

## Univention Corporate Server



**Cyrus mail server**



## Table of Contents

1. Introduction .....	4
2. Installation .....	5
3. Management of the mail server data .....	6
3.1. Management of mail domains .....	6
3.2. Assignment of e-mail addresses to users .....	6
3.3. Management of mailing lists .....	7
3.4. Management of mail groups .....	7
3.5. Management of shared IMAP folders .....	8
3.6. Mail quota .....	9
4. Spam detection and filtering .....	10
5. Identification of viruses and malware .....	11
6. Identification of spam sources with <i>DNS-based Blackhole Lists</i> (DNSBL) .....	12
7. Integration of Fetchmail for retrieving mail from external mailboxes .....	13
8. Configuration of the mail server .....	14
8.1. Configuration of a relay host for sending the e-mails .....	14
8.2. Configuration of the maximum mail size .....	14
8.3. Configuration of a blind carbon copy for mail archiving solutions .....	14
8.4. Configuration of soft bounces .....	14
9. Handling of mailboxes during e-mail changes and the deletion of user accounts .....	16
10. Distribution of an installation on several mail servers .....	17
11. Configuration of mail clients for the mail server .....	18
12. Webmail and administration of e-mail filters with Horde .....	19
12.1. Login and overview .....	19
12.2. Web-based mail access .....	19
12.3. Address book .....	20
12.4. E-mail filters .....	21
Bibliography .....	22

# Chapter 1. Introduction

Univention Corporate Server provides mail services that users can access both via standard mail clients such as Thunderbird and via the webmail interface Horde.

## Note

This is the documentation for the Univention Corporate Server mail server component using Cyrus instead of Dovecot as IMAP and POP3 server.

Since Univention Corporate Server version 4.0-2 Dovecot is used as the default IMAP and POP3 server. The documentation for using Dovecot can be found in the main user manual [ucs-manual].

Postfix is used for sending and receiving mails. In the basic installation, a configuration equipped for local mail delivery is set up on every UCS system. In this configuration, Postfix only accepts mails from the local server and they can also only be delivered to local system users.

The installation of the mail server component implements a complete mail transport via SMTP (see Chapter 2). Postfix is reconfigured during the installation of the component so that a validity test in the form of a search in the LDAP directory is performed for incoming e-mails. That means that e-mails are only accepted for e-mail addresses defined in the LDAP directory or via an alias.

The IMAP service Cyrus is also installed on the system along with the mail server component. It provides e-mail accounts for the domain users and offers corresponding interfaces for access via e-mail clients. Cyrus is preconfigured for the fetching of e-mails via IMAP and POP3. Access via POP3 can be deactivated by setting the Univention Configuration Registry variable `mail/cyrus/pop` to `no`. The same applies to IMAP and the Univention Configuration Registry variable `mail/cyrus/imap`. The further configuration of the mail server is performed via Univention Configuration Registry, as well (see Chapter 8).

The management of the user data of the mail server (e.g., e-mail addresses or mailing list) is performed via Univention Management Console and is documented in Chapter 3. User data are stored in LDAP. The authentication is performed using a user's primary e-mail address, i.e., it must be entered as the user name in mail clients. As soon as a primary e-mail address is assigned to a user in the LDAP directory, a listener module creates an IMAP mailbox on the mail home server. By specifying the mail home server, user e-mail accounts can be distributed over several mail servers, as well (see Chapter 10).

Optionally, e-mails received via Postfix can be checked for spam content and viruses before further processing by Cyrus. Spam e-mails are detected by the classification software SpamAssassin (Chapter 4); ClamAV is used for the detection of viruses and other malware (Chapter 5).

In the default setting, e-mails to external domains are delivered directly to the responsible SMTP server of that domain. Its location is performed via the resolution of the MX record in the DNS. Mail sending can also be taken over by the relay host, e.g., on the Internet provider (see Section 8.1).

The Horde framework is available for web-based mail access (see Chapter 12). The UCS mail system does not offer any groupware functionality such as shared calendars or invitations to appointments. However, there are groupware systems based on UCS which integrate in the UCS management system such as Kolab, Zarafa and Open-Xchange. Further information can be found in the Univention App Center.

## Chapter 2. Installation

There are two ways to install the mail server package with Cyrus instead of Dovecot:

- First install the application *Mail server* from the Univention App Center, then use the UMC module *Package Management* to install the package ***univention-mail-cyrus***.
- Run on the command line (logged in as root):

```
univention-install univention-mail-server univention-mail-cyrus
```


A mail server can be installed on all server system roles. The use of a domain controller is recommended because of frequent LDAP accesses.

The runtime data of the Cyrus server are stored in the `/var/spool/cyrus/` directory. This directory should not be operated on a NFS share.

The webmail interface Horde can be installed via the Univention App Center.

# Chapter 3. Management of the mail server data

## 3.1. Management of mail domains

Feedback 


A mail domain is a common namespace for e-mail addresses, mailing lists and IMAP group folders. Postfix differentiates between the delivery of e-mails between local and external domains. Delivery to mailboxes defined in the LDAP directory is only conducted for e-mail addresses from local domains. The name of a mail domain may only be composed of lowercase letters, the figures 0-9, full stops and hyphens.

Several mail domains can be managed with UCS. The managed mail domains do not need to be the DNS domains of the server - they can be selected at will. The mail domains registered on a mail server are automatically saved in the Univention Configuration Registry variable `mail/hosteddomains`.

To ensure that external senders can also send e-mails to members of the domain, MX records must be created in the configuration of the authoritative name servers, which designate the UCS server as mail server for the domain. These DNS adjustments are generally performed by an Internet provider.

Mail domains are managed in the UMC module *Mail* with the **Mail domain** object type.

## 3.2. Assignment of e-mail addresses to users

Feedback 

E-mail addresses can consist of the following characters: letters a-z, figures 0-9, dots, hyphens and underscores. The address has to begin with a letter and must include an @ character. At least one mail domain must be registered for to be able to assign e-mail addresses (see Section 3.1).

A user can be assigned two different types of e-mail addresses:

- The *primary e-mail address* is used for authentication on Postfix and Cyrus. Primary e-mail addresses must always be unique. Only one primary e-mail address can be configured for every user. It also defines the user's IMAP mailbox. If a mail home server is assigned to a user (see Chapter 10), the IMAP inbox is automatically created by a Univention directory listener module. The domain part of the e-mail address must be registered in Univention Management Console (see Section 3.1).
- E-mails to *alternative e-mail addresses* are also delivered to the user's mailbox. As many addresses can be entered as you wish. The alternative e-mail addresses do not have to be unique: if two users have the same e-mail address, they both receive all the e-mails which are sent to this address. The domain part of the e-mail address must be registered in Univention Management Console (see Section 3.1).

E-mail addresses are managed in the UMC module *Users*. The **primary e-mail address** is entered in the **General** tab in the **User account** submenu. **Alternative e-mail addresses** can be entered under **Advanced settings -> Mail**.

### Note

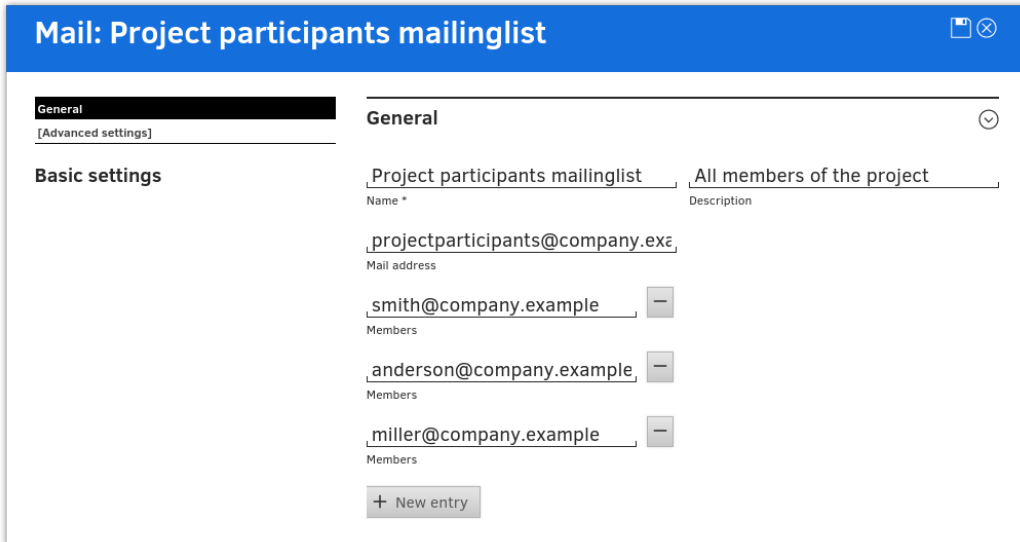
Once the user account is properly configured authentication to the mail stack is possible (IMAP/POP3/SMTP). Please keep in mind that after disabling the account or changing the password the login to the mail stack is still possible for 30min due to authentication cache of the mail stack. To invalidate the authentication cache restart the `saslauthd` service on the mail server. The expiration time of the authentication cache can be configured with the Univention Configuration Registry variable `mail/saslauthd/cache/timeout` on the mail server.

### 3.3. Management of mailing lists

Feedback 

Mailing lists are used to exchange e-mails in closed groups. Each mailing list has its own e-mail address. If an e-mail is sent to this address, it is received by all the members of the mailing list.

**Figure 3.1. Creating a mailing list**



Mail domains are managed in the UMC module *Mail* with the **Mailing list** object type. A name of your choice can be entered for the mailing list under **Name**; the entry of a **Description** is optional. The e-mail address of the mailing list should be entered as the **Mail address**. The domain part of the address needs to be the same as one of the managed mail domains. As many addresses as necessary can be entered under **Members**. In contrast to mail groups (see Section 3.4), external e-mail addresses can also be added here. The mailing list is available immediately after its creation.

In the default settings, everyone can write to the mailing list. To prevent misuse, there is the possibility of restricting the circle of people who can send mails. To do so, the Univention Configuration Registry variable `mail/postfix/policy/listfilter` on the mail server must be set to `yes` and Postfix restarted. **Users that are allowed to send e-mails to the list** and **Groups that are allowed to send e-mails to the list** can be specified under **Advanced settings**. If a field is set here, only authorised users/groups are allowed to send mails.

### 3.4. Management of mail groups

Feedback 

There is the possibility of creating a mail group: This is where an e-mail address is assigned to a group of users. E-mails to this address are delivered to the primary address of each of the group members.


Mail groups are managed in the UMC module *Groups*.

The address of the mail group is specified in the **mail address** input field under **Advanced settings**. The domain part of the address must be the same as one of the managed mail domains.

In the default settings, everyone can write to the mail group. To prevent misuse, there is the possibility of restricting the circle of people who can send mails. To do so, the Univention Configuration Registry variable `mail/postfix/policy/listfilter` on the mail server must be set to `yes` and Postfix restarted.

Users that are allowed to send e-mails to the group and Groups that are allowed to send e-mails to the group can be specified under **Advanced settings**. If a field is set here, only authorised users/groups are allowed to send mails.

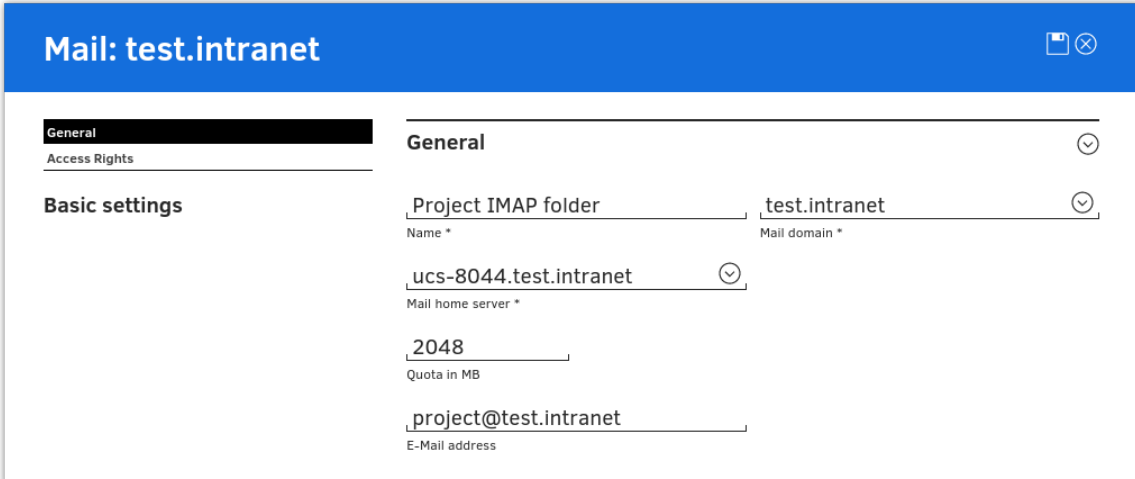
## 3.5. Management of shared IMAP folders

 Feedback 

Shared e-mail access forms the basis for cooperation in many work groups. In UCS, users can easily create folders in their own mailboxes and assign permissions so that other users may read e-mails in these folders or save additional e-mails in them.

Alternatively, individual IMAP folders can be shared for users or user groups. This type of order is described as a shared IMAP folder. Shared IMAP folders are managed in the UMC module *Mail* with the **Mail folder (IMAP)** object type.

**Figure 3.2. Creating a shared IMAP folder**



The screenshot shows the configuration page for a shared IMAP folder. The title is "Mail: test.intranet". On the left, there are tabs for "General" (selected), "Access Rights", and "Basic settings". The main area contains the following fields:

- Name \***: Project IMAP folder
- Mail domain \***: test.intranet
- Mail home server \***: ucs-8044.test.intranet
- Quota in MB**: 2048
- E-Mail address**: project@test.intranet

**Table 3.1. 'General' tab**


Attribute	Description
Name (*)	The name under which the IMAP folder is available in the e-mail clients.
Mail domain (*)	Every shared IMAP folder is assigned to a mail domain. The management of the domains is documented in the Section 3.1.
Mail home server (*)	An IMAP folder is assigned to a mail home server. Further information can be found in Chapter 10.
Quota in MB	This setting can be used to set the maximum total size of all e-mails in this folder.
E-Mail address	<p>An e-mail address can be entered here via which e-mails can be sent directly to the IMAP folder. If no address is set here, it is only possible to write in the folder from e-mail clients.</p> <p>The domain part of the e-mail address must be registered in Univention Management Console (see Section 3.1).</p> <p>As soon as an e-mail address is entered for a folder, at least the IMAP rights <code>lrs</code> are set for the user <code>anyone</code> so that the IMAP server can save e-mails in the IMAP folder.</p>



**Table 3.2. 'Access rights' tab**

Attribute	Description												
Name (*)	<p>Access permissions based on users or groups can be entered here. Users are entered with their user name; the groups saved in Univention Management Console can be used as groups.</p> <p>The access permissions have the following consequences for individual users or members of the specified group:</p> <table border="0"> <tr> <td>No access</td> <td>No access is possible. The folder is not displayed in the folder list.</td> </tr> <tr> <td>Read</td> <td>The user may only perform read access to existing entries.</td> </tr> <tr> <td>Append</td> <td>Existing entries may not be edited; only new entries may be created.</td> </tr> <tr> <td>Write</td> <td>New entries may be created in this directory; existing entries may be edited or deleted.</td> </tr> <tr> <td>Post</td> <td>Sending an e-mail to this directory as a recipient is permitted. This function is not supported by all the clients.</td> </tr> <tr> <td>All</td> <td>Encompasses all permissions of <i>write</i> and also allows the changing of access permissions.</td> </tr> </table>	No access	No access is possible. The folder is not displayed in the folder list.	Read	The user may only perform read access to existing entries.	Append	Existing entries may not be edited; only new entries may be created.	Write	New entries may be created in this directory; existing entries may be edited or deleted.	Post	Sending an e-mail to this directory as a recipient is permitted. This function is not supported by all the clients.	All	Encompasses all permissions of <i>write</i> and also allows the changing of access permissions.
No access	No access is possible. The folder is not displayed in the folder list.												
Read	The user may only perform read access to existing entries.												
Append	Existing entries may not be edited; only new entries may be created.												
Write	New entries may be created in this directory; existing entries may be edited or deleted.												
Post	Sending an e-mail to this directory as a recipient is permitted. This function is not supported by all the clients.												
All	Encompasses all permissions of <i>write</i> and also allows the changing of access permissions.												

## 3.6. Mail quota

 Feedback 

The size of the users' mailboxes can be restricted via the mail quota. When this is attained, no further e-mails can be accepted for the mailbox by the mail server until the user deletes old mails from her account. The limit is specified by the *Mail quota* policy, which is managed under *Policies* in the UMC module *Users*. The maximum size of the mailbox of a user is specified in the **Quota limit (MB)** field.

The user can be warned once a specified portion of the mailbox is attained and then receives a message with every incoming mail that his available storage space is almost full. This warning is shown by the e-mails clients and must thus be supported by them. The administrator can enter the threshold in percent or remaining disk space in kB:

- The threshold for when the warning message should be issued can be configured in the Univention Configuration Registry variable `mail/cyrus/imap/quotawarnpercent`. The value must be entered as a number between 0 and 100 without the percent sign.
- The Univention Configuration Registry variable `mail/cyrus/imap/quotawarnkb` is used to configure the threshold in kilobytes.

The quota is transferred to the quota settings of the Cyrus server during authentication on the mail server. The update interval is evaluated so that the quota settings are only updated once this time period has expired. This interval can be configured in minutes by Univention Configuration Registry variable `mail/cyrus/imap/quotainterval`.

No limit values are set for the IMAP storage space in the default setting. The use of mail quotas can be generally deactivated with the Univention Configuration Registry variable `mail/cyrus/imap/quota`.

## Chapter 4. Spam detection and filtering

Undesirable and unsolicited e-mails are designated as spam. The software SpamAssassin and Postgrey integrated in UCS for the automatic identification of these e-mails. SpamAssassin attempts to identify whether an e-mail is desirable or not based on heuristics concerning its origin, form and content. Postgrey is a policy server for Postfix, which implements grey listing. Grey listing is a spam detection method which denies the first delivery attempt of external mail servers. Mail servers of spammers most often do not perform a second delivery attempt, while legitimate servers do so. Integration occurs via the packages *univention-spamassassin* and *univention-postgrey*, which are automatically set up during the installation of the mail server package.

SpamAssassin operates a point system, which uses an increasing number of points to express a high probability of the e-mail being spam. Points are awarded according to different criteria, for example, keywords within the e-mail or incorrect encodings. In the standard configuration only mails with a size of up to 300 kilobytes are scanned, this can be adjusted using the Univention Configuration Registry variable `mail/antispam/bodysize/limit`. E-mails which are classified as spam - because they exceed a certain number of points - are not delivered to the recipient's inbox by Cyrus, but rather in the *Spam* folder below it. The filtering is performed by a Sieve script, which is automatically generated when the user is created.

The threshold in these scripts as of which e-mails are declared to be spam can be configured with the Univention Configuration Registry variable `mail/antispam/requiredhits`. The presetting (5) generally does not need to be adjusted. However, depending on experience in the local environment, this value can also be set lower. This will, however, result in more e-mails being incorrectly designated as spam. Changes to the threshold do not apply to existing users, but the users can change the value themselves in the Horde web client (see Section 12.4).

There is also the possibility of evaluating e-mails with a Bayes classifier. This compares an incoming e-mail with statistical data already gathered from processed e-mails and uses this to adapt its evaluation to the user's e-mail. The Bayes classification is controlled by the user himself, whereby e-mails not identified as spam by the system can be placed in the *Spam* subfolder by the user and a selection of legitimate e-mails copied into the *Ham* subfolder. This folder is evaluated daily and data which have not yet been collected or were previously classified incorrectly are collected in a shared database. This evaluation is activated in the default setting and can be configured with the Univention Configuration Registry variable `mail/antispam/learndaily`.

The spam filtering can be deactivated by setting the Univention Configuration Registry variable `mail/antispam/active/spam` to `no`. When modifying Univention Configuration Registry variables concerning spam detection, the AMaViS service and Postfix must be restarted subsequently.

## Chapter 5. Identification of viruses and malware

The UCS mail services include virus and malware detection via the *univention-antivir-mail* package, which is automatically set up during the set up of the mail server package. The virus scan can be deactivated with the Univention Configuration Registry variable `mail/antivir`.

All incoming and outgoing e-mails are scanned for viruses. If the scanner recognises a virus, the e-mail is sent to quarantine. That means that the e-mail is stored on the server where it is not accessible to the user. The original recipient receives a message per e-mail stating that this measure has been taken. If necessary, the administrator can restore or delete this from the `/var/lib/amavis/virusmails/` directory. Automatic deletion is not performed.

The AMaViSd-new software serves as an interface between the mail server and different virus scanners. The free virus scanner ClamAV is included in the package and enters operation immediately after installation. The signatures required for virus identification are procured and updated automatically and free of charge by the Freshclam service.

Alternatively or in addition, other virus scanners can also be integrated in AMaViS. Postfix and AMaViS need to be restarted following changes to the AMaViS or ClamAV configuration.

## Chapter 6. Identification of spam sources with *DNS-based Blackhole Lists* (DNSBL)

Another means of combating spam is to use a *DNS-based Blackhole List* (DNSBL) or *Real-time Blackhole List* (RBL). DNSBLs are lists of IP addresses that the operator believes to be (potential) sources of spam. The lists are checked by DNS. If the IP of the sending e-mail server is known to the DNS server, the message is rejected. The IP address is checked quickly and in a comparatively resource-friendly manner. The check is performed *before* the message is accepted. The extensive checking of the content with SpamAssassin and anti-virus software is only performed once it has been received. Postfix has integrated support for DNSBLs ([http://www.postfix.org/postconf.5.html#reject\\_rbl\\_client](http://www.postfix.org/postconf.5.html#reject_rbl_client)).

DNSBLs from various projects and companies are available on the Internet. Please refer to the corresponding websites for further information on conditions and prices.

The Univention Configuration Registry variable `mail/postfix/smtpd/restrictions/recipient/SEQUENCE=RULE` must be set to be able to use DNSBLs with Postfix. It can be used to configure recipient restrictions via the Postfix option `smtpd_recipient_restrictions` (see [http://www.postfix.org/postconf.5.html#smtpd\\_recipient\\_restrictions](http://www.postfix.org/postconf.5.html#smtpd_recipient_restrictions)). The sequential number is used to sort multiple rules alphabetically, which can be used to influence the ordering.

### Tip

Existing `smtpd_recipient_restrictions` regulations can be listed as follows:

```
ucr search --brief mail/postfix/smtpd/restrictions/recipient
```

In an unmodified Univention Corporate Server Postfix installation, the DNSBL should be added to the end of the `smtpd_recipient_restrictions` rules. For example:

```
ucr set mail/postfix/smtpd/restrictions/recipient/80="reject_rbl_client  
ix.dnsbl.manitu.net"
```

## Chapter 7. Integration of Fetchmail for retrieving mail from external mailboxes

Usually, the UCS mail service accepts mails for the users of the UCS domain directly via SMTP. UCS also offers optional integration of the software Fetchmail for fetching emails from external POP3 or IMAP mailboxes.

Fetchmail can be installed via the Univention App Center; simply select the **Fetchmail** application and then click on **Install**.

Once the installation is finished, there are additional input fields in the **Advanced settings -> Remote mail retrieval** tab of the user administration which can be used to configure the collection of mails from an external server. The mails are delivered to the inboxes of the respective users (the primary e-mail address must be configured for that).


The mail is fetched every twenty minutes once at least one e-mail address is configured for mail retrieval. After the initial configuration of a user Fetchmail needs to be started in the UMC module **System services**. In that module the fetching can also be disabled (alternatively by setting the Univention Configuration Registry variable `fetchmail/autostart` to `false`).

**Table 7.1. 'Remote mail retrieval' tab'**

Attribute	Description
Username	The user name to be provided to the mail server for fetching mail.
Password	The password to be used for fetching mail.
Protocol	The mail can be fetched via the IMAP or POP3 protocols.
Remote mail server	The name of the mail server from which the e-mails are to be fetched.
Encrypt connection (SSL/TLS)	If this option is enabled, the mail is fetched in an encrypted form (when this is supported by the mail server).
Keep mails on the server	In the default settings, the fetched mails are deleted from the server following the transfer. If this option is enabled, it can be suppressed.

# Chapter 8. Configuration of the mail server

## 8.1. Configuration of a relay host for sending the e-mails

Feedback 

In the default setting, Postfix creates a direct SMTP connection to the mail server responsible for the domain when an e-mail is sent to a non-local address. This server is determined by querying the MX record in the DNS.

Alternatively, a mail relay server can also be used, i.e., a server which receives the mails and takes over their further sending. This type of mail relay server can be provided by a superordinate corporate headquarters or the Internet provider, for example. To set a relay host, it must be entered as a fully qualified domain name (FQDN) in the Univention Configuration Registry variable `mail/relayhost`.

If authentication is necessary on the relay host for sending, the Univention Configuration Registry variable `mail/relayauth` must be set to `yes` and the `/etc/postfix/smtp_auth` file edited. The relay host, user name and password must be saved in this file in one line.


```
FQDN-Relayhost    username:password
```

The command

```
postmap /etc/postfix/smtp_auth
```

must then be executed for this file to adopt the changes via Postfix.


## 8.2. Configuration of the maximum mail size

Feedback 

The Univention Configuration Registry variable `mail/messagesize` can be used to set the maximum size in bytes for incoming and outgoing e-mails. Postfix must be restarted after modifying the setting. The preset maximum size is 10240000 bytes. If the value is configured to 0 the limit is effectively removed. Please note that e-mail attachments are enlarged by approximately a third due to the base64 encoding.

If Horde (see Chapter 12) is used, the Univention Configuration Registry variables `php/limit/filesize` and `php/limit/postsize` must also be adjusted. The maximum size in megabytes must be entered as the value in both variables. Then the Apache web server has to be restarted.


## 8.3. Configuration of a blind carbon copy for mail archiving solutions

Feedback 

If the Univention Configuration Registry variable `mail/archivefolder` is set to an e-mail address, Postfix sends a blind carbon copy of all incoming and outgoing e-mails to this address. This results in an archiving of all e-mails. As standard the variable is not set. If there is no mailbox for this address, one will be created automatically.

Postfix must then be restarted.

## 8.4. Configuration of soft bounces

Feedback 

If a number of error situations (e.g., for non-existent users) the result may be a mail bounce, i.e., the mail cannot be delivered and is returned to the sender. When Univention Configuration Registry variable `mail/`

`postfix/softbounce` is set to `yes` e-mails are never returned after a bounce, but instead are held in the queue. This setting is particularly useful during configuration work on the mail server.

# Chapter 9. Handling of mailboxes during e-mail changes and the deletion of user accounts

A user's mailbox is linked to the primary e-mail address and not to the user name. The Univention Configuration Registry variable `mail/cyrus/mailbox/rename` can be used to configure the reaction when the primary e-mail address is changed:

- If the variable is set to `yes`, the name of the user's IMAP mailbox is changed. This is the standard setting since UCS 3.0.
- If the setting is `no`, it will not be possible to read previous e-mails any more once the user's primary e-mail address is changed! If another user is assigned a previously used primary e-mail address, she receives access to the old IMAP structure of this mailbox.

The Univention Configuration Registry variable `mail/cyrus/mailbox/delete` can be used to configure, whether the IMAP mailbox is also deleted when a user account is deleted. In the basic setting, the mailboxes are kept when a user account is deleted.



## Chapter 10. Distribution of an installation on several mail servers

The UCS mail system offers the possibility of distributing users across several mail servers. To this end, each user is assigned a so-called mail home server on which the user's mail data are stored. When delivering an e-mail, the responsible home server is automatically determined from the LDAP directory.

It must be observed that global IMAP folders (see Section 3.5) are assigned to a mail home server.

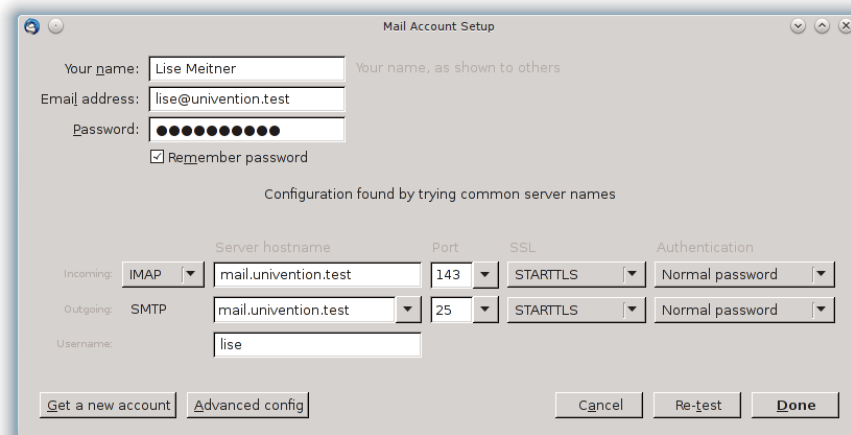
If the mail home server is changes for a user, the user's mail data is *not* moved to the server automatically.

The Cyrus Murder expansion is provided for the implementation of a mailbox cluster.

## Chapter 11. Configuration of mail clients for the mail server

The use of IMAP is recommended for using a mail client with the UCS mail server. STARTTLS is used to switch to a TLS-secured connection after an initial negotiation phase when using SMTP (for sending mail) and IMAP (for receiving/synchronising mail). *Password (plain text)* should be used in combination with *STARTTLS* as the authentication method. The method may have a different name depending on the mail client. The following screenshot shows the setup of Mozilla Thunderbird as an example.

**Figure 11.1. Setup of Mozilla Thunderbird**




	Server hostname	Port	SSL	Authentication
Incoming:	mail.univention.test	143	STARTTLS	Normal password
Outgoing:	mail.univention.test	25	STARTTLS	Normal password

# Chapter 12. Webmail and administration of e-mail filters with Horde

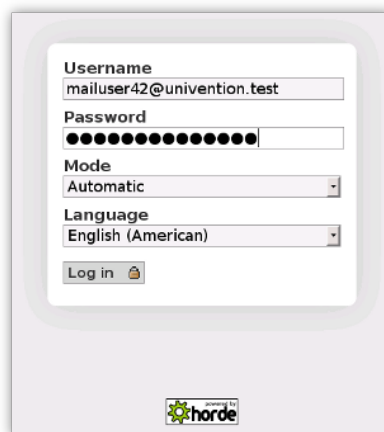
UCS integrates a number of applications from the Horde framework for web access to e-mails and web-based administration of server-side e-mail filter rules based on Sieve. Horde can be installed via the Univention App Center.

## 12.1. Login and overview

Feedback 

The Horde login mask is linked on the system overview page under **Horde web client** and can be opened directly at `http://SERVERNAME/horde/login.php`.

Figure 12.1. Login on Horde




Either the UCS user name or the primary e-mail address can be used as the user name. The webmail interface can be used in a number of display modes. The preferred version can be selected under **Mode**. We recommend the use of the dynamic interface for standard workstations. The remaining documentation refers to this version. Selecting the **Language** has no effect in many web browsers, as the browser's preferred language settings take precedence.

In the top toolbar there are a number of menu points (e.g., **Mail** and **Address Book**), which can be used to switch between the individual modules.

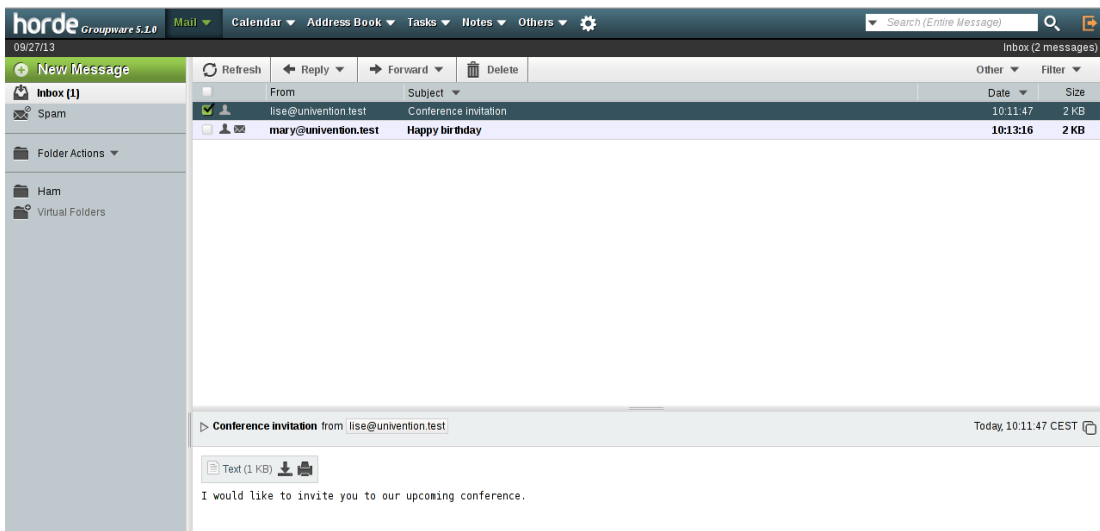
The user can personalise Horde by clicking the cog symbol.

## 12.2. Web-based mail access

Feedback 


Horde offers all the standard functions of an e-mail client such as the sending, forwarding and deletion of e-mails. E-mails can be sorted in folders and are stored in **Inbox** as standard. A *Sent* folder is created automatically the first time an e-mail is sent.

**Figure 12.2. Web mail (Inbox)**



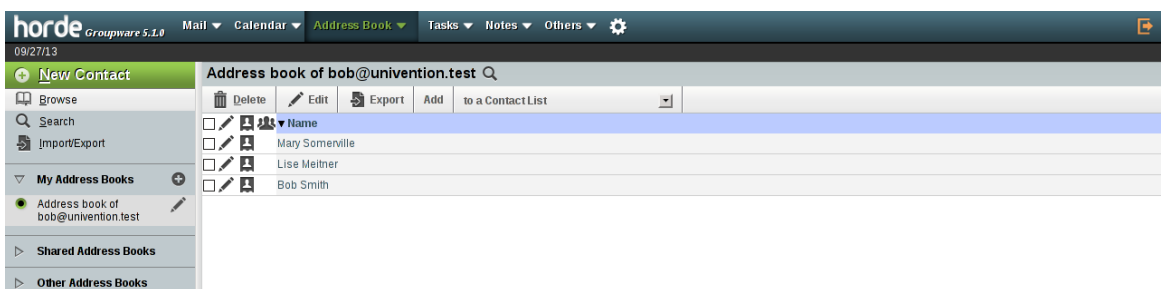
Horde differentiates between two types of deletion: An e-mail deleted with **Delete** is initially moved to the *Trash* folder. From there, it can be moved into any other folder as long as the trash can has not been emptied with **Empty**.

## 12.3. Address book

Feedback 

This module is used to administrate e-mail addresses and additional contact information. The information compiled here are saved in Horde's own SQL database.

**Figure 12.3. Address book for webmail**



Contact information found using the simple or advanced search can then be copied into individual address books and edited there. New contacts can be entered via the **New Contact** menu item. Personal address books can also be created via **My Address Books**.

The **Browse** menu item can be used to display the contents of address books. The lists can be sorted alphabetically by clicking on the preferred column title (surname, first name, etc.). Clicking on the magnifying glass in the header of the respective address book (directly next to the name of the address book) opens a search field that can be used easily to search within the open address book. Individual addresses in a list can be marked with an X for subsequent use, i.e., to export them as a file in a certain file format or to copy them into another address book.

## 12.4. E-mail filters

Cyrus supports server-side filter scripts written in an individual script language called Sieve. The filter module allows the generation of these filter scripts. They apply generally and thus also apply for users accessing their inboxes via a standard mail client.

**Figure 12.4. Filter management in Horde**



Filters can be edited and expanded under **Mail -> Filters**. The filters are applied to incoming e-mails in the consecutively numbered order. Their position can be altered either using the arrows to the right or by entering a number in the **Move** column directly. Individual filter rules can be switched on and off in the **Enabled** column.

The **Spam** filter can be used user-specifically to set which spam threshold should apply. The specified **Spam Level** is the SpamAssassin threshold. An e-mail which returns this value will be sent to the specified folder.

A **Vacation** filter can be used to specify a period in which incoming e-mails are automatically replied to with an answer e-mail by the mail server. The text and subject of the e-mail can be selected as required.

**New Rule** can be used to create new rules, e.g., for the automatic sorting of incoming mails into topic-specific mail folders.

Clicking on **Script** displays the source text of the generated Sieve script.

# Bibliography

[ucs-manual] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. <http://docs.univention.de/manual-4.0.html>.