

ZCP trunk (build 34619)

Z-Admin Manual

The Z-Admin Manual



Zarafa

ZCP trunk (build 34619) Z-Admin Manual

The Z-Admin Manual

Edition 7.0

Copyright © 2012 Zarafa BV.

The text of and illustrations in this document are licensed by Zarafa BV under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at [the *creativecommons.org website*](http://creativecommons.org/website)⁴. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Red Hat®, Red Hat Enterprise Linux®, Fedora® and RHCE® are trademarks of Red Hat, Inc., registered in the United States and other countries.

Ubuntu® and Canonical® are registered trademarks of Canonical Ltd.

Debian® is a registered trademark of Software in the Public Interest, Inc.

SUSE® and eDirectory® are registered trademarks of Novell, Inc.

Microsoft® Windows®, Microsoft Office Outlook®, Microsoft Exchange® and Microsoft Active Directory® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

The Trademark BlackBerry® is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Zarafa BV is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited.

All trademarks are the property of their respective owners.

Disclaimer: Although all documentation is written and compiled with care, Zarafa is not responsible for direct actions or consequences derived from using this documentation, including unclear instructions or missing information not contained in these documents.

The Zarafa Collaboration Platform (ZCP) combines the usability of Outlook with the stability and flexibility of a Linux server. It features a rich web-interface, the Zarafa WebAccess, and provides brilliant integration options with all sorts of clients including all most popular mobile platforms.

Most components of ZCP are open source, licensed under the [AGPLv3](http://www.gnu.org/licenses/agpl-3.0.html)¹, can therefore be downloaded freely as [ZCP's Community Edition](http://www.zarafa.com/content/community)².

Several closed source components exist, most notably:

⁴ <http://creativecommons.org/licenses/by-sa/3.0/>

¹ <http://www.gnu.org/licenses/agpl-3.0.html>

² <http://www.zarafa.com/content/community>

-
- the Zarafa Windows Client providing Outlook integration,
 - the Zarafa BES Integration providing Blackberry Enterprise Server connectivity,
 - the Zarafa ADS Plugin providing Active Directory integration, and
 - the Zarafa Backup Tools.

These components, together with several advanced features for large setups and hosters, are only available in combination with a support contract as part of *ZCP's Commercial Editions*³.

Alternatively there is a wide selection of hosted ZCP offerings available.

This document, the Administrator Manual, describes how to install, upgrade, configure and maintain ZCP on your Linux server. In addition various advanced configurations and integration options are discussed.

³ <http://www.zarafa.com/content/editions>

1. Installation	1
1.1. System requirements	1
1.2. Procedure	1
1.2.1. Ubuntu 10.04.2 LTS	1
1.2.2. Red Hat Enterprise Linux 5	2
1.3. First steps	3
1.4. Additional Steps	3
2. System	5
2.1. Services	5
2.1.1. Start and Stop Services	5
2.1.2. System Time	5
2.1.3. Time Server	5
2.1.4. Restart / Shutdown	5
2.2. Certificate / Key Management	5
2.2.1. Manage Certificates	5
2.2.2. Create Own Certificates	6
2.2.3. Upload Certificates	6
3. Network	7
3.1. Configuration	7
3.1.1. Basic Configuration	7
3.1.2. Proxy Settings	7
3.1.3. Interface Configuration	7
3.2. SNMP	7
4. Accounts	9
4.1. Authentication Server	9
4.1.1. Local Authentication	9
4.1.2. Z-Admin LDAP Server	9
4.1.3. Remote LDAP Authentication	10
4.1.4. Active Directory	10
4.2. User Management	11
4.2.1. Adding and editing users	11
4.3. Group Management	11
4.4. Admin password	12
5. Maintenance	13
5.1. Save Configuration	13
5.1.1. Save Configuration	13
5.1.2. Restore Configuration	13
5.2. Log file viewer	13
5.3. Notification	14
5.4. Support	14
6. Zarafa	15
6.1. Zarafa Licence Key	15
6.2. Groupware Configuration	15
6.3. Resources	15
6.4. Zarafa Setup	16
6.5. Allocation of Email Addresses	16
6.6. Zarafa Web Access	16
6.7. Backup Path	16

Installation

1.1. System requirements

- Ubuntu or Red Hat Enterprise Linux
- about 22 MB of additional disk space

1.2. Procedure

Yaffas can be installed from the repositories described below.

1.2.1. Ubuntu 10.04.2 LTS

Adding required repositories

```
echo "deb http://repo.yaffas.org/ubuntu ./" >> /etc/apt/sources.list
echo "deb http://archive.canonical.com/ubuntu lucid partner" >> /etc/apt/sources.list
```

Import package key

```
wget -O - http://repo.yaffas.org/ubuntu/repo.key | apt-key add -
```

Install the packages

```
apt-get update
apt-get install zadmin
```

This will install Z-Admin base modules and zarafa.

The package manager will usually ask questions for some packages. You can skip all of these by pressing "enter" when the dialog pops up. Only if you are asked for a MySQL server root password you should enter a password and note it down as you will be asked for MySQL credentials when first using Z-Admin.

Optional: installing the configuration packages

This package and its dependencies are used to make a freshly installed system manageable with Z-Admin. Without yaffas-config, a number of manual adjustments to configuration files need to be made so the admin interface can function properly.

```
apt-get install yaffas-config
```

Answer "yes" if the installation system asks to replace configuration files.



Warning

When installing the **yaffas-config** package and its dependencies, the following settings and data will be deleted or overwritten:

- existing LDAP tree
- slapd configuration
- Samba configuration
- smbldap-tools configuration
- postfix configuration
- zarafa configuration
- MySQL configuration (optimizations for Zarafa will be made)

1.2.2. Red Hat Enterprise Linux 5

The installation on Red Hat Enterprise Linux is similar.



Warning

The package **yaffas-config** will overwrite the same configuration files as mentioned above.

Adding the required repositories

Prior to the installation of Z-Admin Zarafa packages have to be installed. Otherwise the open source packages included in the EPEL repository will be used. Packages can be downloaded from <http://www.zarafa.com/download-release>.

For automatic dependency resolution the [EPEL](http://www.fedoraproject.org/wiki/EPEL)¹ and [RPMforge](http://rpmrepo.org/RPMforge)² repositories should be included into the yum configuration.

Create a file "yaffas.repo" in folder /etc/yum.repos.d with the following contents:

```
[yaffas]
name = Yaffas $releasever
baseurl = http://repo.yaffas.org/rhel/
enabled = 1
protect = 0
gpgcheck = 1
```

Import GPG keys

```
rpm --import http://repo.yaffas.org/rhel.key
```

Packages installation

¹ <http://fedoraproject.org/wiki/EPEL>

² <http://rpmrepo.org/RPMforge>

```
yum install yaffas yaffas-zarafa yaffas-config
```

1.3. First steps

After installation, the Z-Admin web interface is accessible at the following URL: **https://<your-server's-ip>:10000**

The username is "admin" and password is "yaffas".

On first log in the admin password has to be changed. If you installed the yaffas-zarafa package you have to specify a MySQL user who has permission to create a database for Zarafa.

After the first login an authentication server should be selected in Accounts → Authentication. Choices are Active Directory, remote LDAP and local authentication. Please note that currently the configuration files (yaffas-config) have to be installed for this step.

On Red Hat Enterprise Linux you also need to start the required services and configure them for automatic start at boot. This can be done in "System → Services". Since by default an iptables firewall is active in Red Hat Enterprise Linux, the ports for the needed services have to be opened manually.

The next step should be to configure the mail server. Without a working mail server configuration some parts of the system will not work. It will also not be possible to create resources for Zarafa when no local domain is set for the mail server.



Important

The language in the Z-Admin UI has to be set for the folders in Zarafa to be created in the right language. This should be done prior to the creation of users.

1.4. Additional Steps

When using the supported zarafa packages there will be two more packages available:

- zarafa-webaccess-muc
- zarafa-backup

These have to be installed manually for the corresponding functionality to be available.

System

2.1. Services

2.1.1. Start and Stop Services

By selecting the menu item "services" the state of each system service can be shown. If you right click on a service, you can start, stop or re-start the service. Furthermore, you can choose to start the service by booting the system and to monitor the service. Then the admin will receive an email notification if the service fails to start.

2.1.2. System Time

At this tab you can manually set the system time. Time can be set with drop-down fields and be saved afterwards.

2.1.3. Time Server

Additionally, time can be synchronized with a time server. This is possible once or in hourly or daily intervals. For this purpose enter the IP address or the hostname of the time server and choose an interval.

For example, the below listed time servers can be used. The precondition is that a valid DNS server is configured.

- time.fu-berlin.de
- ntp0.fau.de
- ntp1.ptb.de

2.1.4. Restart / Shutdown

At the tab "Shutdown System" you can reboot or shut down the system.

2.2. Certificate / Key Management

Certificates and keys are required to encrypt communications with the web interface as well as the mail traffic. They guarantee the authenticity, confidentiality and integrity of the data to third parties. Free signed SSL certificates are available at <http://www.cacert.org>.

Under the menu item "Certificate / Key Management" they can be managed. You can even create certificates and sign it with your own key. You can also import or delete existing certificates.

2.2.1. Manage Certificates

Using the tab "Manage Installed Certificates" all certificates existing on the system are displayed. If you want to delete a certificate, tick the box on the left of the certificate and click on the button "delete". The default certificate "default.crt", which is used for all services of the system, cannot be deleted.

Tip

If you want to replace "default.crt", you must either create a new certificate for all services or import an existing certificate.

2.2.2. Create Own Certificates

To create a certificate yourself, click on the tab "Generate Self Signed Certificate and Key", fill in all fields and create the certificate by clicking on "Generate Key". If you choose "all" at the drop-down field "service", you can create a default certificate. This is always used if no other certificates are available specific to a service. All other choices for "service" create a certificate for the respective service.

2.2.3. Upload Certificates

If you want to upload an existing certificate, click on the tab "Upload Certificate" and click on "Browse" to choose the file from your hard disk. Select the file with the certificate and click "Open". After the dialog closed itself you have to select the service to which your certificate shall apply. Finally, you should delete any remaining duplicates.



Important

The key and the certificate must be contained together in one file to successfully import a certificate. Please note that the key should come **first** and the file **must not be** encrypted.

Network

3.1. Configuration

3.1.1. Basic Configuration

Basic network configurations can be set under the menu item "Networking" → "Configuration" at the tab "Base Settings".



Note

Type the name of the computer into the field "Host Name". With this name the computer will be reachable in the network. The name is also used in the Windows network. The "Domain Name" must be formatted as required in [RFC 1034](http://www.ietf.org/rfc/rfc1034.txt)¹ (e. g. "bitbone.de"). The "Workgroup" is required for Windows networks.

3.1.2. Proxy Settings

The settings for HTTP proxy are required for downloading Z-Admin updates if your network doesn't have a direct internet access.

Please type the address into the field "Proxy" and the port of your HTTP proxy server into the second field. If your proxy needs user authentication, enter the required data in "User" and "Password". Confirm with "Save".

3.1.3. Interface Configuration

Each available interface has an own tab for it's basic settings at the "Interface" tabs.

If your network contains multiple network areas and the mail server or individual workstations are located in a different network, the default gateway must be specified. In this case the address of your DNS server must be entered in the field "DNS Server IP". You can also enter several search domains, which are used for resolving host names if a full name is not provided.

The settings for each interface are only active when the interface is activated. If multiple interfaces are activated simultaneously, the settings for all interfaces can be processed.

By clicking the button "New Virtual IP Address" you can configure an additional IP address for the associated interface. For this virtual interface you can use the same values as used for a usual interface.

3.2. SNMP

Click the checkbox under the menu item "Networking → SNMP Configuration" to enable access via SNMP protocol. You can set the password for SNMP access in the field "Community".

¹ <http://www.ietf.org/rfc/rfc1034.txt>



Important

Using SNMP data is generally transmitted unencrypted via network. For your own safety, please choose another password than "root" or the administrator's password!

The field "Access For" defines who has access to the SNMP agent. The entry "default" means, that only requests from the local machine are allowed.

You can enter a single IP address or a subnet following the *CIDR*²-pattern *address/mask* (e. g. 192.168.0.1/24).

² <http://tools.ietf.org/html/rfc4632>

Accounts

4.1. Authentication Server

The menu topic "*Accounts → Authentication Server*" leads to a page for configuring the source for authentication.

After installation of Z-Admin this has to be configured first because other services depend on it. Users and groups can only be created after selecting an authentication type.

Z-Admin can use a local LDAP, a remote Z-Admin LDAP or a Microsoft Windows Active Directory domain for authentication.

When using the local LDAP for authentication the server can also be used as (LDAP) authentication server for other remote systems.



Warning

When changing the authentication type all settings that apply to users will be deleted. Those settings have to be re-applied after the change.

Z-Admin tried to find existing users in the new authentication source. Data from users that can not be found will be deleted.

To select a type of authentication choose the tab "*Select authentication*" below the menu topic "*Accounts → Authentication Server*"

4.1.1. Local Authentication

When choosing these method a local LDAP will be used for storing users and groups. You can optionally choose to let this server be used by other servers as authentication source.

4.1.2. Z-Admin LDAP Server

If you already use another Z-Admin server with local LDAP authentication you can enter it's connection details here. Users and groups on the remote system can then be used on the local server.



Note

A Z-Admin server which authenticates it's users against a remote server can not act itself as an authentication server. Should this option be active it will automatically be deactivated.

The following values have to be configured to run the LDAP server:

Value	Function
Server/IP	DNS name or IP address of the remote Z-Admin server. The remote side has to be configured to accept authentication requests.

Value	Function
Base DN	The base DN defines at which point in the LDAP-Tree a search for a certain object should be started.
Bind DN	The bind DN and the bind password are used for authentication against the remote LDAP server.
Bind password	The password for LDAP authentication. In case of problems with the authentication try using a CRYPT-hashed password.

4.1.3. Remote LDAP Authentication

You can use Z-Admin together with any remote LDAP server. Only the schema as to be installed on the remote LDAP server.

Value	Function
Server/IP	Enter the remote LDAP server's IP.
Base DN	Enter the searchbase of you LDAP server. e.g. o=yaffas,c=org
Bind DN	Enter the user dn that should be used for authentication against LDAP. e.g. cn=ldapadmin,ou=People,o=yaffas,c=org
Base DN user	Enter the part of the users subtree. e.g. ou=People
Base DN group	Enter the part of the groups subtree. e.g. ou=Groups
Bind password	Enter the password of the Bind DN user.
Search attribute user	Enter the attribute where user and group information should be searched for.

4.1.4. Active Directory

When using this type of authentication Z-Admin can join an Active Directory domain. All users and groups of this domain will be available in Z-Admin.



Note

When using Active Directory authentication it is advisable to enter the domain controller as first DNS server in the network configuration.

Field	Function
Domain Controller	Name or IP address of the Active Directory server.
Domain	Name of the AD domain.
Domain administrator	Username of an account with administrator privileges. Used for joining the domain. This user is searched in the cn=users organization unit.

Field	Function
Username	User for readonly queries. Only this information will be saved. The domain administrator settings are only needed for joining the domain.

For simple queries to the domain controller a standard user account is sufficient. Please enter the account information for this.



Warning

If you change the active directory user, his password or the DN of your server, you have to change those in the authentication module too!

4.2. User Management

In the UI under *Accounts* → *User management* all existing users are shown. When you have a lot of users the sort and filter options can be useful. To edit or delete an existing user you have to right-click on that user's entry.



Note

The options for editing are only available if you use local LDAP.

4.2.1. Adding and editing users

To create a new user open the *"Add user"* tab. To edit a user right click on it and select *"Edit user"*.

The username, given name, surname and password fields are required. During editing you can not change the username. Setting group memberships is optional. Selecting multiple groups or removing a group from the selection can be achieved by pressing <CTRL> while clicking.

You can select which features (right now only IMAP and POP3) should be enabled or disabled for the user. The sendas configuration is needed if you want to allow other users or groups to send in the name of this user.

Shared accounts are a special accounts that are not allowed to login. You have to give permissions for other users to this store to work with it. This account type will also not use a whole license. A zarafa administrator is a special user who has the permission to open and edit stores of other users. Please use this option with care!

The field *"email alias"* can be used to add e-mail aliases for this user. You have to insert a whole email adress as alias.

4.3. Group Management

The menu topic *"Group Management"* will show an overview of the available groups.

New groups can be created on the tab *"Create group"*. After entering a name for the new group and clicking on "create" the new group will be created. Optionally a group can also have an email adress. Every account that is member of this group will receive this message.

Existing groups can be edited by right-clicking on their entry and selecting *"Edit group"*.

4.4. Admin password

The admin password for the Z-Admin Web-UI can be changed after selecting this this menu topic. The password has to be entered twice before clicking on "Save".

Tip

Passwords should not contain user related strings, dictionary words or "*simple*" combinations of characters (e.g. characters next to each other on the keyboard).

Maintenance

5.1. Save Configuration

5.1.1. Save Configuration

At this menu item you can restore a saved configuration or save the current configuration by clicking on "Save Backupfile".



Note

Remember to save configurations regularly!

5.1.2. Restore Configuration

If you have to use this option, install the server with a fresh operating system, install Z-Admin and then select the authentication method that was used before. After selecting a configuration file, click on the button "Apply Backupfile" and the configuration file will be uploaded. This may take a few minutes.



Warning

Please consider that the following items will not be restored:

- network configuration
- admin and root password
- settings for authentication server
- alias settings if you use a remote authentication server
- UI language

5.2. Log file viewer

The log file viewer enable the administrator to download log files for analysis. Just right click on the log file you wish to download and select "*download*". After download and saving of the selected log file it can be viewed with any text editor (e.g. Wordpad).

Examples of log files are:

file	content
/var/log/maillog	postfix MTA log file. Contains information about in and outgoing mails.
/var/log/messages	less important kernel messages.
/var/log/samba/log.nmbd	messages from the NetBIOS service
/var/log/samba/log.smbd	samba server log messages
/var/log/zarafa	This directory contains zarafa logs for every component.

5.3. Notification

Error messages (disk full, license issues) from the Z-Admin server will be sent to this e-mail address. A local or remote address can be used. This e-mail account should be checked on a regular basis.

Please enter a valid e-mail address, so critical messages can reach an administrator and the system can be kept running.

Tip

If you would like to enter multiple recipients you can enter an alias as recipient, e.g. "admins@localhost", then you can set "admins" as alias under *Mail alias configuration* and supply the addresses of the recipients.

5.4. Support

The menu topic *Support* offers the option to download a file which can assist in solving problems and speed up searching for bugs.

Z-Admin is a free community project, so no support is included. Support can be performed by anybody who knows his way around Z-Admin and linux.

The bitbone AG offers a commercial and supported derivate of Z-Admin named bitkit|SOLUTIONS.

Zarafa

6.1. Zarafa Licence Key

In this module you can extend the numbers of users with Outlook access to Zarafa. Three users have access via Outlook without any licence key. If you want more users to have access you may buy a licence pack. The licence key has two components: a basis key and an additional user key. Please insert the key into the specific (basis or user) field and click the button "key upload".

At the tab "Installed Licences" all licences are shown. You will get more information at the tab "Licence Log".

6.2. Groupware Configuration

In this module you can optimize memory (RAM) for Zarafa, define the size of attachments or the content of quota emails for users.

Click "Optimize" to optimize the memory settings on your system. This is only necessary if the size of the RAM changes. The RAM settings will be optimized for Zarafa and MySQL.

You can also set the maximum size of attachments uploadable via the Zarafa Webaccess Interface.



Note

This limitation does **not** overwrite the setting of the mailserver. If there is a smaller size of attachments allowed, the mailserver settings are valid.

At the tab "Messages At Reaching Quota" you can customize the messages for reaching limits. The description of variables is available at the online help.

The following variables are available:

Variable	Meaning
\${ZARAFA_QUOTA_NAME}	name of the Zarafa account
\${ZARAFA_QUOTA_STORE_SIZE}	current size of the account
\${ZARAFA_QUOTA_WARN_SIZE}	limit for a warning
\${ZARAFA_QUOTA_SOFT_SIZE}	limit for a transmission lock of the account
\${ZARAFA_QUOTA_HARD_SIZE}	limit for a transmission AND reception lock of the account

6.3. Resources

In this module you can create and delete resources. For deleting or modifying right-click on an existing resource and choose an action.

Please note at the creation of a new resource: A resource needs a name - this name is shown in the global addressbook - and a description. You may decide whether a resource can be booked once ("Decline Conflicts") and whether recurring appointments are permitted.



Important

If you want to change resource settings, you may change the properties and description but not the name!

6.4. Zarafa Setup

The configuration of Z-Admin & ZARAFa is done via the known interface. There are some specifics to explain:

As a matter of principle each user account in Z-Admin is also a Zarafa user. Please pay attention that you have a corresponding license of Z-Admin and of Zarafa. If you have less Zarafa user licences than Z-Admin users, only the users with the lowest UIDs have access to Zarafa.

6.5. Allocation of Email Addresses

Please pay attention that during the creation of an user account the entry in the field "Email Address" is formatted as follows: "username@configured_maildomain" Otherwise, mail reception is not possible. If you want to use a different email address for reception, please insert it at "Email Alias" .

The registered address at "Email Address" is also used as sender for all mails sent via web access. For a proper function please set the local domain(s) on the mailservr at first(menu Mailservr → Configuration → Local Domains).

6.6. Zarafa Web Access

Insert the URL into your browser, e.g. <https://zarafaserver.local/webaccess>. Alternatively, you can choose name or IP address of Z-Admin without mentioning a port number. (e.g. <http://zarafaserver.local>)

A complete manual and current documentation of Zarafa Web Access can be downloaded here: <http://www.zarafaserver.com/doc>.

6.7. Backup Path

At this point we show an unspecific way to backup the data of the server. For a successful recovery of the data the Z-Admin server must be on the same level of version and patches!

the paths for the backup of Z-Admin & ZARAFa are:

path	entry
/var/log/	log-files
/data/mail/	mail boxes and Sieve filter scripts
/var/lib/fetchmail/.fetchmail-UIDL-cache	if fetchmail is used with POP3
Database MySQL (mysqldump)	all data of the Zarafa Server
/data/zarafa/	email attachments

Procedure for backup of data:

- backup of configuration via system → save configuration
- init 1 → change to single user mode

- backup of single paths in a temporary directory
- init 2 → normal mode of use
- backup of data to an external data medium

Procedure for recovery of data:

- recovery of configuration via system → save configuration
- copy the data into a temporary directory
- init 1 → change to single user mode
- delete all files below the named paths
- restore of single paths out of the temporary directory
- init 2 → normal mode of use

