Kerio Workspace

Kerio Workspace Administrator’s Guide

Kerio Technologies

Contents

Creating user accounts in Kerio Workspace 6

What are user accounts 6

Creating new user accounts 6

Adding new local account 6

Adding accounts from a directory service 7

How to activate users from a directory service 7

Removing users 7

Additional settings 7

Creating groups in Kerio Workspace 8

What are user groups 8

Creating user groups 8

Creating a new local user group 8

Adding user groups from directory service 8

Activating user groups from directory services 9

Removing user groups 9

Additional settings 9

Setting administration access rights 10

What are the levels of access rights 10

Access to administration 10

Access to all content 10

How to set access rights 10

Transferring access rights of deleted users and groups 11

Using SSL certificates 12

What are SSL certificates 12

How to add certificate 12

How to create new certificate 12

How to get and apply certificate signed by certification authority . . . 13

More settings for SSL certificates 13

Connecting Kerio Workspace to directory service 14

Which directory services Kerio Workspace supports 14

What is the connection used for 14

How to connect to directory service 15

Microsoft Active Directory 15

Apple Open Directory 15

Setting email communication 17

When does Kerio Workspace send email messages 17
How to set sender address 17
How to configure the SMTP server 17
What are the requirements for receiving email messages 17

Displaying information about active connections 18
Displaying information about active connections 18

Managing data stored in Kerio Workspace 19
How to manage data store 19

Managing logs in Kerio Workspace 22
What are logs in Kerio Workspace 22
Logs Settings 22
Types of logs in Kerio Workspace 23
Activity 23
Config 23
Security 23
Warning 23
Error 23
Server log 24

Changing ports and redirecting all traffic to secure connection 25
How to solve the problem with several HTTP servers on one computer? 25
Virtualization 25
How to change the ports 25
How to force secure connection 26

Login to Kerio Workspace 27
Which Kerio Workspace interfaces are available 27
Kerio Workspace Administration 27
How to login 27
First login 28
Kerio Workspace client 28
How to login to Kerio Workspace client 28

Restoring Kerio Workspace from backup 30
How to create and schedule backups 30
How to restore Kerio Workspace from backup 30

Updating Kerio Workspace 32
How to check for new versions 32
How to install new version 32

Kerio Workspace VMware Virtual Appliance 33
What is Kerio Workspace VMware Virtual Appliance for 33
How to get Kerio Workspace Virtual Appliance 33
Working with Kerio Workspace VMware Virtual Appliance 33
Network configuration 34
Time zone settings 35
Updating Kerio Workspace 35

Creating user accounts in Kerio Workspace

What are user accounts

User accounts in Kerio Workspace are used for:

- setting access rights to:
  - spaces and pages,
  - administration,
- logging users to Kerio Workspace,
- setting user email addresses used for sending *news feeds* from your Workspace.

Creating new user accounts

Users with the Admin role can create additional groups in Kerio Workspace.

You can add either new local accounts or existing accounts from a directory service.

Adding new local account

If you do not use directory services, create a local user in Kerio Workspace administration.

1. In Kerio Workspace administration, go to section **Accounts** → **Users**.
2. Click on **Add** → **Add local**.
3. Enter username.

   > Do not use spaces, national and special characters.

4. Enter user's email address so that they can receive news feed from their favorite pages.
5. Decide whether the user will be allowed to change their password
6. On tab **Rights**, set access rights to the administration.
7. Save the settings.

Adding accounts from a directory service

You need basic login credentials to connect the directory service to Kerio Workspace.

To add users from a directory service, you need to:

- to set mapping from directory service
- activate users

How to activate users from a directory service

1. In Kerio Workspace administration, go to section **Accounts** → **Users**.
2. Click on the **Add** → **Add from Directory Service** option.
3. Select users you wish to connect with Kerio Workspace.

Users from directory services have a special icon. You cannot edit these users in Kerio Workspace. Any changes must be done in the directory service.

Removing users

The **Remove** button removes the selected user. Since users have created their content in Kerio Workspace and have rights to other content, you need to decide what to do the access rights once you delete the user:

- **Do not transfer rights**
- **Transfer sharing rights to another user or group** — select a user/group to inherit the rights

No matter which option you select, the content will still be available in Kerio Workspace.
If you do not transfer the rights to anyone and no other users has rights for access to the specific content, you can use the Content admin function.

Additional settings

Users can be assigned access rights to administration. These settings are described in a separate article.

Information about adding, removing or editing users can be found in the Config log.

Creating groups in Kerio Workspace

What are user groups

User groups in Kerio Workspace are used for:

- setting access rights to:
    - spaces and pages,
    - administration.

Creating user groups

Kerio Workspace offers one default group - **Whole organization.**

Users with the Admin role can create additional groups in Kerio Workspace.

You can add either new local user group or existing user group from a directory service.

Creating a new local user group

If you do not use directory services, create a local user group in Kerio Workspace administration.

1. In Kerio Workspace administration, go to section **Accounts** → **Groups**.
2. Click on **Add** → **Add local**.
3. Enter name for the group.

> Do not use special characters.

4. On tab **Members**, add users/groups.
5. On tab **Rights**, set access rights to the administration.
6. Save the settings.

Adding user groups from directory service

You need basic login credentials to connect the directory service to Kerio Workspace.

To add user groups from a directory service, you need to:

- set mapping from directory service
- activate groups

Activating user groups from directory services

1. In Kerio Workspace administration, go to section **Accounts** → **Groups**.
2. Click on the **Add** → **Add from Directory Service** option.
3. Select user groups you wish to connect with Kerio Workspace.

User groups from directory services have a special icon. You cannot edit these groups in Kerio Workspace. Any changes must be done in the directory service.

Removing user groups

The **Remove** button removes the selected group. Since group have sharing rights set, you need to decide what to do the access rights once you delete the group:

- **Do not transfer rights**
- **Transfer sharing rights to another user or group** — select a user/group to inherit the rights

> No matter which option you select, the content will still be available in Kerio Workspace.
> If you do not transfer the rights to anyone and no other users has rights for access to the specific content, you can use the Content manager function.

Additional settings

Groups can be assigned access rights to the administration. These settings are described in a separate article.

Information about adding, removing or editing user groups can be found in the Config log.

Setting administration access rights

What are the levels of access rights

There are two types of access rights for users and groups:

- access to administration
- access to all content

Access to administration

Administration access right have the following levels in Kerio Workspace:

- **Full access to administration** — user have read and write rights to administration (they can add and delete users and change all other settings in Kerio Workspace)
- **Read-only access to administration** — user can view Kerio Workspace settings but cannot change it
- **No access to administration** — user cannot access the Kerio Workspace administration

Access to all content

Content Manager is a special level of access rights — user with such right can view and manage all content (spaces, pages) in Kerio Workspace.

Content manager can review all activities and content in Kerio Workspace enabling them to prevent users from illegal activities (uploading protected content), from exploiting the server (uploading large files) and so on.

How to set access rights

In Kerio Workspace administration, go to user settings to tab **Rights** and select the level of administration access rights. You can also check the **Allow user to administer all content** option.

If you set the rights for a group, they will apply to all its members.

If user is member of a group and access rights for the user and group differ, the higher level of access rights applies.

To administer all content in Kerio Workspace, users have to use the option in the menu available under their name in the user interface.

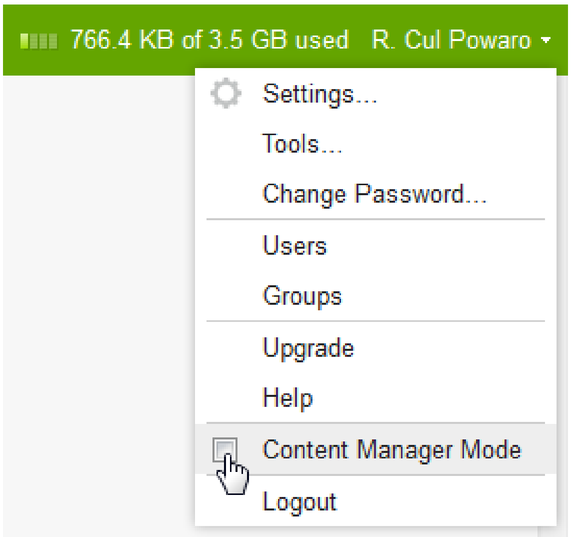


Figure 1 Switching to content manager mode (in the user interface)

Transferring access rights of deleted users and groups

If administrator deletes a user or a group, they can transfer their rights view and manage content in Kerio Workspace to another user or group.

If you do not transfer the rights to anyone and no other users has rights for access to the specific content, you can use the **Content Manager** function (see above).

Information about transferring access rights can be viewed in the Config log.

Using SSL certificates

What are SSL certificates

The principle behind secure services in Kerio Workspace (services encrypted by SSL, namely HTTPS) is that all communication between the client and the server is encrypted to protect it from tapping and to prevent it from misuse of transmitted information. SSL certificates verify the server identity which protects both the server and the client.

> If you wish to ensure high security in Kerio Workspace, enable communication only via SSL. Once you configure the server, it is necessary to install a certificate (you can also use so-called *self-signed* certificate which is easier to create. However, certificates signed by certification authorities are more secure).

Section **Configuration** → **SSL Certificates** in the administration interface provides you with a list of security certificates. You may add, import, edit, delete or export a certificate as well as display certificate details.

How to add certificate

Certificates can be added by using the following methods:

- create a new certificate (so called self-signed certificate)
- import a certificate (e.g. signed by a certification authority)

How to create new certificate

Newly created certificate is called *self-signed* certificate. It is original, unique and will be issued by your company for the name of your server. This certificate ensures security for your clients as it explicitly shows the identity of your server.

One self-signed certificate is created automatically immediately upon the first startup of Kerio Workspace. However, you can add a new one any time later whenever needed:

1. In the Kerio Workspace administration interface, go to **Configuration** → **SSL Certificates.**
2. Select **New** → **New certificate.**
3. Fill in the form and set time which the certificate will be valid for.

The clients will be notified by their web browsers that the certification authority is not trustworthy (when using the HTTPS protocol). However, since they know who created the certificate and for what purpose, they can feel secure to install it. Secure communication is then ensured for them and no warning will be displayed again because your certificate has all it needs.

How to get and apply certificate signed by certification authority

To get a legitimate certificate, contact a public certificate authority (e.g. Verisign, Thawte, SecureSign, SecureNet, Microsoft Authenticode, etc.). The process of certification is quite complex and requires a certain expertise. Kerio Workspace enables certification request that can be exported and the file can be delivered to a certification authority.

1. In the Kerio Workspace administration interface, go to **Configuration** → **SSL Certificates**.
2. Select **New** → **New certificate request**.
3. Fill in the form and confirm.
4. In the list of certificates, select the created request, click on **Export** → **Export Request** and save the `csr` file.
5. Now click on **Export** → **Export Private Key** and save the `key` file.
6. Send the `csr` file to a certification authority.

When you get the signed certificate from the certification authority back, import it to Kerio Workspace:

1. In the Kerio Workspace administration interface, go to **Configuration** → **SSL Certificates**.
2. Select **Import** → **Import Signed Certificate from CA**.
3. Load the files obtained (certificate and private key) and click on **Import**.

More settings for SSL certificates

Certificates can be backed up by exporting them to corresponding files (`crt` and `key`). Then it is possible to import certificates whenever needed.

Select a certificate and click the **Show Details** button to display detailed information.

Selected certificate can be deleted by clicking on *Remove*.

The *Set as Active* option activates the certificate which will be used for incoming *HTTPS* connections.

Information about changes in SSL certificates settings are recorded in the Config log.

Connecting Kerio Workspace to directory service

Which directory services Kerio Workspace supports

Kerio Workspace supports the following directory services:

- Microsoft Active Directory
- Apple Open Directory

What is the connection used for

In practice, mapping accounts from a directory service provides the following benefits:

Easy account administration

Apart from the internal database of user accounts, *Kerio Workspace* can also import accounts and groups from an LDAP database. Using LDAP, user accounts can be managed from a single location. This reduces possible errors and simplifies administration.

Online cooperation of Kerio Workspace and directory service

Additions, modifications or removals of user accounts/groups in the LDAP database are applied to Kerio Workspace immediately.

⚠

- Accounts created in Kerio Workspace will be created only locally — such accounts will not be copied into the LDAP database.
- If the directory service is unavailable, users will not be able to login to Kerio Workspace. It is therefore recommended to create at least one local account with read/write permissions.
- When creating a user account, ASCII must be used to specify username. If the username includes special characters or symbols, it might happen that the user cannot log in.

Once you connect Kerio Workspace to a directory service, you can activate users and groups from the database.

How to connect to directory service

The following chapters describe how to connect Kerio Workspace to directory services. Information about mapping can be found in the Config log.

Microsoft Active Directory

Go to section **Configuration** → **Directory Service** → **LDAP Server** in the administration interface.

1. In the *Directory Service* dialog, check the **Map user accounts from a directory service** option and fill in the following data:

   - **Directory Service Type** — select *Active Directory* from the drop-down menu.

   - **Domain Name** — enter the name of the domain

2. Next, define the directory service sources:

   - **Connect to directory servers looked up in DNS (SRV records)** — DNS records are used to look up directory servers.

   - **Use the specified directory servers** — set the directory servers manually. Enter the **Hostname** of the computer for the primary and backup directory servers.

   You may use **Encrypted connection (SSL)** to connect to the directory service servers.

3. In section **Account with read access to the directory service**, enter the username and password of the admin account in *Microsoft Active Directory*.

4. Use the *Test Connection* button to test the connection.

5. Click *Apply* to confirm the settings.

Apple Open Directory

Go to section **Configuration** → **Directory Service** → **LDAP Server** in the administration interface.

1. In the *Directory Service* dialog, check the **Map user accounts from a directory service** option and fill in the following data:

   - **Directory Service Type** — select *Apple Open Directory* from the drop-down menu.

   - **Domain Name** — enter the name of the domain

2. Set the primary and/or secondary directory server (**Hostname**).

3. You may use **Encrypted connection (SSL)** to connect to the directory service servers.

4. In section **Account with read access to the directory service**, enter the username and password of an account in *Apple Open Directory*. In *Apple Open Directory*, assign this account read rights.

5. **LDAP Search Suffix** will be added automatically once you enter the domain name.

6. Use the *Test Connection* button to test the connection.

7. Click *Apply* to confirm the settings.

Setting email communication

When does Kerio Workspace send email messages

If user has activated sending news feed via email and once they add a space or a page to their favorites, Kerio Workspace will send an email about every commented change in their favorite space or page. You can configure the parameters in the administration interface. All information about sending email messages can be found in the **Config** log.

How to set sender address

In the administration interface in section **Configuration** → **Email settings**, set parameters **Default From Address**.

> ⚠ The address should be real. Otherwise the mail server may flag the messages sent from Kerio Workspace as spam.

Automatic messages may be sent in several languages. If you wish to change the language of the messages, select one in **Notification Language**.

How to configure the SMTP server

1. In the administration interface in section **Configuration** → **Email settings**, set parameters for the SMTP server.
2. Enter the port number.

   > If you wish to you the encrypted traffic , use SSL (port 465) or TLS (port 25).

3. If the SMTP server requires authentication, enter a username and password.

What are the requirements for receiving email messages

If a user wished to receive email messages with notifications, the following requirements must be met:

- email address configured for their account to which email messages will be sent,
- pages and spaces added to Favorites,
- option **Receive email notifications about updates in my favorite items** enabled in the **Settings** on tab **Notifications**.

Displaying information about active connections

Displaying information about active connections

In the administration interface, you can display information about users who are currently connected to Kerio Workspace and its administration.

Table in section **Status** → **Active Sessions** displays information about:

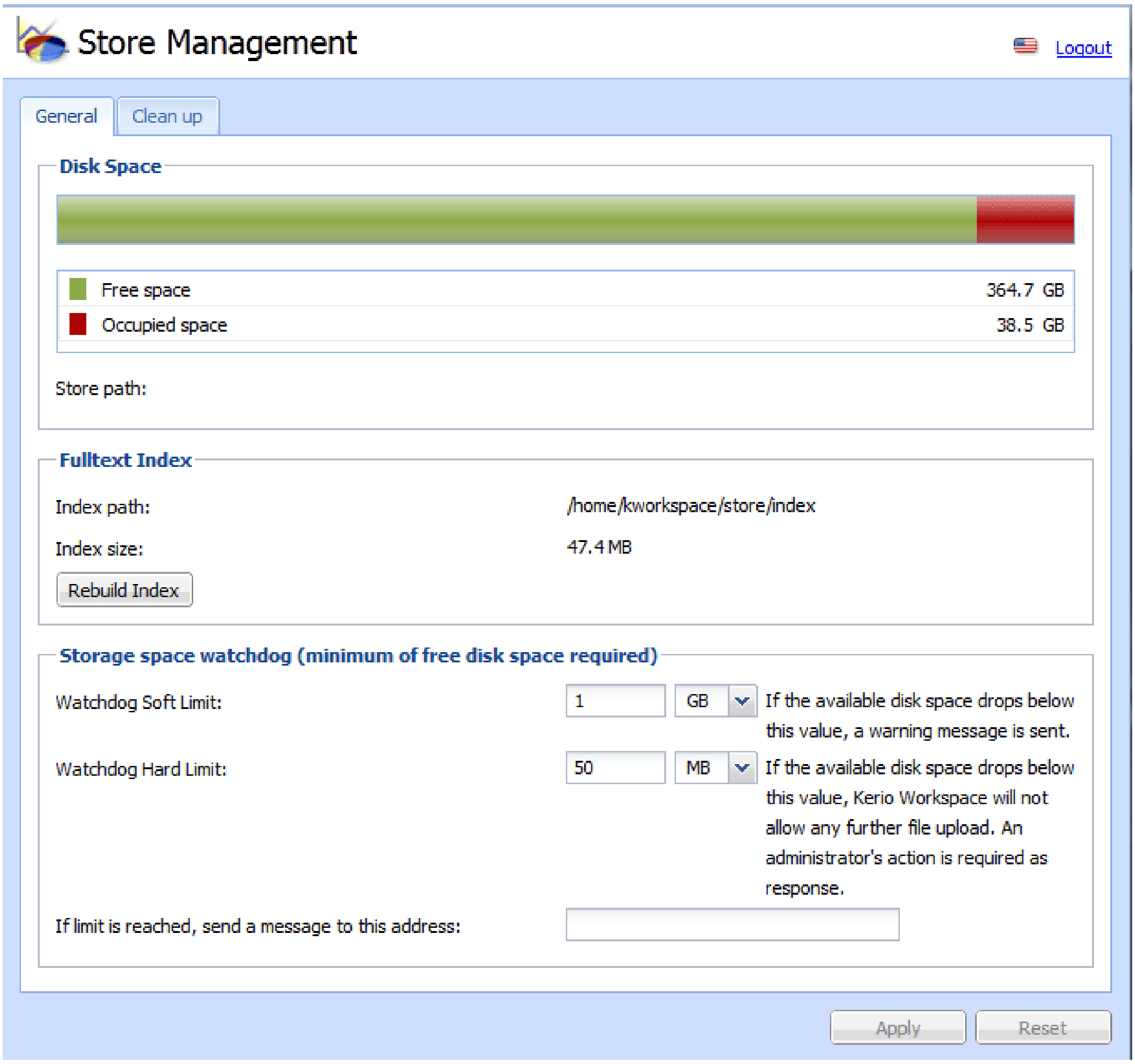
- who is connected (**User**),
- from which IP address,
- when the connection will expire,
- whether the user is connected to Kerio Workspace or its administration,
- which client they use,
- what protocol they use.

You can view detailed information about user activities in the Activity log.

Managing data stored in Kerio Workspace

How to manage data store

Your Kerio Workspace data can be managed in section **Store Management**.



Disk Space

🟩	Free space	364.7 GB
🟥	Occupied space	38.5 GB

Store path:

Fulltext Index

Index path: /home/kworkspace/store/index

Index size: 47.4 MB

Storage space watchdog (minimum of free disk space required)

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

Watchdog Hard Limit: 50 MB — If the available disk space drops below this value, Kerio Workspace will not allow any further file upload. An administrator's action is required as response.

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

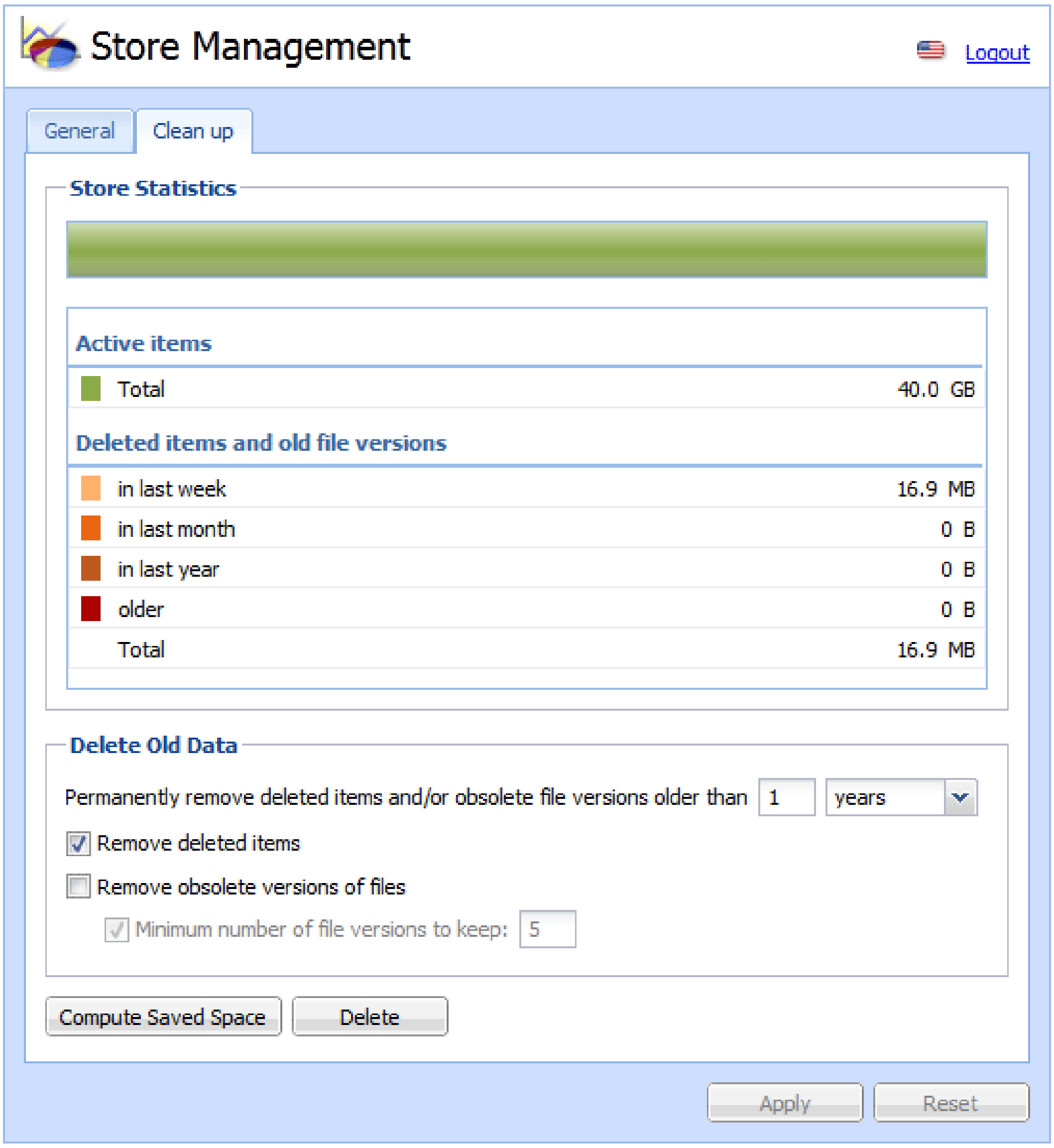
Figure 1 Basic information and settings for data stored on the server

It provides information on free and occupied disc space.

In addition, it allows to rebuild index if it gets damaged or if you install a new product version and restore your data from backup.

This section allows to set space watchdog, so that you can receive alerts any time the free disc space drops below the soft limit. If It drops below the hard limit, an alert email is also delivered to your address and Kerio Workspace disallows further uploads unless some space is freed again by the administrator.

The **Clean up** section allows to remove old items and get more free space on the server.



Store Management

Store Statistics

Active items	
🟩 Total	40.0 GB
Deleted items and old file versions	
🟧 in last week	16.9 MB
🟧 in last month	0 B
🟫 in last year	0 B
🟥 older	0 B
Total	16.9 MB

Delete Old Data

Permanently remove deleted items and/or obsolete file versions older than 1 years

☑ Remove deleted items

☐ Remove obsolete versions of files

☑ Minimum number of file versions to keep: 5

Figure 2 The Clean up section allows remove old items and get more space on the server

You can view status bar informing on old and deleted items kept on the disc, with corresponding numbers attached. The values do not overlap (the **last week** value is not included in the **last month** value, etc.).

With this knowledge, you can easily decide how old versions of obsolete files will be kept/removed and set it in the bottom part of the dialog. Here you can also define, how many numbers of file versions will be kept. You can view estimated space to be saved by clicking on **Compute Saved Space**.

The redundant data will be permanently removed from the server.

Managing logs in Kerio Workspace

What are logs in Kerio Workspace

Kerio Workspace records critical information in files called logs. This information includes error and warning reports, debugging information, etc. Logs make one row for each piece of information. Each row starts with a timestamp (date and time of the event). Messages in logs are displayed in English for every language version of Kerio Workspace.

Logs Settings

Logs can be found in the Kerio Workspace administration. By right-clicking in the content pane of any log, you open the context menu:

Save Log

The **Save log** option enables saving of the entire log or its selected part in a text file to a selected path on the disk.

The log may be saved as in plain text (TXT) or in hypertext (HTML). If the log is saved in HTML, the encoding and colors (where highlighting was used) will be saved. If it is expected that the log would be processed by a script, it might be better to save it in plain text.

You can either save the whole log or use mouse pointer to select a part of the text to save. The **Only selected rows** is active only if you select a part of the text with cursor.

Highlighting

Kerio Workspace enables highlighting of any part of text in logs. This function is used for better reference.

New highlighting can be set in the **Add highlighting** dialog box:

- **Description** — description used for better reference.
- **Condition (substring)** — every line containing the substring specified will be highlighted according to the parameters set in this dialog. If option **Regular expression** is enabled, any regular expression can be entered (for advanced users).
- **Color** — select a color used for the highlighting.

Log Settings

Select this option to open the dialog where you can set parameters for rotating (see below) or saving logs. The **File Logging** tab:

- **Enable logging to file** — if this option is enabled, the log will be save to the corresponding file under *Logs* in the product's installation directory.
- **Rotate regularly** — offers the possibility to save log in a regular time period.

- **Rotate when file exceeds size** — set the maximum log file size (in kBs) in **Max log file size**.
- **Number of rotated log files to keep** — once number of files reaches the value set here, the oldest file gets removed within any future rotation.

Open the **External Logging** dialog to set logging to a *Syslog* server:

- **Enable Syslog logging**
- **Syslog server** — DNS name or IP address of the particular Syslog server.

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

Types of logs in Kerio Workspace

Activity

The **Activity** log contains information about all operations performed by **Kerio Workspace** users (creating spaces, pages, editing, uploading files, login, content manager activities, etc.).

Config

The **Config** log preserves a complete history of operations performed by all application administrators in the administration interface.

This log stores information such as administrator login, user deactivation, changes in user account settings, changes in certificate settings, changes in language settings and so on.

Security

The **Security** log stores security warnings (information on failed login, attempts to upload dangerous content, etc.).

Warning

The **Warning** log displays warning messages about errors of little significance. A typical warning is a message informing that a document preview has not been generated.

Events which produce warning messages in this log do not have any crucial effects on Kerio Workspace. The Warning log can help if for example a user is complaining that certain services are not working.

Error

The **Error** log displays information about serious errors that affect the functionality of the entire server. The Kerio Workspace administrator should check this log regularly and try to eliminate problems found here. Otherwise, users might have problems with some services or/and serious security problems might arise.

Server log

All technical information is stored in this log. This includes, for example, error logs which are used by technical support and developers of this product.

Changing ports and redirecting all traffic to secure connection

How to solve the problem with several HTTP servers on one computer?

⚠ Do not change the default ports in Kerio Workspace unless it is necessary. You sentence your users to writing ugly and unrememberable URLs with a port number following a colon.

Virtualization

The easiest way to solve this problem is the virtualization. We have prepared a preinstalled VMware Virtual Appliance which you can use in the VMware products. Every HTTP server will operate on a different IP addresses on standard ports.

How to change the ports

1. In the administration interface, go to **Configuration** → **Web Server Ports**.
2. Change the port numbers.
3. Click **Apply** to confirm the settings.

If the settings are correct, information about the service running is displayed.

⚠ Once you change the ports, you have to use the port number if you wish to access Kerio Workspace (for example: `http://workspace.fairywood.com:8040`).

Kerio Workspace listens on all network interfaces and configured addresses (*IPv4* or *IPv6*). If you do not wish to use the *IPv6* addresses, disable them on your system.

All information about these settings can be found in the Config log.

How to force secure connection

You can access Kerio Workspace from a local network or from outside. Users may be required to use only secure connection for security reasons. To ensure it, check option **Redirect all requests to HTTPS.**

How it works Once these settings are done, users do not have to think about whether to use HTTP or HTTPS they just enter the server DNS name (for example, `workspace.fairywood.com`) and they will be automatically directed to a SSL connection (`https://workspace.fairywood.com`)

All information about these settings can be found in the Config log.

Login to Kerio Workspace

Which Kerio Workspace interfaces are available

- administration interface
- user interface

We recommend to use the supported browsers to connect to the interfaces. For the list of the browsers, refer to the Kerio Workspace product pages.

Web interfaces are currently localized into several languages. Select yours in the top right corner of the interface. The default language is set according to your browser language settings.

Kerio Workspace Administration

How to login

Before you login the first time, make sure you have:

- DNS name of the server with Kerio Workspace.
- Supported browser

To login, enter the DNS name of the computer with Kerio Workspace:

```
kerio.workspace.name/admin
```

Administration runs solely via the HTTPS protocol on port 4060. The address is automatically redirected to:

```
https://kerio.workspace.name:4060/admin
```

> If Kerio Workspace is located behind firewall, HTTPS on port 4060 must be enabled.

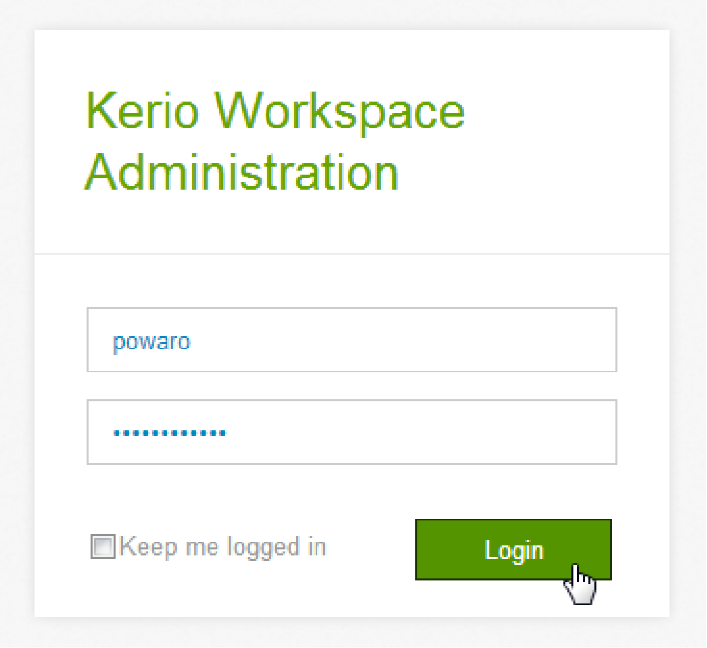
If the URL is entered correctly, your browser displays a warning about a SSL certificate. After the installation, Kerio Workspace creates a certificate which is not signed by a trusted certificate authority — it is a self-signed certificate (for more information, read article about the SSL certificates). Since you know the certificate can be trusted, you can add the security exception and continue to a login page.

First login

When you connect to Kerio Workspace for the first time, a configuration wizard is displayed where you:

- Enter the initial admin account details.
- Set data store path and language for sample content.

After successful configuration, the login page is displayed. Enter the username and password you created earlier.



Kerio Workspace Administration

powaro

••••••••••••

Figure 1 Login to administration

Kerio Workspace client

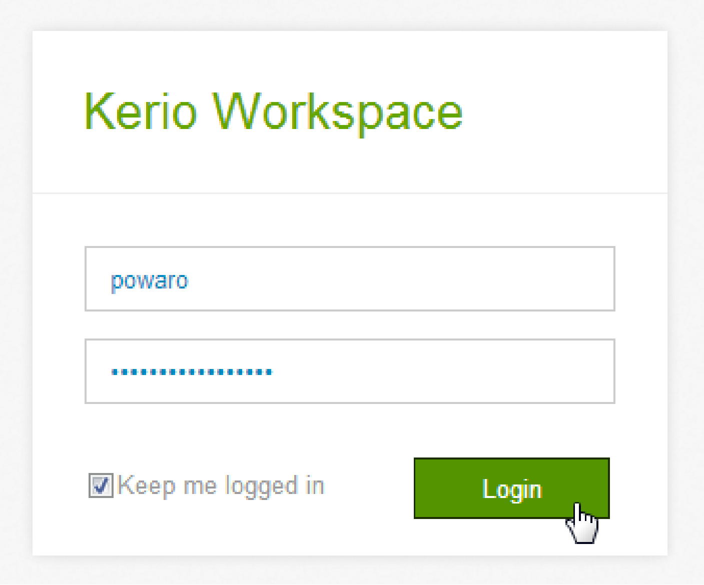
How to login to Kerio Workspace client

1. Specify URL in the browser in the following format:

   `http://kerio.workspace.name/`

2. If the URL is entered correctly, Kerio Workspace client login page is displayed.

3. Use credentials of Kerio Workspace user.



Kerio Workspace

poworo

••••••••••••••••••

☑ Keep me logged in

Figure 2 Login to Kerio Workspace client

Restoring Kerio Workspace from backup

How to create and schedule backups

Kerio Workspace allows two basic backup methods:

- Full backup — creates a full backup copy
- Differential backup — creates a copy including only data created or changed since the last full backup

As implied by these definitions, there must always be at least one full backup created before creating a differential backup, as the differential backup is only complementary.

You can schedule backups as needed. It is recommended to create one full backup at the beginning or the end of the week and keep making differential backups on every day between.

> Bear in mind that creating full backup takes some time as the data included might be quite voluminous. It is therefore recommended to schedule such backups for off-peak hours, for example for nights or weekends.

To add or edit scheduled backups, it is first necessary to check option **Enable data store and configuration backup**.

To set number of full backups to be kept, click on **Advanced** and set the desired value.

If you want to perform an immediate full backup, click on **Start now**. This is understood as an exceptional full backup and not counted in the number of full backups kept.

All records related to backups can be found in the **Config** log.

How to restore Kerio Workspace from backup

If you, by accident, lose your Kerio Workspace data and need to restore them from a backup, follow these instructions:

1. Install Kerio Workspace again.
2. Stop the Kerio Workspace server.
3. In your backup directory (*Workspace Store*), take the latest full backup ZIP file and unzip it in the new Kerio Workspace installation directory.

> On Mac, the standard decompression tool cannot be used for files larger than 2 GB. Use the *xz* application instead.

4. Now apply the process described in the step 3 also on all differential backup files created since the last full backup.

5. Run the Kerio Workspace server.

6. Since 2.1.0, the fulltext index is not included in the backup and it is necessary to take this extra step: Go to **Store Management** in the Kerio Workspace administration and click on **Rebuild Index**.

Updating Kerio Workspace

How to check for new versions

If you wish to be automatically informed about new version of Kerio Workspace, go to section **Configuration** → **Update Checker** and check option **Automatically check for new versions**. Once a new version is available, you will be notified upon your login to administration.

You can also be notified about new beta versions (beta versions are suitable for testing, we do not recommend to use them in a production environment).

If you wish to help us with Kerio Workspace development, check the option for sending anonymous usage statistics. You can view which data will be sent.

By using the **Check now** button, you can check for new versions anytime.

All information about these settings can be found in the **Config** log.

How to install new version

You can install new version of Kerio Workspace in case your Software Maintenance is active.

Save the new version to your harddrive and install it according to your operating system.

Kerio Workspace VMware Virtual Appliance

What is Kerio Workspace VMware Virtual Appliance for

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

For supported VMware product versions, check the product pages.

How to get Kerio Workspace Virtual Appliance

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

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

  ```
  http://www.kerio.com/workspace/download/
  kerio-workspace-appliance-2.x.x-1270-linux.ovf
  ```

  VMware ESX/ESXi automatically downloads the `OVF` configuration file and a corresponding disk image (`.vmdk`).

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

Working with Kerio Workspace VMware Virtual Appliance

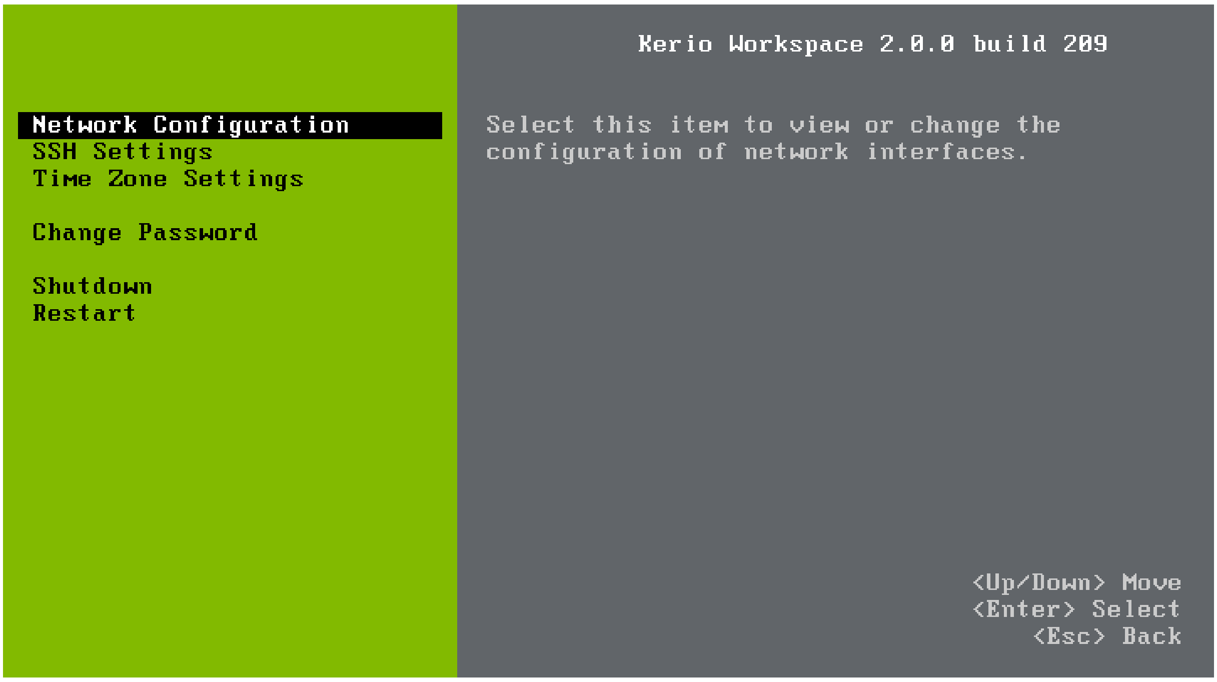
When you run the virtual computer, Kerio Workspace interface is displayed.

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

- Kerio Workspace administration account username and password,
- email,
- data store (folder path).

This console provides several actions to be taken:

- change network configuration
- allow SSH connection
- set time zone
- change user `root` password
- restart a power off Kerio Workspace Appliance



```
                                   Kerio Workspace 2.0.0 build 209

Network Configuration              Select this item to view or change the
SSH Settings                       configuration of network interfaces.
Time Zone Settings

Change Password

Shutdown
Restart

                                                             <Up/Down> Move
                                                             <Enter> Select
                                                               <Esc> Back
```

Figure 1 Console — network configuration

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

Network configuration

The network configuration allows you to:

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

If you use a DHCP service on your network, the server will be assigned an IP address automatically and will connect to the network. If you do not use or do not wish to use DHCP for Kerio Workspace, 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 Workspace so that it will not change.
If you run Kerio Workspace 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 display of date and time in logs. Event start date and time, task due date, etc. don't depend on time zone settings on the server side (they are saved in UTC/GMT on the server side and recalculated in accordance with the client's time zone).

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

Updating Kerio Workspace

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.

Updating Kerio Workspace

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

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