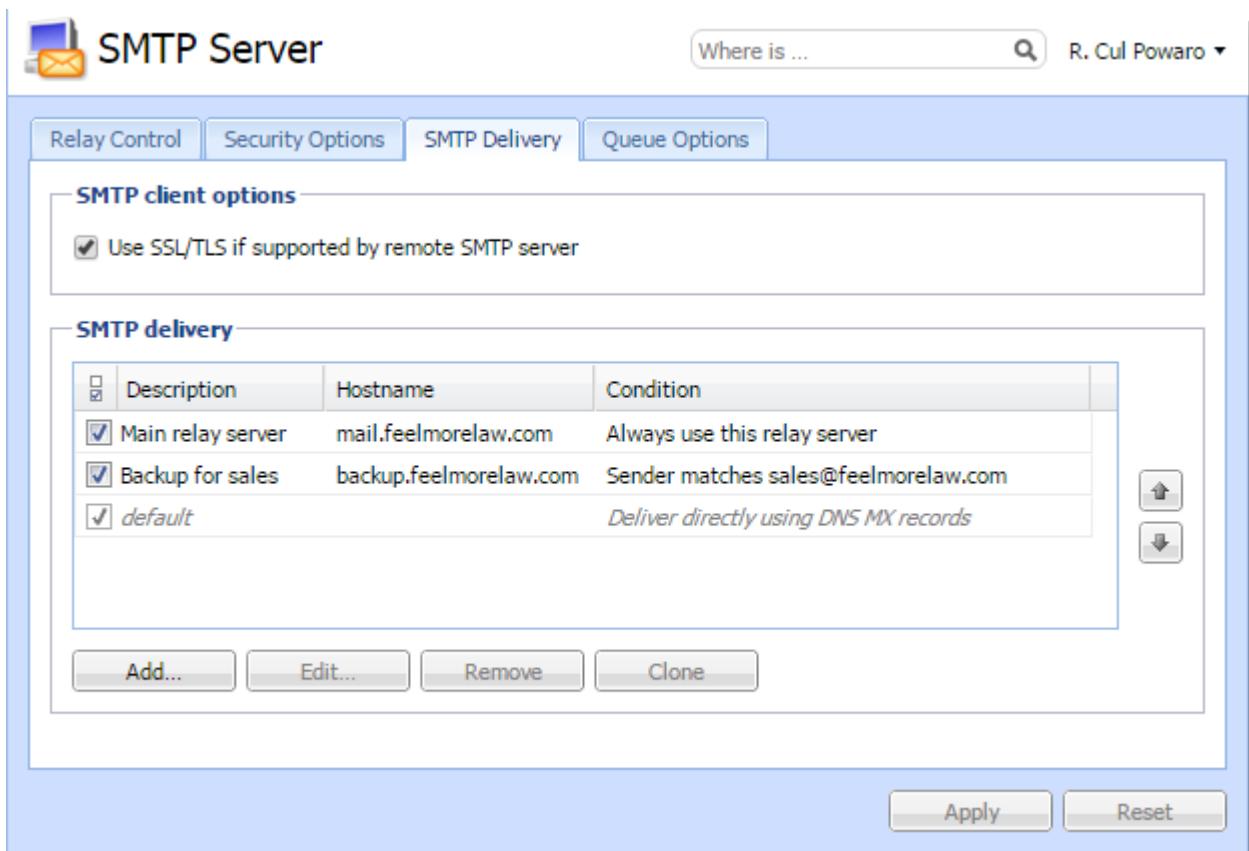
NOTE

New in Kerio Connect 9!

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

Kerio Connect can deliver messages:

- » Directly to destination domains using their MX records (the default SMTP relay server rule)
- » Through multiple SMTP servers. For example, Kerio Connect can use different SMTP relay servers for different domains in Kerio Connect.

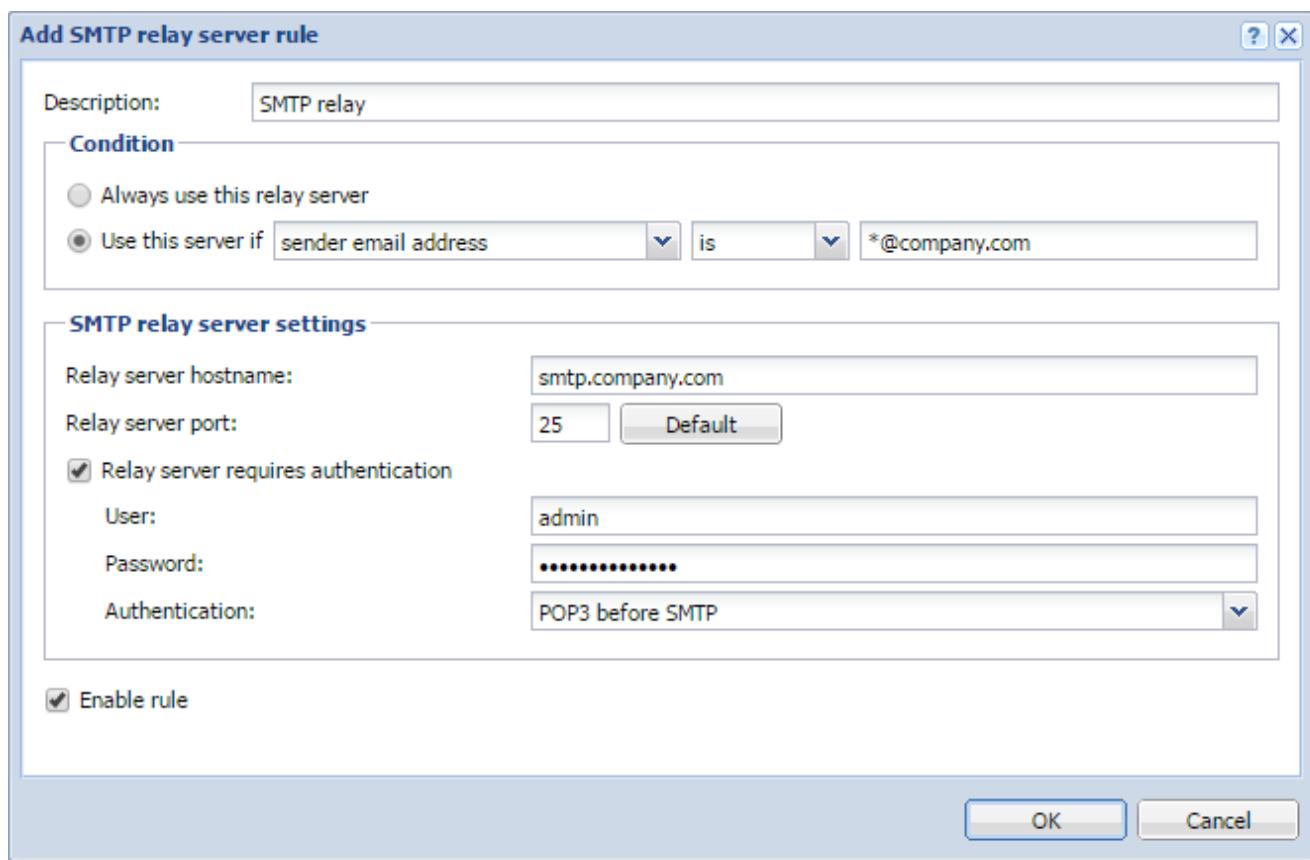


To define a SMTP relay server:

1. In the administration interface, go to **Configuration > SMTP Server > the SMTP Delivery tab**.
2. Click **Add**.
3. Type 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.

The screenshot shows the 'Condition' configuration dialog. It includes a radio button for 'Always use this relay server' (unselected) and another for 'Use this server if' (selected). The 'Use this server if' section contains fields for 'sender email address' (set to 'is *@company.com') and 'recipient email address' (set to 'is not'). There are also dropdown menus for operators like 'is' and 'is not'.

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**.



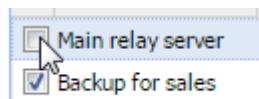
Kerio Connect processes the rules from the top down. The first server that matches is used to send the message. To change the order of the rules, select a rule and use the arrows on the right side to move it up or down.

The screenshot shows the 'SMTP delivery' rules list. It contains three rules:

Description	Hostname	Condition
Backup for sales	backup.feelmorelaw.com	Sender matches sales@feelmorelaw.com
Main relay server	mail.feelmorelaw.com	Always use this relay server
default		Deliver directly using DNS MX records

On the right, there are up and down arrow buttons for reordering. The 'Main relay server' rule has its checkbox cleared, indicating it is disabled.

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



Securing the SMTP server

For more information, refer to [Securing Kerio Connect](#) (page 324).

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.

4.8.3 Securing the SMTP server

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.

NOTE

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 Denial of Service (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 Kerio Connect administration interface with the title bar "SMTP Server". Below the title bar are four tabs: "Relay Control", "Security Options" (which is selected and highlighted in blue), "SMTP Delivery", and "Queue Options". A search bar "Where is ..." and a user profile "R. Cul Powaro" are also visible. The main content area is titled "IP address based limits" and contains the following configuration options:

- Max. number of messages per hour from one IP address:
- Max. number of concurrent SMTP connections from one IP address:
- Max. number of unknown recipients (directory harvest attack protection):
- Do not apply these limits to IP address group:

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**.



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.

4.8.4 Can I run Kerio Connect and IIS web services on the same computer?

Kerio Connect can be run on the same server as IIS, though a strategy must be devised since both applications will use some of the same ports. As an example, Kerio Connect and IIS web services will both use port 80 (HTTP) and port 443 (HTTPS), and will cause a port conflict unless some changes are made. Either Kerio Connect must be configured to use a different set of ports for its services or both applications must bind their services to different IP addresses. The second option of binding to a specific IP requires that you have assigned at least 2 IP addresses to the operating system, and your firewall is capable of routing for multiple Internet IP addresses over the same protocol (in case your mail server is behind a NAT firewall).

Alternate Ports

Do the following in the Kerio Connect administration interface:

- Go to Configuration > Services
- Edit the HTTP and/or the HTTPS services
- On the "Properties" tab, select the port value and choose to "Edit"
- Change the number in the "Port" field to a value of your choice, usually between 49152 and 65535
- Apply the changes

Note: Running protocols on non-standard ports may cause connection problems in some cases. For example, some mobile devices do not support Activesync through ports other than 80 and 443.

Solution 2: Kerio Connect on a different IP address, using the same standard ports as IIS

Do the following in the Kerio Connect administration interface:

1. Go to Configuration > Services
2. Edit the HTTP and/or the HTTPS services
3. On the "Properties" tab, select the IP Addresses value and choose to "Edit"
4. Select the alternate IP address in the "IP Address" pull down menu
5. Apply the changes

This solution also requires the disabling of socket pooling in Windows. To disable socket pooling, please visit [this Microsoft knowledge base article](#) for details.

5 Troubleshooting

This section helps you resolve possible issues you may encounter information about:

5.1 Common issues	414
5.2 General errors	429
5.3 Vulnerabilities	439

5.1 Common issues

This section helps you fix problems you might encounter when using Kerio Connect or synchronizing your accounts.

5.1.1 Cannot start HTTP or HTTPS services on Mac OS	415
5.1.2 Detecting that Kerio Connect has been compromised and used for spamming	415
5.1.3 Browser extensions or add-ons may interfere with Kerio products	417
5.1.4 Distributed Sender Blackhole List Errors (DSBL)	417
5.1.5 How do I get older versions of Kerio software?	418
5.1.6 How do I get the .eml source for an email?	418
5.1.7 How do I reset the password for a user if I've lost access to the WebAdmin of Kerio Connect?	419
5.1.8 Active Directory/LDAP error: Unable to search in dc=example,dc=domain,dc=com (Size limit exceeded)	420
5.1.9 How to fix a malformed journal.db with a SQLite error	420
5.1.10 How to repair or reset Anti-Virus in Kerio Connect	421
5.1.11 I can't send outgoing mail if I'm using Open Directory or Active Directory	422
5.1.12 I can't use national characters in my password.	423
5.1.13 I have created a custom rule to allow an email address or domain through but it is still being blocked	423
5.1.14 I've been training the spam filter but I'm still receiving the same spam emails	423
5.1.15 Kerio Connect Client is not displayed correctly in Internet Explorer	424
5.1.16 Kerio Connect user cannot login to their email account	424
5.1.17 Moving user from active directory service to local user database or vice versa causes synchronization errors with Outlook 2011	425
5.1.18 POP3 connection fails during download	426
5.1.19 SMTP Status and Reply codes	426
5.1.20 Users folder size is reporting incorrectly in WebAdmin	427
5.1.21 Why am I getting multiple copies of an email?	428
5.1.22 Why does Kerio Connect automatically expunge messages marked for deletion through IMAP?	428

5.1.23 Why does the Exchange migration tool state I am not an administrator?	429
--	-----

5.1.1 Cannot start HTTP or HTTPS services on Mac OS

Issue encountered

After installing Kerio Connect on Mac OS, the HTTP and HTTPS services may not start because the ports 80 and 443 are already in use by another process.

Solution

Yosemite and El Capitan

Edit the apache configuration file:

```
/Library/Server/Web/Config/Proxy/apache_serviceproxy.conf
```

If you look in `/Library/Server/Web/Config/Proxy/apache_serviceproxy.conf` you'll see apache httpd configured to listen on various ports: 80, 443, 8008, 8800, 8843.

Remove or comment out the following lines:

```
listen 80  
listen 443  
listen 8800  
listen 8843
```

You can also change port numbers in Kerio Connect administration to resolve port conflicts if required.

NOTE

We recommend to restart the Kerio Connect server.

Mountain Lion through Mavericks

The following command will properly disable the built-in Apache web service:

```
sudo launchctl unload -w /System/Library/LaunchDaemons/org.apache.httpd.plist
```

After the service is properly disabled, the 80 and 443 sockets are then available, and you can successfully start the HTTP and HTTPS services in Kerio Connect.

NOTE

We recommend to restart the Kerio Connect server.

5.1.2 Detecting that Kerio Connect has been compromised and used for spamming

Your server may be compromised if any of the following happens:

- » Your Kerio Connect server is slow.
- » Users get bounce backs of emails they did not send.
- » Your Kerio Connect server IP address (external IP) is getting blacklisted.

- » A large email queue consists of multiple email messages sent to addresses that you do not normally send to. These messages maybe send to Yahoo, AOL, Hotmail, and so on.

A combination of the above may point that someone's password being guessed, or a user's machine has received a virus/Trojan that is mass emailing/spamming.

Verifying message senders in the message queue

Kerio Connect can display information on who sends messages and where these messages come from.

1. In the administration interface, go to **Status > Message Queue**.
2. Right-click any column header.
3. Click **Columns**.
4. Select **Authenticated Sender** and **Sender IP**.

Authenticated sender can indicate that user's password may have been compromised.

Sender IP can help to indicate if the email are sent internally (this can point to a virus or a Trojan on a local user machine), or external (this can point to a guessed password of an authenticated user).

Example

The screenshot shows the 'Message Queue' interface in Kerio Connect. At the top, there are tabs for 'Messages in Queue' and 'Message Queue Processing'. Below the tabs, there are two summary statistics: 'Message count: 5' and 'Message volume: 86 kB'. The main area is a table listing five messages. The columns are 'From', 'To', 'Created', 'Status', and 'Authenticated Sender'. The data is as follows:

From	To	Created	Status	Authenticated Sender
<paul@localhost>	fakeuser@fakedomain.com	2012-06-18 11:07	4.1.8 451 4.1.8 Sender address	jack@localhost
<mark@localhost>	fakeuser@fakedomain.com	2012-06-17 17:25	4.4.1 Cannot connect to remote host	jack@localhost
<debbie@localhost>	fakeuser@fakedomain.com	2012-06-16 07:08	4.4.1 Cannot connect to remote host	jack@localhost
<sarah@localhost>	fakeuser@fakedomain.com	2012-06-13 21:08	4.4.1 Cannot connect to remote host	jack@localhost
<jack@localhost>	fakeuser@fakedomain.com	2012-06-18 10:42	4.4.1 421 Too much load; please try again l...	jack@localhost

In the example above:

- » The **From** address is constantly changing and sending to `fakedomain.com`.
- » The **Authenticated Sender** is always `jack@localhost`. This could indicate that Jack's password has been compromised/guessed.

To correct this issue:

1. Change the user's password. As a precaution, change passwords of all users. For information about creating strong passwords, see [Password policy in Kerio Connect](#)
2. Run a virus/malware scan on any machine that the user has used. This should detect any possible compromise and stop spam emails from being sent via your server.

5.1.3 Browser extensions or add-ons may interfere with Kerio products

When you have trouble working with an administration or client interface of Kerio products, you can try to disable or uninstall all your browser's extensions/add-ons.

Here are some tips on how to do it in the most common browsers:

- » **Google Chrome** — Disable your extensions or run the browser in the [incognito mode](#).
- » **Mozilla Firefox** — Disable your add-ons or run the browser in [Save Mode](#).
- » **Safari** — Turn all extension off.
- » **Internet Explorer** — Disable your add-ons or run the browser in [No Add-ons mode](#).

5.1.4 Distributed Sender Blackhole List Errors (DSBL)

Issue encountered

You are seeing errors in your logs indicating a DNS failure, when checking against list. `dsbl.org` or `unconfirmed.dsbl.org` or

You are experiencing delays when receiving emails, due to slow response times, or timeouts when querying `*.dsbl.org`

Cause

The Distributed Sender Blackhole List (DSBL) has been taken offline by the owners, due to their belief that the list is obsolete. As a result, all name server queries submitted against the list will fail. You can read more about this at <http://dsbl.org>

Solution

In order to overcome the errors generated by the failed lookups, you can remove the two DSBL entries in the Blacklist setup screen:

1. Login to the Kerio Connect Administration console
2. Select: **Content Filter > Spam Filter > Blacklists**
3. Highlight the DSBL list and press Remove.
4. Repeat this for both entries of DSBL.
5. Click **Apply**.

5.1.5 How do I get older versions of Kerio software?

Sometimes it is necessary to obtain an older version of Kerio software than the current version that is offered on the main Kerio download web pages. Follow these steps to download an older version of Kerio software:

1. From a web browser on the machine on which the Kerio software will be installed, enter the following URL: <http://download.kerio.com>
2. In the Select a product or component dropdown menu, select the product you wish to download, for example, "Kerio MailServer".
3. Then in the Select a version dropdown menu, select the version of the product that you wish to download, such as "6.7.1 (released on 2009-08-05)". Click on "Show files".
4. In the listing, find the line that displays the combination of application, such as "Kerio MailServer" and platform on which the Kerio software will be installed, such as "Mac OS X". Select the Download link for your location, such as "Download - USA".
5. Save the file to the file system.

You are ready to install an older version of Kerio software.

5.1.6 How do I get the .eml source for an email?

Issue encountered

You have contacted support regarding a problem, and they have requested the ".eml" file or "email source" for a message.

Solution

The email source is easy to obtain with no need to access the mail server store folder. However, it is necessary to log into the full-featured Kerio Connect client.

1. Log into the Kerio Connect client
2. Click on the folder where the message is contained
3. Right-click on the message, then choose "View Source"

4. In the Window that pops up choose "Edit -> Select All" from the application menu
5. Copy the text and paste it into a text editor (notepad / textedit...)
6. Save this message to a file, and send it to Kerio support as requested.

5.1.7 How do I reset the password for a user if I've lost access to the WebAdmin of Kerio Connect?

If you lose your administrator account for Kerio Connect administration, you can reset it by modifying the `users.cfg` file.

Resetting the admin password

Windows

1. Stop the Kerio Connect Engine — right-click the engine monitor icon in the system tray area and select **Stop Kerio Connect**.
2. Go to the Kerio Connect installation directory. The default location is `C:\Program Files\Kerio\MailServer`.
3. [Edit the `users.cfg` file in a text editor](#).
4. Restart Kerio Connect engine.
5. Log in to the administration using an empty password.

OS X

1. Login to the system as the root user.
2. Click the **Stop** button in the Kerio Connect Monitor.
3. Go to the Kerio Connect installation directory. The default location is `/usr/local/kerio/mailserver`.
4. [Edit the `users.cfg` file in a text editor](#).
5. Restart Kerio Connect engine.
6. Log in to the administration using an empty password.

Linux

1. Stop the Kerio Connect Engine. run the following command:`/etc/init.d/kerio-connect stop`
2. Go to the Kerio Connect installation directory. The default location is `opt/kerio/mailserver`.
3. [Edit the `users.cfg` file in a text editor](#).
4. Restart Kerio Connect engine.
5. Log in to the administration using an empty password.

Editing the `users.cfg` file

1. Open the `users.cfg` file in text editor.
2. Search for the name of the admin account in the list: `<variable name="Name">`. For example: `<variable name="Name">jsmith</variable>`

3. Under the administrator's name, search for the line with <variable name="Password">. For example:
<variable name="Password">D3S:1234ab56c7de89</variable>
4. Change the "password variable to NUL:. For example:<variable name-e="Password">NUL:</variable>
5. Under the same administrator's name, search for the line with <variable name-e="Rights">0</variable>
6. Change the value from 0 to 1. For example,<variable name="Rights">1</variable>
7. Save the file.

NOTE

When you log in to the administration, create a new password right away.

Alternate Solution

1. Stop the Kerio Connect Engine.
2. Open **mailserver.cfg** in a text editor.

NOTE

In Mac, use your root account to edit.

3. Under Administration table, set BuiltInAdmin to 1
4. Change BuiltInAdminUsername to kerioadmin.
5. Delete the value set for BuiltInAdminPassword.
6. Save the file.
7. Start the Kerio Connect Server Engine. You should be able to log in using `kerioadmin` as the username without any password.
8. Go to **Webadmin >Configuration > Administration settings** and set a password.

5.1.8 Active Directory/LDAP error: Unable to search in dc=example,dc=domain,dc=com (Size limit exceeded)

When importing users from Active Directory, the import fails and returns the following error:

(8503:4) Active Directory/LDAP error: Unable to search in
dc=example,dc=domain,dc=com (Size limit exceeded)

By default, Active Directory does not respond to LDAP based queries which return more than 1000 results. If you have more than 1000 users configured in Active Directory, it is necessary to increase the maximum page size (MaxPageSize) using the Ntdsutil.exe tool.

5.1.9 How to fix a malformed journal.db with a SQLite error

This article will show you how to fix a corrupt journal.db that is being reported in the error log.

Issue encountered

The best way to see if the .journal.db needs fixing is to look for the following line in the error log:

```
[11/May/2012 10:13:33] SQLiteDbWriteCache.h: [Mail Path]/[Domain]/  
[Username]/.journal.db: runVacuum - SQLite error: code 11, error SQLITE_CORRUPT  
[11]: database disk image is malformed
```

This error normally does not cause the user any problems but it can fill the error log up with many lines of the same error.

Solution

To correct this error:

1. Stop Kerio Connect
2. Navigate to your Kerio Store folder, default paths are below:

- Windows: C:\Program Files\Kerio\MailServer\Store\Mail
- Mac: /usr/local/kerio/mailserver/store/mail
- Linux:/opt/kerio/mailserver/store/mail

4. Delete the .journal.db that is reported in the error log

5. Start Kerio Connect

This file rebuilds itself, usually instantly, but sometimes it can take a while. Note however that this should not affect the users' ability to use their email accounts.

5.1.10 How to repair or reset Anti-Virus in Kerio Connect

NOTE

Kerio Connect 9.2.2 and newer includes a new antivirus engine, Kerio Antivirus. For more information, refer to [Antivirus protection in Kerio Connect](#) (page 370).

This document will help guide you through the process of repairing your AV in Kerio Connect

To reset or repair the Anti-Virus in Kerio Connect you will need to do the following:

Windows

1. Stop Kerio Connect
2. Navigate to the installation folder, by default this will be C:\Program Files\Kerio\MailServer.
3. Then remove the folder 'keriobda', 'Sophos', the folder 'Avirs' or 'avserver' (the Avirs or avserver folder is located inside the 'plugins' folder, depending on the version of Kerio you have installed will depend on the folder name) and the avserver.exe (also located in the plugins folder).
4. Then run a repair install for the Kerio Connect installer (you will need to download a copy of the Kerio Connect installation file from the Kerio website).
5. Then start Kerio Connect.

Mac

1. Stop Kerio Connect
2. Navigate to the installation folder, by default this is /usr/local/kerio/mailserver
3. Then remove the folder 'keriobda', 'Sophos', the folder 'Avirs' or 'avserver' (the Avirs or avserver folder is located inside the 'plugins' folder, depending on the version of Kerio you have installed will depend on the folder name)

4. Then run the Kerio Connect installer and choose the option 'Easy Install' (you will need to download a copy of the Kerio Connect installation file from the Kerio website)
5. Then start Kerio Connect

Linux

1. Stop Kerio Connect
2. Navigate to the installation folder, by default this will be /opt/kerio/mailserver
3. Then remove the folder 'keriobda', 'Sophos', the folder 'Avirs' or 'avserver' (the Avirs or avserver folder is located inside the 'plugins' folder, depending on the version of Kerio you have installed will depend on the folder name)
4. Then run the Kerio Connect installer (you will need to download a copy of the Kerio Connect installation file from the Kerio website)
5. Then start Kerio Connect

Software Appliance

For the software appliance of Kerio Connect unfortunately this would require a fresh installation. You would need to do the following:

1. Make a full backup of Kerio Connect
2. Install a new version of the Kerio Connect Appliance
3. Restore from the backup

There are a few things to take into consideration with the software appliance, because the appliance is a whole package when it comes to repairing a single module it is necessary to redo the entire appliance. However you can minimize downtime if you get a new copy of the software appliance installed and ready before hand. For moving Kerio Connect to a new software appliance you can look at the following KB article to see the best practices to move the data across:

For more information, refer to [Transferring an installation of Kerio Connect to another server or Operating System](#) (page 156).

Once the reinstall is complete this will then give you a new Anti-Virus module for Kerio Connect. You will need to login to the Web Admin and update the Anti-Virus so that it can download up to date definitions.

If you have an older version of Kerio Connect then what is available from the Kerio website you can go to the legacy downloads at the following link:

<http://download.kerio.com>

This will have copies of older Kerio Connect installation files so you use the correct version for what you are using on your machine.

5.1.11 I can't send outgoing mail if I'm using Open Directory or Active Directory

Issue encountered

Some mail clients are unable to send or receive mail if the user is authenticated through Active Directory or Open Directory. Users using the "internal user database" work correctly.

Cause

Your clients are most likely using one of the two forms of MD5 authentication - CRAM-MD5 or DIGEST-MD5. However, you can not use these authentication types when users are defined in a directory service. The directory service contains

the encrypted password and the format is not compatible with these types. Communication between Kerio Connect and the directory services server is encrypted; no further encryption is necessary.

Solution

Find the option for "secure authentication" or "MD5 authentication" in your mail client and turn it off. You may also disable MD5 authentication in Kerio Connect, under **Configuration > Security > Security Policy**.

If you are concerned about the security of user credentials in transmission, we recommend you use the SSL-secured services (SMTPS, IMAPS, LDAPS, etc). Most modern mail clients support these services.

5.1.12 I can't use national characters in my password.

You use national or language specific characters in your username or password. After creating your account or changing your password, you are unable to connect to your mail account.

Only certain characters may be used in the username. For more information, refer to [Creating user accounts in Kerio Connect](#) (page 269).

If the password contains national characters, some mail clients will not be able to connect to Kerio MailServer. It is therefore recommended to use only ASCII characters for user passwords.

5.1.13 I have created a custom rule to allow an email address or domain through but it is still being blocked

Issue encountered

I have created a custom rule to allow an email address or domain through but it is still being blocked.

This article shows why creating a custom rule can sometimes not be enough to allow an email address or domain through Kerio Connect.

Solution

Creating a custom rule to allow an email address or domain through Kerio Connect on some occasions cannot be enough. A common problem with this is that the email address or domain you are trying to 'whitelist' by creating a custom rule is also on an internet blacklist. By default Kerio is set to block any email traffic that is on a blacklist that has been enabled. The way around this is to do the following:

1. Check the spam log to see which blacklist the email address or domain is being detected on
2. Then once you know which blacklist the email address or domain is on you will need to go to Configuration > Content Filter > Spam Filter > Blacklists
3. Double click on the blacklist and change the option from 'Block' to 'Add spam score to message' (You can set the score to a value you see fit or you could make it equal to your block score set in the spam filter so that the blacklist will still block other spam)
4. Then click 'OK' and apply the changes

The reason for changing the blacklist to add a score to the message instead of blocking is because the spam filter checks the blacklists before the custom rules. By setting the blacklist to add a score it allows the rest of the filtering settings to check the email.

5.1.14 I've been training the spam filter but I'm still receiving the same spam emails

Users have been training the mail server by marking messages as spam, or moving messages to the Junk Email folder, however they continue to receive the same spam emails.

Details

Kerio Connect includes a distribution of SpamAssassin, which consists primarily of two components: Static tests and dynamic tests. The tests are comprised of spam signatures that are compared to each message. A cumulative score is assigned to each message. Spam emails will receive a higher score. By default, Kerio Connect will consider any email which receives a score of 5.0 or higher to be spam.

The static tests are updated regularly, and compiled into new releases of Kerio Connect. More information regarding the specific Spamassassin tests is available on the [Spamassassin website](#).

The dynamic or Bayesian tests are adjusted over time based on user feedback. The Bayesian database is updated when a user marks a message as 'spam' or 'not spam', or moves a message from their Inbox to the Junk E-mail folder and vice versa.

It is important to understand how the Bayesian tests really work:

- » It does not outright flag messages as spam if they contain a specific subject, or sender address. It is only collecting specific characteristics of the message.
- » A message can only be flagged one time. If the same message is flagged multiple times, it will not affect anything as the dynamic tests have already been trained by that message.
- » The Bayesian tests are not active until it has received enough information. This includes a minimum of 200 spams and 200 hams (false positives).
- » The Bayesian tests are not always adjusted by user input. If a message receives a negative score, it is perceived as almost certainly NOT spam. Therefore, the entire message will be reprocessed to adjust the Bayesian tests. The same is true for the inverse situation, where a message is almost certainly spam. Any message with a score of 12.0 or greater will satisfy this condition.
- » Once the Bayesian tests are active, most messages will contain a 'bayes' score, viewable in the X-Spam-Status header.

5.1.15 Kerio Connect Client is not displayed correctly in Internet Explorer

The Kerio Connect Client can be incorrectly displayed while using Microsoft Internet Explorer in the incorrect mode.

Microsoft Internet Explorer supports several different compatibility modes; some of these modes might cause Internet Explorer to behave differently and act as the previous version (eg. Internet Explorer 10 in compatibility mode acts as Internet Explorer 7).

Compatibility mode is commonly enabled by default in following scenarios:

- » Connecting to the Kerio Connect Client from local network using the short address, eg. `http://mailserver/`.
- » When it was manually enabled in the past.

[How to disable compatibility mode view:](#)

1. Press F12 to open Developers toolbar
2. Switch the Browser mode: "Internet Explorer 10 Compatibility View" to "Internet Explorer 10" in main toolbar menu
3. Press F12 to close the Developers toolbar

5.1.16 Kerio Connect user cannot login to their email account

This article will cover common fixes for users that all of a sudden cannot login to their Kerio Connect account.

When a user cannot login to Kerio Connect client or through their email client you try the following to solve the issue:

Check if the user has a high amount of opened folders

If a user has a high amount of opened folders then this can prevent them from logging in or slow the login process down a fair bit. To check the opened folders please do the following:

1. Login to the Kerio Web Administration

2. Go to **Status > Opened Folders**

3. Check for the user who cannot login and see if they have any folders with a reference of 10 or higher

If the user does have a folder(s) with a reference count of 10 or higher then you will need to stop and start Kerio Connect. Stopping and starting Kerio Connect is the only way to kill all active connections and reset the folder count of opened folders. If the high reference count continues to return please contact your local reseller or Kerio Technical support for further help.

Check if the user has been locked out from their Kerio account

If a user has entered in their password incorrect a few times or has misconfigured an email client with the wrong password and therefore sending the wrong password to Kerio it is possible that the user has been locked out. To unlock the account please do the following:

1. Login to the Kerio Web Administration

2. Go to **Configuration > Advanced Options > Security Policy**

3. Click the button '**Unlock All Accounts Now**'

This will then unlock all accounts that have been locked, so make sure the user is entering the password correctly and that if they have configured a new connection to their Kerio email account that they are using the correct settings.

Check if the user has changed their AD or OD password.

NOTE

Active Directory/Open Directory users only

If the user has changed their AD or OD password they will need to update their email clients and mobile devices to have the same password to access their Kerio email account.

However if all users are not able to login then the AD or OD admin password that was used to bind Kerio Connect to AD or OD might have been changed and was not changed in the Kerio Web Administration first. Therefore Kerio will try to connect to AD or OD with an incorrect password and this then prevents other Kerio users being able to authenticate to AD or OD. To correct this the admin of the AD or OD machine will need to change the password saved in the Web Administration > Configuration > Domains > [Select your domain] > Directory Services.

5.1.17 Moving user from active directory service to local user database or vice versa causes synchronization errors with Outlook 2011

The user was moved from directory service to the local user database or vice versa. Outlook 2011 starts to produce error messages.

EWS error messages:

```
EwsOperation.cpp: EWS request GetItem: Message conversion failed  
(~user@domain.tld/INBOX/#msgs/00000001.eml)
```

debug log reports these messages:

```
SubscribeOperation: Subscription FAILED, Subscribe: subscribed folders don't have the same owner: first=keriodb://user/0b835b6e-997b-4eee-8209-6346c543d0b1/6cd2995d-8c5b-4e4e-9b02-832c1fa05f8 current=keriodb://user/0b835b6e-997b-4eee-8209-6346c543d0b1/6cd2995d-8c5b-4e4e-9b02-832c1fa05bbb, error code=178
```

Solution

A new Outlook 2011 profile must be created.

5.1.18 POP3 connection fails during download

Downloading mail via POP3 fails part way through. No mail is deleted, so the next download attempts to download the same mails, and fails at the same point.

Check for an abnormal message

Log into the account via the webmail interface. If there is an abnormally large email, please delete & expunge it or move it to a subfolder, and retry the POP3 download.

Check for a corrupt index

Again from the webmail interface, if you see a message like "Cannot access message 000002e5 in folder ~user@domain.com/INBOX" within the list of messages, try the following steps:

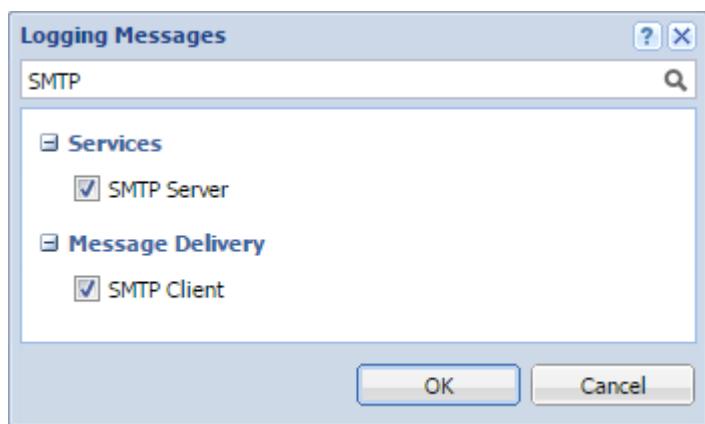
1. Ensure you are an administrator on Windows, or the root user on Linux or Mac.
2. Browse to the user's mail directory. This is normally at /store/mail/domain.com/user/INBOX/.
3. You should see a file there called "index.fld". Rename this to "index.bad".
4. Retry the POP3 download.

If you still cannot login, please contact [support](#).

5.1.19 SMTP Status and Reply codes

This article gives you a list of SMTP status codes and SMTP reply codes that can help you troubleshoot email issues within Kerio Connect.

These codes are present in **Mail log** and **Debug log**. Right-click in the **Debug** log window and select **Messages > SMTP Client**.



Below is a list of the most common codes that appear in the logs.

SMTP status codes

- » 2.0.0 – Email has been delivered to the Inbox.
- » 2.1.5 – Email has been delivered and moved to another folder due to a filtering rule.
- » 4.1.1 – Email address does not exist.
- » 4.4.1 – No answer from host or connection lost.
- » 5.1.7 – Senders email address was incorrect or has bad syntax.

SMTP Reply Codes

- » 220 – Server ready.
- » 250 – Request mail action ok.
- » 450 – Requested mail action not taken, mailbox unavailable.
- » 451 – Request action aborted.
- » 500 – Syntax error, command not recognized.
- » 550 – Requested mail action not taken, mailbox unavailable.
- » 554 – Transaction failed.

The below links show all status codes and what they represent.

- » [SMTP Reply Codes](#)
- » [SMTP Status Codes](#)

5.1.20 Users folder size is reporting incorrectly in WebAdmin

A users storage usage is incorrect in WebAdmin compared to what is being reported by the Operating System for that users folder in the store.

Solution

The storage usage for a user is calculated from a number of files within that users folder.

The first step is to remove the 'stats usr' from the users root folder. This will be recalculated and may resolve the issue.

1. Stop Kerio Connect.
2. Delete 'stats usr' from the user root folder.
3. Start Kerio Connect.

The 'stats usr' file will be re-created automatically.

NOTE

This recalculation process can take some time, so please allow a few hours before moving to the next step.

If you still have the same issue after this then the next step is to re-index the users account.

As of Kerio Connect 7.3.x it is possible to re-index an account from the WebAdmin console. Under Users select the user, then Right-click **More Actions > Re-index mailbox**

For versions of Kerio Connect prior to 7.3.0 use the following:

1. Stop Kerio Connect.
2. Rename 'index.fld' to 'index.bad', this file is in every folder and sub-folder for this user.
3. Start Kerio Connect.
4. Login to webmail as this user, this will start the re-index process.

NOTE

The re-index process will take some time as the system has to check every email and re-calculate the index file accordingly.

If your storage size is still reporting incorrect in the WebAdmin console then you will have to re-calculate the 'status.fld' file. This is not a simple process, as you can't just remove files, as the 'status.fld' contains other information that can not be automatically re-generated.

To recompute the size data in this file you will have to do the following:

1. Stop Kerio Connect.
2. Edit 'status.fld', this can be opened in any standard text editor. There is a 'status.fld' in every folder and sub-folder for this user.
3. Locate the variable 'Sxxxxx' This is the size of this folder in bytes. You can remove this variable, DO NOT alter any other variables.
4. Save the file.
5. Restart Kerio Connect.

NOTE

This users storage use will now be re-computed, again this may take some time to complete.

5.1.21 Why am I getting multiple copies of an email?

You can change this behavior in the Configuration > Delivery > POP3 Download > (Select account) > Edit > Drop duplicate messages option.

Discussion

If you use a single POP3 mailbox from your ISP for all your users, then sort them into separate mailboxes at Kerio Connect, there are some limitations to be aware of.

If you select "Drop duplicate messages" in the POP3 Account settings, then mails to multiple users on the server will only be delivered to one recipient. Alternatively, if you do not select "Drop duplicate messages" then all recipients will receive a copy for each recipient specified.

If you switch to receiving mail directly with SMTP, you will not see this issue at all. Also, you could use ETRN to collect your mail, but this must be supported by your ISP.

5.1.22 Why does Kerio Connect automatically expunge messages marked for deletion through IMAP?

When deleting or moving items through IMAP protocol, the designed behavior is to mark messages for the performed action. The resulting behavior in some IMAP clients is to display these marked messages with a strikethrough. For most users, this behavior is not preferred, so Kerio Connect compensates by automatically performing (expunging) the marked action.

In the case of Apple Mail, the user is not presented with a strikethrough, and the performed action (move/delete) appears to the user as completed, however it does not ask the server to perform the expunge action. As a consequence of Kerio Connect automatically performing the expunge action, the 'undo' option in Apple Mail does not work.

Details

To disable the automatic expunge feature, you need to manually edit the mailserver.cfg file by following these steps:

Navigate to the install directory and locate the mailserver.cfg file:

1. Open the file in a text editor and search for the string "AutoExpungeonDelete".
2. Change the default value from "1" to "0".
3. Stop the Kerio Connect Service.
4. Once Kerio Connect is completely stopped, save your changes to the file.
5. Start the Kerio Connect Service.

5.1.23 Why does the Exchange migration tool state I am not an administrator?

Why does the Exchange migration tool state I am not an administrator?

Details

One of the requirements when running the Kerio Exchange Migration Tool is that the user account you use must be an Exchange Administrator.

Check the following if migrating from Exchange 2000:

1. Go to **Start > Programs > Microsoft Exchange > System Manager**
2. Right-click on the top most folder and left-click on "Delegation Control"
3. Click "Next" on the first window
4. You should see the Exchange Administrators on the second window.
5. If the user account being used is not an Exchange administrator then you can click on the **Add** button and then the **browse** button.
6. Select the correct user account and select Exchange full administrator in the "combo menu".
7. Complete the wizard.

5.2 General errors

This section helps you resolve possible known errors.

5.2.1 Kerio Connect shows disk space warnings	430
5.2.2 550 5.7.1 Relaying to <email@address.com> denied (authentication required)	431
5.2.3 Cannot send to some mail servers with the explanation that the SMTP greeting failed	431
5.2.4 I get an error that says 'create_time < install_time'	432
5.2.5 I get the error 'Error: unable to save settings' when updating settings in the old Webmail	432
5.2.6 I'm receiving errors and bounces when sending email, what do they mean?	433

5.2.7 I receive a 'script error' message	433
5.2.8 I receive the error "Failed to detect the installation setup requirements (code: -5)" when I install the Outlook Connector.	434
5.2.9 Login problem on 64bit Windows when using Kerberos	434
5.2.10 Message body is garbled when email is received by Microsoft Exchange server	435
5.2.11 My Calendar/Contacts/Tasks/Notes folders are now showing as Mail folders. How do I fix this?	436
5.2.12 Outlook generates MAPI_E_TIMEOUT error during certain operations	436
5.2.13 Some POP3 clients generate an authentication error in the security log, but successfully download new email	437
5.2.14 Some services, for example WebMail, do not start. How do I fix this?	437
5.2.15 Why am I getting multiple copies of an email?	438
5.2.16 Why do I see 'IP address x.x.x.x rejected: too many connections' in the warning log?	438
5.2.17 Why is a new attendee created when the original attendee accepts a meeting invitation?	439

5.2.1 Kerio Connect shows disk space warnings

Issues encountered

One of the following issues is encountered:

- » The administration interface shows a warning message indicating that disk space is low.
- » Kerio Connect stops working and the administration interface shows a warning message indicating that disk space is too low.

Cause

These issues are encountered when the free space of the disk drive where the Kerio Connect data store is saved, is running low. Kerio Connect stops working when the data store disk space is running critically low.

NOTE

The parameters for these limits are configurable from the administration interface. For more information, refer to [Setting the data store notification limits](#) (page 178).

Possible solutions

The recommended solution is to move the Kerio Connect data store to a larger disk. Consider the long-term disk requirements to determine the minimum disk size required by your organization and minimize the chance of re-encountering this issue in the future.

If using a Kerio Connect virtual appliance, you may first add another disk partition to your appliance and then move the data store to the new partition.

To move the message store to the new drive:

1. Create a new virtual disk for your Kerio Connect virtual appliance on VMware. Click [here](#) for information on how to perform this operation.

2. When the new virtual disk is created, create a new directory on the new partition for the Kerio Connect data store. Do not use diacritics in the directory name or path.
3. In the Kerio Connect administration interface, go to **Configuration > Advanced Options > Store Directory**.
4. Select the new folder in the new location. Do not use a UNC path. Click **Apply**.
5. Stop Kerio Connect.
6. Copy all files from the old store directory to the new directory.
7. Run Kerio Connect.

5.2.2 550 5.7.1 Relaying to <email@address.com> denied (authentication required)

Below are two options to look at in the Administration Console for a possible misconfigured setting.

1. Verify the relay control settings within the Administration Console. Navigate to Configuration > SMTP Server > Relay Control.

A brief description of each option:

- **Users from IP Address Group.** This option allows SMTP relaying if the traffic originates from an IP address contained within the selected IP Address Group.
- **Users authenticated through SMTP for outgoing mail.** This option requires the user's mail client to supply a user name and password for all the outgoing mail.
- **Users previously authenticated through POP3 from the same IP address (POP3 before SMTP).** This option requires the user's mail client to check for new POP mail and authenticate before trying to send any outgoing messages.

2. Verify the SMTP service has not been restricted to an IP Address Group.

- a. Navigate to **Configuration > Services**
- b. Double-click on the SMTP service
- c. Click on the Access tab

If an IP Address Group has been selected then disable that option, apply the change and then ask the user to try sending another email.

5.2.3 Cannot send to some mail servers with the explanation that the SMTP greeting failed

Issue encountered

Users report that some messages are returned with the explanation that the SMTP greeting failed because no valid DNS name or pointer record was identified.

Causes

When a message is sent through SMTP, the client and server are expected to identify each other. This identification is part of the SMTP greeting.

The following example is a simplified version of a mail server (mail.sender.com) successfully transmitting a message to user@recipient.com:

1. mail.sender.com connects to mail.recipient.com
2. mail.recipient.com accepts the connection and identifies itself "Hello, I'm mail.recipient.com".

3. mail.sender.com identifies itself "Hello, I'm mail.sender.com".
4. mail.recipient.com acknowledges mail.sender.com and says, "OK, give me your message".

In the above example, mail.recipient.com has allowed mail.sender.com to transmit the message. In order to prevent spam, some mail servers will validate the name provided by the connecting mail server before allowing the message to be transmitted. The following example is similar to above, however mail.sender.com will provide a false name, and therefore mail.recipient.com will refuse to accept the message.

1. mail.sender.com connects to mail.recipient.com
2. mail.recipient.com accepts the connection and identifies itself "Hello, I'm mail.recipient.com".
3. mail.sender.com identifies itself "Hello, I'm mail.anothersender.com".
4. mail.recipient.com determines that mail.anothersender.com is someone else, or does not exist and says, "You are not who you say you are, Goodbye".

mail.sender.com will then return the email to the original sender address, quoting the reason why it could not deliver the message.

For example:

I'm sorry but I could not deliver your message. The remote mailserver (mail.recipient.com) says: "You are not who you say you are, Goodbye"

Solution

Set the Internet hostname (e.g. mail.domain.com) of the mail server in **Configuration > Domains > 'Internet hostname'**. This domain name must resolve to the Internet IP address used by Kerio MailServer for Internet communication.

5.2.4 I get an error that says 'create_time < install_time'

Issue encountered

I get an error that says 'create_time < install_time'

Cause

You are running the 30 day trial of Kerio Connect, and have either moved data from a different machine or reinstalled the software. The timestamps for your files and your install date do not match. Kerio detects this as an attempt to subvert the 30 day trial. There are no other reasons for this to happen.

Solution

Please contact our sales department for a trial extension key.

5.2.5 I get the error 'Error: unable to save settings' when updating settings in the old Webmail

This problem is typically caused by a corrupted user setting file. This problem can be resolved by deleting this file.

1. The user should close Outlook, any other mail applications, and WebMail.
2. On the mail server, go to the user's mail directory.
3. Find the `settings usr` file, and delete it.

The user should then be able to log in and not experience this error. If the error persists, [contact Kerio Support](#).

5.2.6 I'm receiving errors and bounces when sending email, what do they mean?

You have users who complain that emails are not being delivered. Emails are rejected with errors from the Kerio Connect server and make mention of "RBL" or "blacklist" errors.

Errors are typically of the form:

- » Spam blocked see: <http://spamcop.net/bl.shtml?192.168.203.234>
- » 554 Service unavailable; Client host [192.168.203.234] blocked using blackholes.five-ten-sg.com
- » 192.168.203.234 blocked - see <http://www.spamhaus.org/query/bl?ip=192.168.203.234>

Solution

These errors appear to be sent from Kerio Connect, but they are not. They are errors other mail servers returned to Kerio Connect while trying to relay your outgoing mail. Kerio Connect is simply passing the errors back to the sender. The remote mail server reporting the error should be mentioned somewhere in the error message usually as a internet name or an IP address or both. The most important information from these errors is the name of the RBL you are reportedly listed on.

Your mail server IP addresses is likely listed on other RBL (Realtime Black List) lists also. A RBL is a DNS service that provides a reverse lookup on IPs that have been reported as SPAM sources or open relays. It is likely that you are mistakenly listed, or your mail server is configured with an open relay and is visible on the internet.

Determine which RBLs your IP is listed on

Find out which RBLs your IP address is listed on so you can take steps to remove yourself. Use an RBL checker such as the one at rbls.org. There are plenty of RBL checkers on the internet. They are an essential tool for this kind of troubleshooting.

Take steps to get removed from the RBLs

If an IP address is listed on an RBL, that RBL must be dealt with on an individual basis. They are individually maintained by various organizations and companies. They each have a website you can visit or contact information with instructions on how to request list removal.

Check the IP for open relay

If the mail server has is open relay, it's internet IP address will constantly be listed on RBL lists. They will usually remove the IP at your request, but it won't take long to be listed again unless the open relay is fixed.

To identify if you are an open relay, refer to KB [Detecting that Kerio Connect has been compromised and used for spamming](#).

Check for private blacklist

Finally, if you are not listed on any known RBL list, it is possible you are listed in the remote mail server's private blacklist. Some ISP's have aggressive private blacklists that might accidentally include small domains who are innocent. Fix this by contacting the postmaster at the remote domain and ask to be removed. Mail servers typically accept email sent to postmaster@domainname. Sometimes the bounce message contains specific information on how to be removed so read the message carefully. It might be necessary to send any email to the remote domain from another email address outside of the blacklisted domain.

5.2.7 I receive a 'script error' message

When you receive new mail, or attempt to edit the mail filtering rules, you receive a "script error" message.

Your mail filtering script has become corrupted. In order to fix this, delete the filter file.

1. Close Outlook or WebMail.
2. On the server hosting Kerio MailServer, go to the mail store directory:

- Windows: C:\Program Files\Kerio\MailServer\store\mail
- OS X: /usr/local/kerio/mailserver/store/mail
- Linux: /opt/kerio/mailserver/store/mail

3. Go to the user's directory: domain/user - eg.us.kerio.com/jthomas.

4. You will see a `filter.siv` file. Delete this file.

On the next start of Outlook or WebMail this problem should be gone.

NOTE

This procedure removes any custom mail filtering rules you have created.

5.2.8 I receive the error "Failed to detect the installation setup requirements (code: -5)" when I install the Outlook Connector.

If you receive the error Failed to detect the installation setup requirements (code: -5) when installing the Outlook Connector, you may be running Outlook 2000 in "Internet only" mode. To fix this, re-enable Groupware mode.

1. Open the Tools menu, and select Options > Mail Services > Reconfigure Mail Support. Choose either "Corporate" or "Workgroups".

2. Close Outlook.

You should now be able to install Kerio Outlook Connector.

5.2.9 Login problem on 64bit Windows when using Kerberos

Issue encountered

This article applies only to Windows 64-bit system, 32-bit versions of Windows do not require these steps for Kerio MailServer user authentication.

This problem occurs when all of the following are true:

1. When users are mapped from some Unix KDC (eg. OpenDirectory) according to the following [Microsoft's Knowledge Base article](#)
2. Kerberos authentication enabled
3. Users are not mapped to local database (using "ksetup /mapuser ldapuser@REALM localuser")

Then they cannot authenticate even their username and password is correct. Warning log reports a problem similar to `Authenticating user xxx failed, error codes c000006d, 0, (1326) Logon failure: unknown user name or bad password.`

Cause

This problem is based on current API limitations.

Solutions

To solve this problem, you must map LDAP users to local user accounts. The solution is divided into two parts, the OpenDirectory part and the MS Windows part. We used COMPANY.COM as a realm in following example.

Apple Open Directory configuration

1. Open Workgroup manager and switch to the user management. You will see a list of users stored in the directory service.
2. Create some testing user in the directory service, for example testuser account.
3. Run kadmin or kadmin.local again and verify that the user (Principal Name) `testuser@COMPANY.COM` was created using the `listprincs` command.

MS Windows configuration

1. Now we can map the Open Directory users (authenticated via Kerberos5) to the Windows local users. The Open Directory user has testuser login name, create the same user locally in Windows.
2. Open the Support Tools command line again and run `ksetup /mapuser testuser@COMPANY.COM testuser`
3. The user mapping can be done several times, each run of `ksetup /mapuser` adds a new user mapping. Do it for all user accounts. See example below:

```
ksetup /mapuser diradmin@COMPANY.COM administrator  
ksetup /mapuser user1@COMPANY.COM user1  
ksetup /mapuser user2@COMPANY.COM user1  
ksetup /mapuser *@COMPANY.COM anotheruser  
ksetup /mapuser * guest
```

The diradmin will be mapped to the local administrator account on Windows, user1 and user2 accounts will be mapped to the user1 local account on Windows machine. The other accounts from the COMPANY.COM realm will be mapped to anotheruser account. Accounts from another Kerberos realms will be mapped to the local windows guest account.

If the directory service username matches the windows local one, it's a good practice to set some random password for the local user account to be sure the authentication runs via Kerberos (local account can be used instead of Kerberos one if the password is same for the Kerberos and the local account).

5.2.10 Message body is garbled when email is received by Microsoft Exchange server

This is a known Microsoft issue caused by the email message format. When the email message uses different encoding in email header and different encoding in email body, the message body becomes garbled because Outlook uses header encoding to parse the entire email message. This can also happen when the message body contains multiple parts each using different encoding (character set). More details can be found in following Microsoft's knowledge base article:

[The body of an e-mail message is garbled when the message is viewed in Outlook in an Exchange Server 2003 organization](#)

5.2.11 My Calendar/Contacts/Tasks/Notes folders are now showing as Mail folders. How do I fix this?

Issue encountered

My Calendar/Contacts/Tasks/Notes folders are now showing as Mail folders. How do I fix this?

Cause

This folder might have the wrong folder type associated with it.

Solution

On the mailserver system, go to this directory:

- » (Windows) C:\Program Files\Kerio\MailServer\store\mail\[domain]\[user]\
- » (Linux) /opt/kerio/mailserver/store/mail/[domain]/[user]/
- » (OS X) /usr/local/kerio/mailserver/store/mail/[domain]/[user]/

Where [domain] is your email domain name and [user] is the username of the user with the folder issue. Then, go into the folder with the incorrect folder type.

Edit the status.fld file with a text editor and look at the very first line of the file. The first line will be the letter T and some number. This number determines the folder type.

Folder types:

- » T0 = mail folder
- » T1 = contacts
- » T2 = calendar
- » T3 = tasks
- » T5 = notes

Please remember to save the Status.fld file after you have finished modifying it.

If the folder type specified in the folder is wrong then change the number to the correct value. Don't make any other changes to the file. Log into webmail again and see if that fixes the error.

NOTE

This also fixes problem starting Microsoft Outlook. If Outlook tells you your folders are corrupt, or that the data store could not be opened, try changing your fixing the status.fld file in your contacts, calendar, and tasks folders. That should fix the problem.

5.2.12 Outlook generates MAPI_E_TIMEOUT error during certain operations

Issue encountered

You receive one of the following errors:

0x80041204:er_network_timeout
0x80040401: MAPI_E_TIMEOUT

0x80048002: 'This task was cancelled before it was completed.'

Solution

One common cause of these problems is the Exchange Extension property pages Add-In of Outlook. This should be disabled.

Go to Outlook's **Options > Other tab > "Advanced Options" > "Add-In Manager"** and disable 'Exchange Extension property pages'.

Restart Outlook after making these changes. If you continue to experience problems, please report them to [Kerio Support](#).

5.2.13 Some POP3 clients generate an authentication error in the security log, but successfully download new email

Issue encountered

The security log is reporting the following event:

```
[19/Jul/2006 16:46:47] Failed POP3 login from 10.0.0.187, user someone@domain.com
```

Cause

Typically this simply means that the user provided the wrong password. In some cases, you may find that the mail client doesn't report any problems, and successfully downloads new email. This is because the mail client tries to use a secure authentication method that fails, so it switches to insecure authentication.

Solution

In most cases, the client should be able to use secure authentication. There are some circumstances however, when secure authentication cannot be used.

Password is stored in SHA format

In the edit dialog of any user, there is a checkbox to store user passwords in SHA format. If this option is selected, the client will not be able to use any type of secure authentication method. It is recommended therefore to use an SSL connection and Plain Authentication.

Users are mapped from a Directory Service

If Kerio MailServer is mapping users from a Directory Service, the password is managed by the Directory Server. In order to verify credentials against the Directory Server, Kerio Connect must receive the password in Plain Text. To ensure secure communication, it is recommended to use an SSL connection between the mail client and Kerio Connect. The communication between Kerio Connect and the Directory Server is secured by Kerberos.

5.2.14 Some services, for example WebMail, do not start. How do I fix this?

Issue encountered

One or more services do not start, despite being set to Automatic start. The error log shows something like:

```
[27/Feb/2004 12:04:46] socklib.cpp: Bind to port 80 failed: (10048) Only one usage  
of each socket address (protocol/network address/port) is normally permitted.
```

```
[27/Feb/2004 12:04:46] services.cpp: Cannot start service WEBMAIL on port 80
```

Cause

Only one application can run on a single port at a time. The WebMail service runs on port 80, which is the standard port for web servers. If you have a web server on your computer, eg IIS or Apache, this may be using the port.

Solution

You can either change the port the WebMail runs on, or identify what else is using the port, and set that to use another port.

Changing the port in the MailServer

Go to **Configuration > Services**. Select the service that is not starting, and click "Edit". Change the port to a different number.

Identifying the other server

1. On Windows XP you can use the command `netstat -a -n -o` to determine the ID number of the process using this port. For Windows NT/2000, download the [TCPView](#) tool from SysInternals.

2. Refer to the task manager to see which ID is associated with the process. The task manager is accessed by pressing **ctrl + alt + del**.

3. Select the processes tab.

4. From the top menu, choose **view > select columns**.

5. Enable the PID column and click **ok**

6. Once you have identified the process, determine if this program can use a port other than the default, or consider removing the conflicting application.

5.2.15 Why am I getting multiple copies of an email?

This can occur when using the POP3 download feature in Kerio Connect.

You can change this behavior in the **Configuration > POP3 Download > (Select account) > Edit > Drop duplicate messages** option.

If you use a single POP3 mailbox from your ISP for all your users, then sort them into separate mailboxes in Kerio Connect, there are some limitations to be aware of.

If you select "Drop duplicate messages" in the POP3 Account settings, then mails to multiple users on the server will only be delivered to one recipient. Alternatively, if you do not select **Drop duplicate messages** then all recipients will receive a copy for each recipient specified.

If you switch to receiving mail directly with SMTP, you will not see this issue at all. Also, you could use ETRN to collect your mail, but this must be supported by your ISP.

5.2.16 Why do I see 'IP address xxxx rejected: too many connections' in the warning log?

This message, **Connection attempt to service IMAP from IP address x.x.x.x rejected: too many connections**.

Connection limit is 100, indicates that the IMAP service in Kerio Connect has received the maximum number of allowed connections per IP address. This may occur NAT scenarios, where Kerio Connect receives all of the connections from a single IP address. The max connections per IP setting is not adjustable from within the Administration Console. For this reason, our recommendation is to contact technical support so that we may assist you in resolving this issue.

Please visit our [support center](#) to submit a ticket to technical support.

5.2.17 Why is a new attendee created when the original attendee accepts a meeting invitation?

Issue encountered

In Outlook, create a meeting and invite an attendee. The attendee will receive this invitation and receive the option to accept or decline and send the response back. Under certain circumstances, when the response is received it will create a new attendee in the event instead of updating the original attendee.

Outlook (not KOC) matches an attendee by her whole name e.g. "John Smith <john.smith@domain.com>" not only by <john.smith@domain.com>. That means if you invite John and he has set his whole name as "Johny <john.smith@domain.com>" and answers you, then you will encounter this problem because "John Smith <john.smith@domain.com>" is not the same text as "Johny <john.smith@domain.com>" .

Solution

This behavior is a problem of Outlook. It occurs for all supported versions of Microsoft Outlook - 2000, XP and 2003.

Because Microsoft has not fixed this problem we only have a workaround for this issue.

To prevent this issue, only use the addresses from the Public Contacts address book when sending an invitation. Do not enter the mail address manually. You will also wish to disallow your users from overriding their email addresses and names in KOC's dialogue.

5.3 Vulnerabilities

Vulnerability	Description
Bash vulnerability CVE-2014-6271, CVE-2014-7169 (ShellShock)	The shellshock vulnerability (aka CVE-2014-6271 and CVE-2014-7169) is a security bug affecting Unix-like operating systems through the Bash shell. For information on its impact on Kerio products, read Bash vulnerability CVE-2014-6271, CVE-2014-7169 (ShellShock) article.
Linux Glibc vulnerability CVE-2015-7547	A vulnerability in the Linux glibc system library has been found. An attacker can gain root access to the server and execute a code. For more details on its impact on Kerio products, read Linux Glibc vulnerability CVE-2015-7547 article.
Linux vulnerability CVE-2015-0235 (GHOST)	There is a vulnerability in Linux glibc system library. An attacker can exploit this vulnerability and gain root access to your server and execute a code. For more details on its impact on Kerio products, read Linux vulnerability CVE-2015-0235 (GHOST) article.
OpenSSL vulnerability CVE-2014-0160 (Heartbleed)	The National Institute of Standards and Technology (NIST) has published a vulnerability to OpenSSL 1.0.1. Details regarding the vulnerability are available from the NIST website . Kerio Connect 8.2.0 up to 8.2.3 used the affected version of the OpenSSL library. However, a fix is available for Kerio Connect as of version 8.2.4. You can download this release from the Kerio Website . For additional information and security precautions, read OpenSSL vulnerability CVE-2014-0160 article.
SSL 3.0 vulnerability CVE-2014-3566 and POODLE	This vulnerability is a flaw in the protocol design. An attacker that controls the network between the client and the server can interfere with any attempted handshake offering TLS 1.0 or later and force both client and server to use SSL 3.0 protocol instead. They can then use other attack techniques (eg. BEAST attack) to decipher transmitted data. For information on its impact on Kerio products, read SSL 3.0 vulnerability CVE-2014-3566 (POODLE) article.

6 Glossary

A

Active directory

A directory service for Windows domain networks.

B

BYOD

Bring your own device - a company strategy for using employees' personal devices for work.

C

CalDAV

Calendaring extension to WebDAV that enables you to synchronize calendars.

Caller ID

A DNS based test that filters out messages with fake sender addresses.

CardDAV

vCard Extensions to WebDAV that enables you to synchronize contacts.

Certification authority

Issues digital certificates that prove the legitimate owner.

Click to Call

A feature of Kerio Connect Client that enables you to call any number from a message or from contact details just by clicking the number.

Clickjacking

A malicious technique that makes user click on something different than they expect.

CNAME record

Canonical Name record is a record in DNS that specifies an alias of the domain name.

D

DHCP

Dynamic Host Configuration Protocol - A protocol that automatically gives IP addresses and additional configuration to hosts in a network.

Directory harvest

An attack that spammers use to discover existent email addresses.

DKIM

DomainKeys Identified Mail - An authentication method that signs outgoing messages from Kerio Connect with a special signature for identification.

DNS

Domain Name System - Enables the translation of hostnames to IP addresses and provides other domain related information.

domain controller

A server that runs the authentication process in Microsoft Active Directory.

DoS

Denial of Service - An attack that can overload the server and makes it unavailable to users.

E

EAS

Exchange ActiveSync - A protocol that synchronizes data with computers and mobile devices.

ETRN

Extended Turn is an extension to SMTP that enables you to forward messages to another SMTP server.

EWS

Exchange Web Services - Web services that enables applications to communicate with an Exchange server.

Exchange ActiveSync

A protocol that synchronizes data with computers and mobile devices.

G

Greylisting

Greylisting is an antispam method that temporarily rejects messages from unknown senders.

H

HTTP

Hypertext Transfer Protocol - A protocol for exchange of hypertext documents in HTML.

HTTPS

Secure version of secured by SSL.

I

IM

Instant Messaging - A real-time online chat.

IMAP

Internet Message Access Protocol - One of the two most commonly used Internet standard protocols for e-mail retrieval, the other being POP3.

Instant Messaging

Instant messaging is a real-time online chat.

Internet Service Provider

An organization that can provide Internet service.

IP address

An identifier assigned to devices connected to a TCP/IP network.

ISP

Internet Service Provider - an organization that can provide Internet service.

K

Kerberos

An authentication protocol for client/server applications.

Kerio Anti-spam

A proprietary antispam engine that uses Bitdefender online scanning service.

Kerio Antivirus

An integrated antivirus engine powered by Bitdefender.

Kerio Cloud

A secure messaging and voice service provided by Kerio Technologies.

L

LDAP

Lightweight Directory Access Protocol - A protocol that enables users to access centrally managed contacts.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol enables users to access centrally managed contacts.

M

Multitenancy

Deployment option where you can host multiple independent organizations or tenants on a single Kerio Connect server.

MX record

Mail Exchanger record is a record in DNS that specifies which server handles email messages.

MyKerio

Web-based application for monitoring and managing appliances of Kerio products.

N

NNTP

Network News Transfer Protocol - A transfer protocol for discussion groups over the Internet.

NTLM

NT LAN Manager - Security protocols that provide authentication for Windows networks.

O

Open directory

A directory service for Apple based networks.

P

PCI DSS

Payment Card Industry Data Security Standard - A set of security standards for organizations to securely process and store data of credit cards.

POP3

Post Office Protocol 3 - A protocol used by local email clients to retrieve emails from mailboxes over a TCP/IP connection.

Public folder

A common folder that allows users to share information.

R

regular expression

Enables to define a sequence of characters that specify a search pattern.

root certificate

A certificate issued by a trusted certificate authority (CA). In the SSL, anyone can generate a signing key and sign a new certificate.

S

S/MIME

Secure/Multipurpose Internet Mail Extensions - Email protocol based on SMTP used to digitally sign and encrypt messages.

SMTP

Simple Mail Transport Protocol - An internet standard used for email transmission across IP networks.

SNMP

Simple Network Management Protocol - A protocol for gathering and organizing information about devices in IP networks, and changing devices behavior.

SPF

Sender Policy Framework is an open source equivalent to Caller ID.

SRV record

Service record is a record in DNS that specifies the location of server for individual services.

SSH

Secure Socket Shell - A network protocol that provides administrators with a secure way to access a remote machines.

SSL

Secure Sockets Layer - A protocol that ensures integral and secure communication between networks.

SSL certificate

SSL certificates are used to authenticate an identity on a server.

T

TCP

Transmission Control Protocol - ensures packet transmission.

TLS

Transport Layer Security - A follower of the SSL protocol and ensures secure communication between networks.

U

UNC path

A standard that specifies the location path of a network resource.

URL

Uniform Resource Locator is the address of a web page on the world wide web.

V

Virtual Appliance

Pre-configured Kerio Connect virtual machine image for VMware.

W

WebDAV

Web Distributed Authoring and Versioning is a framework that enables users to work with documents on a server.

X

XMPP

Extensible Messaging and Presence Protocol is a protocol used for real-time communication (chat).

7 Legal notices

7.1 Trademarks and registered trademarks

Microsoft®, Windows®, Windows NT®, Windows Vista®, Internet Explorer®, Active Directory®, Outlook®, ActiveSync®, Entourage® and Windows Mobile® are registered trademarks of Microsoft Corporation.

Apple®, iCal®, macOS®, Mac OS®, OS X®, Safari™, Tiger™, Panther®, Open Directory logo™, Leopard®, Snow Leopard® and Lion® are registered trademarks or trademarks of Apple, Inc.

Palm®, Treo™, Pre™ and VersaMail® are registered trademarks or trademarks of Palm, Inc.

Red Hat® and Fedora™ are registered trademarks or trademarks of Red Hat, Inc.

SUSE®, openSUSE® and the openSUSE logo are registered trademarks or trademarks of Novell, Inc.

Mozilla® and Firefox® are registered trademarks of Mozilla Foundation.

Linux® is registered trademark of Linus Torvalds.

Kerberos™ is trademark of Massachusetts Institute of Technology (MIT).

avast!® is registered trademark of AVAST Software.

eTrust™ is trademark of Computer Associates International, Inc.

ClamAV™ is trademark of Tomasz Kojm.

Cybertrust® is registered trademark of Cybertrust Holdings, Inc. and/or their filials.

Thawte® is registered trademark of VeriSign, Inc.

Entrust® is registered trademark of Entrust, Inc.

Sophos® is registered trademark of Sophos Plc.

ESET® and NOD32® are registered trademarks of ESET, LLC.

AVG® is registered trademark of AVG Technologies.

IOS® is registered trademark of Cisco Systems, Inc.

NotifyLink® is registered trademark of Notify Technology Corporation.

BlackBerry® is registered trademark of Research In Motion Limited (RIM).

RoadSync™ is trademark of DataViz Inc.

Nokia® and Mail for Exchange® are registered trademarks of Nokia Corporation.

Symbian™ is trademark of Symbian Software Limited.

Sony Ericsson® is registered trademark of Sony Ericsson Mobile Communications AB.

SpamAssassin™ is trademark of Apache Software Foundation.

SpamHAUS® is registered trademark of The Spamhaus Project Ltd.

Android™ and Nexus One™ are trademarks of Google Inc. This trademark can be used only in accord with [Google Permissions](#).

DROID™ is trademark of Lucasfilm Ltd. and affiliated companies.

Motorola® is registered trademark of Motorola, Inc.

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.

7.2 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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

libIDL

LibIDL is a front-end for CORBA 2.2 IDL and Netscape's XPIIDL.

Copyright © 1998, 1999 Andrew T. Veliahi.

libdkim++

libdkim++ is a lightweight and portable DKIM (RFC4871) library for *NIX, supporting both signing and SMDID/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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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://download.kerio.com/archive/>

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 Auldrige

Copyright ©1999-2005 The Apache Software Foundation.

Tigase

The Tigase Jabber/XMPP Server is Open Source and Free (GPLv3) {Java} based server.

Copyright © 2004 Tigase.org. <<http://www.tigase.org/>>

Copyright © 2001-2006 Tigase Developers Team. All rights Reserved.

Copyright © 2004-2011 "Artur Hefczyc" <artur.hefczyc@tigase.org>

Copyright © 2009 "Tomasz Sterna" <tomek@xiaoka.com>

Copyright © 2001-2008 Julien Ponge, All Rights Reserved.

Copyright © 2008 "Bartosz M. Małkowski" <bartosz.malkowski@tigase.org>

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.