Install Roundcube Webmail on Ubuntu 22.04/20.04 with Apache/Nginx

Roundcube Features

Roundcube functionality includes:

- Address book
- Folder management
- Message searching
- Message filter
- Spell checking
- MIME support
- PGP encryption and signing
- Mailvelope integration
- Users are able to change their passwords in Roundcube.
- Import MIME or Mbox formatted emails.
- Email Resent (Bounce)
- Support for Redis and Memcached cache
- Support for SMTPUTF8 and GSSAPI
- A responsive skin called *Elastic* with full mobile device support
- OAuth2/XOauth support (with plugin hooks)
- Collected recipients and trusted senders
- Full unicode support with MySQL database
- Support of IMAP LITERAL- extension

Requirements

To follow this tutorial, it's assumed that

- Postfix SMTP server and Dovecot IMAP server have been installed on your Ubuntu 22.04/20.04 server
- You have already installed a LAMP stack or LEMP stack on Ubuntu 22.04/20.04 server.

If not, please click the above links and follow the instructions to complete prerequisites. Note that if you set up your email server using iRedMail before, then your server meets all requirements and Roundcube is already installed on your server.

Now let's proceed to install Roundcube.

Step 1: Download Roundcube Webmail on Ubuntu 22.04/20.04

Log in to your Ubuntu server via SSH, then run the following command to download the latest 1.6 stable version from Roundcube Github repository.

```
wget https://github.com/roundcube/roundcubemail/releases/download/1.6.0/roundcubemail-1.6.0-complete.tar.gz
```

Note: You can always use the above URL format to download Roundcube from command line. If a new version comes out, simply replace 1.6.0 with the new version number. You can check if there's a new release on Roundcube downloade page.

Extract the tarball, and move the newly created folder to web root (/var/www/) and rename it as roundcube at the same time.

```
tar xvf roundcubemail-1.6.0-complete.tar.gz


sudo mkdir -p /var/www/


sudo mv roundcubemail-1.6.0 /var/www/roundcube
```

Change into the roundcube directory.

```
cd /var/www/roundcube
```

Make the web server user (www-data) as the owner of the temp and logs directory so that web server can write to these two directories.

```
sudo chown www-data:www-data temp/ logs/ -R
```

Step 2: Install PHP Extensions

Run the following command to install the required PHP extensions. PHP8.1 is fully supported in the 1.6 release.

```
sudo apt install software-properties-common

sudo add-apt-repository ppa:ondrej/php

sudo apt update


sudo apt install php-net-ldap2 php-net-ldap3 php-imagick php8.1-common php8.1-gd php8.1-imap php8.1-mysql php8.1-curl php8.1-zip php8.1-xml php8.1-mbstring php8.1-bz2 php8.1-intl php8.1-gmp php8.1-redis
```

Step 3: Create a MariaDB Database and User for Roundcube

Log into MariaDB shell as root.

```
sudo mysql -u root
```

Then create a new database for Roundcube using the following command. This tutorial name it roundcubemail, you can use whatever name you like for the database.

```
CREATE DATABASE roundcubemail DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;
```

Next, create a new database user on localhost using the following command. Again, this tutorial name it roundcube, you can use whatever name you like. Replace password with your preferred password.

```
CREATE USER roundcube@localhost IDENTIFIED BY 'roundcube_password';
```

Then grant all permission of the new database to the new user so later on Roundcube webmail can write to the database.

```
GRANT ALL PRIVILEGES ON roundcubemail.* TO roundcube@localhost;
```

Flush the privileges table for the changes to take effect.

```
flush privileges;
```

Exit MariaDB Shell:

```
exit;
```

Import the initial tables to roundcube database.

```
sudo mysql roundcube < /var/www/roundcube/SQL/mysql.initial.sql
```

Step 4: Create Apache Virtual Host or Nginx Config File for Roundcube

Apache

If you use Apache web server, create a virtual host for Roundcube.

```
sudo nano /etc/apache2/sites-available/roundcube.conf
```

Note: If you followed my Postfix/Dovecot tutorial, a virtual host already exists. you should edit the following file. (Delete the existing content.)

```
sudo nano /etc/apache2/sites-available/mail.example.com.conf
```

Put the following text into the file. Replace mail.example.com with your real domain name and don’t forget to set DNS A record for it.

```
<VirtualHost *:80>
  ServerName mail.example.com
  DocumentRoot /var/www/roundcube/

  ErrorLog ${APACHE_LOG_DIR}/roundcube_error.log
  CustomLog ${APACHE_LOG_DIR}/roundcube_access.log combined

  <Directory />
```

```
    Options FollowSymLinks
    AllowOverride All
  </Directory>

  <Directory /var/www/roundcube/>
    Options FollowSymLinks MultiViews
    AllowOverride All
    Order allow,deny
    allow from all
  </Directory>

</VirtualHost>
```

Save and close the file. Then enable this virtual host with:

```
sudo a2ensite roundcube.conf
```

Reload Apache for the changes to take effect.

```
sudo systemctl reload apache2
```

Now you should be able to see the Roundcube web-based install wizard at http://mail.example.com/installer.

Nginx

If you use Nginx web server, create a virtual host for Roundcube.

```
sudo nano /etc/nginx/conf.d/roundcube.conf
```

Note: If you followed my Postfix/Dovecot tutorial, a virtual host already exists. you should edit the following file. (Delete the existing content.)

```
sudo nano /etc/nginx/conf.d/mail.example.com.conf
```

Put the following text into the file. Replace the domain name and don’t forget to set DNS A record for it.

```
server {
  listen 80;
  listen [::]:80;
  server_name mail.example.com;
  root /var/www/roundcube/;
  index index.php index.html index.htm;
  error_log /var/log/nginx/roundcube.error;
  access_log /var/log/nginx/roundcube.access;

  location / {
    try_files $uri $uri/ /index.php;
  }

  location ~ \.php$ {
   try_files $uri =404;
    fastcgi_pass unix:/run/php/php8.1-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    include fastcgi_params;
  }

  location ~ /.well-known/acme-challenge {
    allow all;
  }
 location ~ ^/(README|INSTALL|LICENSE|CHANGELOG|UPGRADING)$ {
    deny all;
  }
  location ~ ^/(bin|SQL)/ {
    deny all;
  }
 # A long browser cache lifetime can speed up repeat visits to your page
  location ~* \.(jpg|jpeg|gif|png|webp|svg|woff|woff2|ttf|css|js|ico|xml)$ {
       access_log        off;
       log_not_found     off;
       expires           360d;
  }
}
```

Save and close the file. Then test Nginx configurations.

```
sudo nginx -t
```

If the test is successful, reload Nginx for the changes to take effect.

```
sudo systemctl reload nginx
```

Now you should be able to see the Roundcube web-based install wizard at http://mail.example.com/installer.

Step 5: Enabling HTTPS

It's highly recommended that you use TLS to encrypt your webmail. We can enable HTTPS by installing a free TLS certificate issued from Let's Encrypt. Run the following command to install Let's Encrypt client (certbot) on Ubuntu 22.04/20.04 server.

```
sudo apt install certbot
```

If you use Nginx, then you also need to install the Certbot Nginx plugin.

```
sudo apt install python3-certbot-nginx
```

Next, run the following command to obtain and install TLS certificate.

```
sudo certbot --nginx --agree-tos --redirect --hsts --staple-ocsp --email you@example.com -d mail.example.com
```

If you use Apache, install the Certbot Apache plugin.

```
sudo apt install python3-certbot-apache
```

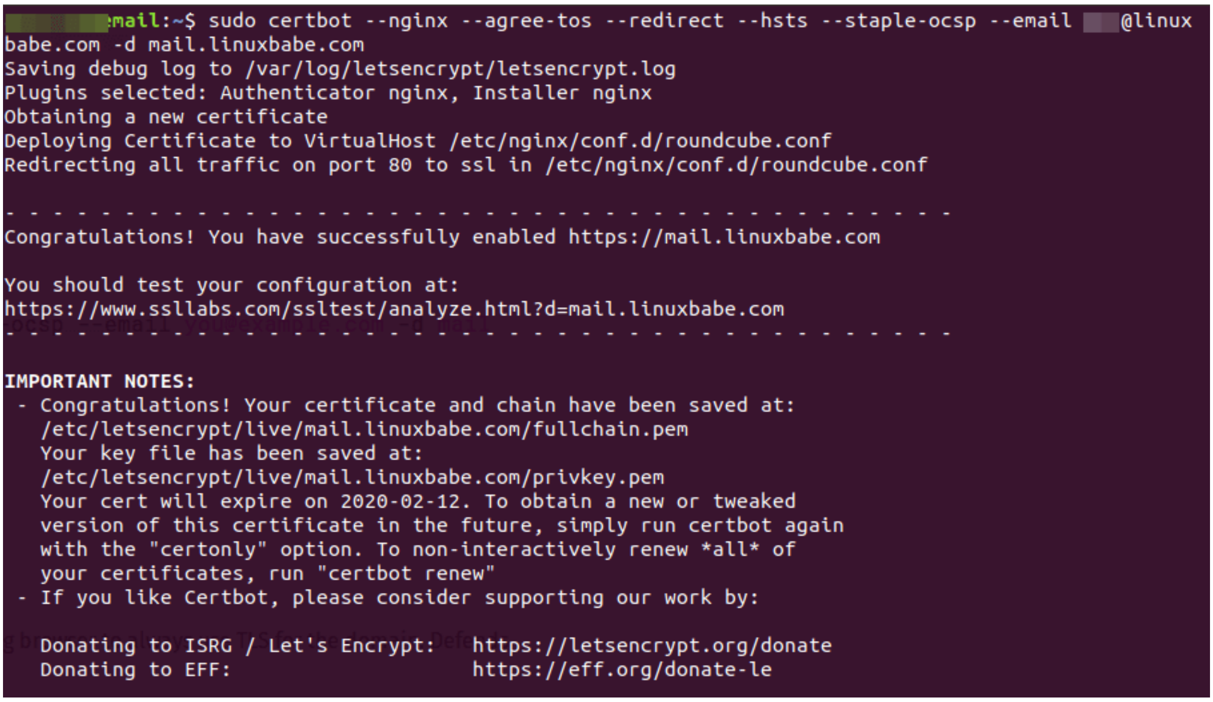
And run this command to obtain and install TLS certificate.

```
sudo certbot --apache --agree-tos --redirect --hsts --staple-ocsp --email you@example.com -d mail.example.com
```

Where

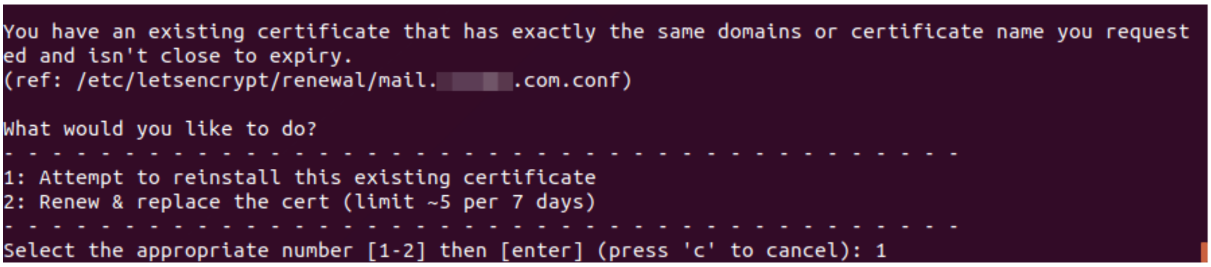
- --nginx: Use the nginx plugin.
- --apache: Use the Apache plugin.
- --agree-tos: Agree to terms of service.
- --redirect: Force HTTPS by 301 redirect.
- --hsts: Add the Strict-Transport-Security header to every HTTP response. Forcing browser to always use TLS for the domain. Defends against SSL/TLS Stripping.
- --staple-ocsp: Enables OCSP Stapling. A valid OCSP response is stapled to the certificate that the server offers during TLS.

The certificate should now be obtained and automatically installed.



```
[redacted]mail:~$ sudo certbot --nginx --agree-tos --redirect --hsts --staple-ocsp --email [redacted]@linux
babe.com -d mail.linuxbabe.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Obtaining a new certificate
Deploying Certificate to VirtualHost /etc/nginx/conf.d/roundcube.conf
Redirecting all traffic on port 80 to ssl in /etc/nginx/conf.d/roundcube.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://mail.linuxbabe.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=mail.linuxbabe.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/mail.linuxbabe.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/mail.linuxbabe.com/privkey.pem
   Your cert will expire on 2020-02-12. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Note: If you followed my Postfix/Dovecot tutorial, and now you install Roundcube on the same server, then certbot will probably tell you that a certificate for mail.example.com already exists as shown below, so you can choose to install the existing TLS certificate to your web server configuration file.



```
You have an existing certificate that has exactly the same domains or certificate name you request
ed and isn't close to expiry.
(ref: /etc/letsencrypt/renewal/mail.[redacted].com.conf)

What would you like to do?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Attempt to reinstall this existing certificate
2: Renew & replace the cert (limit ~5 per 7 days)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
```

Step 6: Adding Local DNS Entry

It’s recommended to edit the /etc/hosts file on the mail server and add the following entry, so that Roundcube won’t have to query the public DNS, which will speed up web page loading a little bit.

127.0.0.1 localhost mail.example.com

Step 7: Configure Roundcube

Go to the Roundcube configuration directory.

cd /var/www/roundcube/config/

Copy the sample configuration file.

sudo cp config.inc.php.sample config.inc.php

Edit the new file.

```
sudo nano config.inc.php
```

Find the following line, which tells Roundcube how to connect to the database.

```
$config['db_dsnw'] = 'mysql://roundcube:pass@localhost/roundcubemail';
```

You need to replace pass with the real Roundcube password. If the password contains special characters, you need to use percent encoding. For example, if the password is mPcEIRxyJhCz8uiWIUopqWzaSTk=, then the line will look like this:

```
$config['db_dsnw'] =
'mysql://roundcube:mPcEIRxyJhCz8uiWIUopqWzaSTk%3D@localhost/roundcubemail';
```

The special character = is represented by %3D.

Then find the following two lines.

```
$config['imap_host'] = 'localhost:143';


$config['smtp_host'] = 'localhost:587';
```

Replace the value as follows:

```
$config['imap_host'] = 'tls://mail.example.com:143';


$config['smtp_host'] = 'tls://mail.example.com:587';
```

Find the following line.

```
$config['des_key'] = 'rcmail-!24ByteDESkey*Str';
```

Replace the default key with some random characters like below.

```
$config['des_key'] = '58kptbzEcNKi/bc9OL90//3ATnQ=';
```

Next, find the following lines

```
// List of active plugins (in plugins/ directory)

$config['plugins'] = [

   'archive',

   'zipdownload',

];
```

By default, only two plugins are enabled. We can enable more plugins like below.

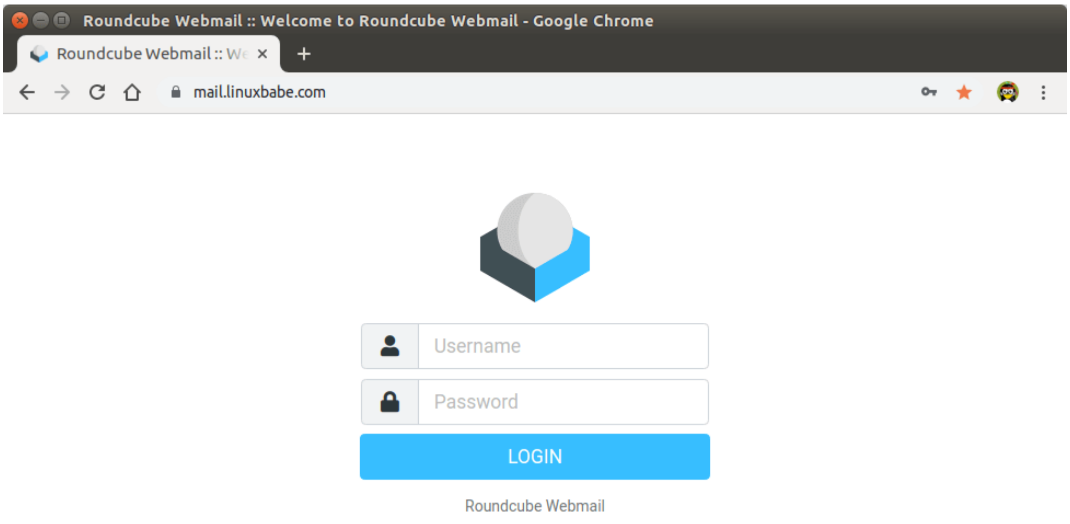
```
// List of active plugins (in plugins/ directory)

$config['plugins'] = ['acl', 'additional_message_headers', 'archive', 'attachment_reminder',
'autologon', 'debug_logger', 'emoticons', 'enigma', 'filesystem_attachments', 'help',
'hide_blockquote', 'http_authentication', 'identicon', 'identity_select', 'jqueryui',
'krb_authentication', 'managesieve', 'markasjunk', 'new_user_dialog', 'new_user_identity',
'newmail_notifier', 'password', 'reconnect', 'redundant_attachments', 'show_additional_headers',
'squirrelmail_usercopy', 'subscriptions_option', 'userinfo', 'vcard_attachments', 'virtuser_file',
'virtuser_query', 'zipdownload'];
```

Finally, we can enable the built-in spell-checker by adding the following line at the end of this file.

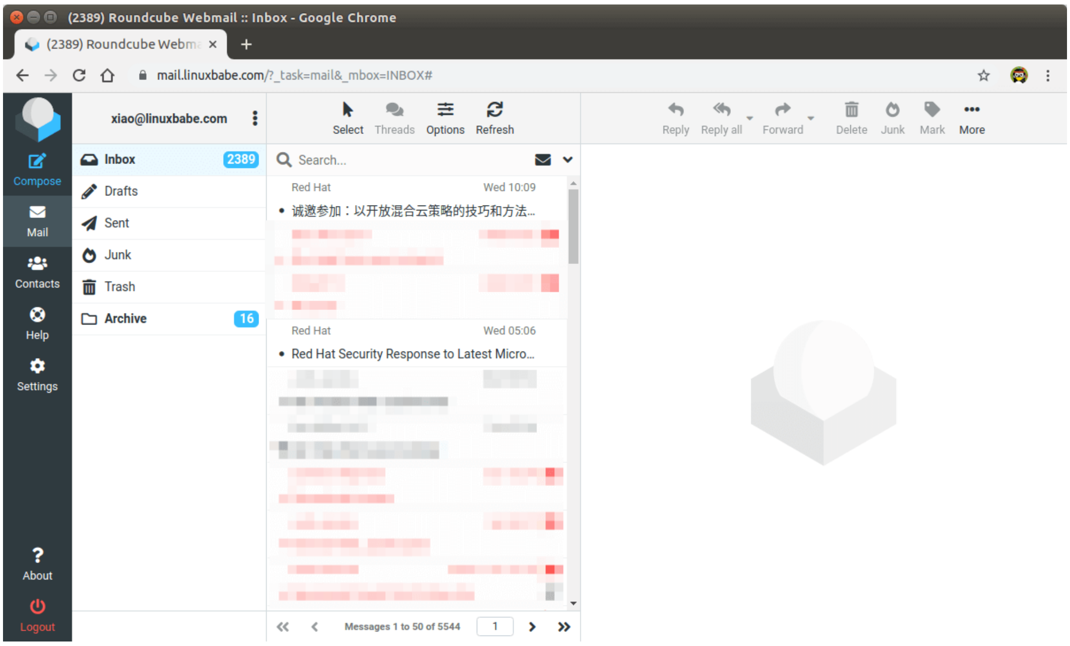
```
$config['enable_spellcheck'] = true;
```

Save and close the file.

Go to your Webmail domain and log in.



Roundcube Webmail interface



Red Hat Wed 10:09
• 诚邀参加：以开放混合云策略的技巧和方法...

Red Hat Wed 05:06
• Red Hat Security Response to Latest Micro...

Messages 1 to 50 of 5544 1

Now you should **remove** the whole installer folder from the document root or make sure that enable_installer option in config.inc.php file is disabled.

```
sudo rm /var/www/roundcube/installer/ -r
```

These files may expose sensitive configuration data like server passwords and encryption keys to the public. Make sure you cannot access the installer page from your browser.

Step 8: Configure the Sieve Message Filter

You can create folders in Roundcube webmail and then create rules to filter email messages into different folders. In order to do this, you need to install the ManageSieve server with the following command.

```
sudo apt install dovecot-sieve dovecot-managesieved
```

By default, Postfix uses its builtin local delivery agent (LDA) to move inbound emails to the *message store* (inbox, sent, trash, Junk, etc). We can configure it to use Dovecot to deliver emails, via the LMTP protocol, which is a simplified version of SMTP. LMTP allows for a highly scalable and reliable mail system and it is required if you want to use the sieve plugin to filter inbound messages to different folders.

Install the Dovecot LMTP Server.

```
sudo apt install dovecot-lmtpd
```

Edit the Dovecot main configuration file.

```
sudo nano /etc/dovecot/dovecot.conf
```

Add lmtp and sieve to the supported protocols.

```
protocols = imap lmtp sieve
```

Save and close the file. Then edit the Dovecot *10-master.conf* file.

```
sudo nano /etc/dovecot/conf.d/10-master.conf
```

Change the lmtp service definition to the following.

```
service lmtp {
 unix_listener /var/spool/postfix/private/dovecot-lmtp {
   group = postfix
   mode = 0600
   user = postfix
  }
}
```

Next, edit the Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

Add the following lines at the end of the file. The first line tells Postfix to deliver emails to local message store via the dovecot LMTP server. The second line disables SMTPUTF8 in Postfix, because Dovecot-LMTP doesn’t support this email extension.

```
mailbox_transport = lmtp:unix:private/dovecot-lmtp
```

```
smtputf8_enable = no
```

Save and close the file. Open the /etc/dovecot/conf.d/15-lda.conf file.

```
sudo nano /etc/dovecot/conf.d/15-lda.conf
```

Scroll to the end of the file, uncomment the mail_plugins line and add the sieve plugin to local delivery agent (LDA).

```
protocol lda {

  # Space separated list of plugins to load (default is global mail_plugins).

  mail_plugins = $mail_plugins sieve

}
```

Save and close the file. If you can find the 20-lmtp.conf file under /etc/dovecot/conf.d/ directory, then you should also enable the sieve plugin in that file like below.

```
protocol lmtp {

    mail_plugins = quota sieve

}
```

Edit the /etc/dovecot/conf.d/10-mail.conf file.

```
sudo nano /etc/dovecot/conf.d/10-mail.conf
```

Sieve scripts are stored under each user's home directory. If you followed my PostfixAdmin tutorial and are using virtual mailbox domains, then you need to enable mail_home for the virtual users by adding the following line in the file, because virtual users don't have home directories by default.

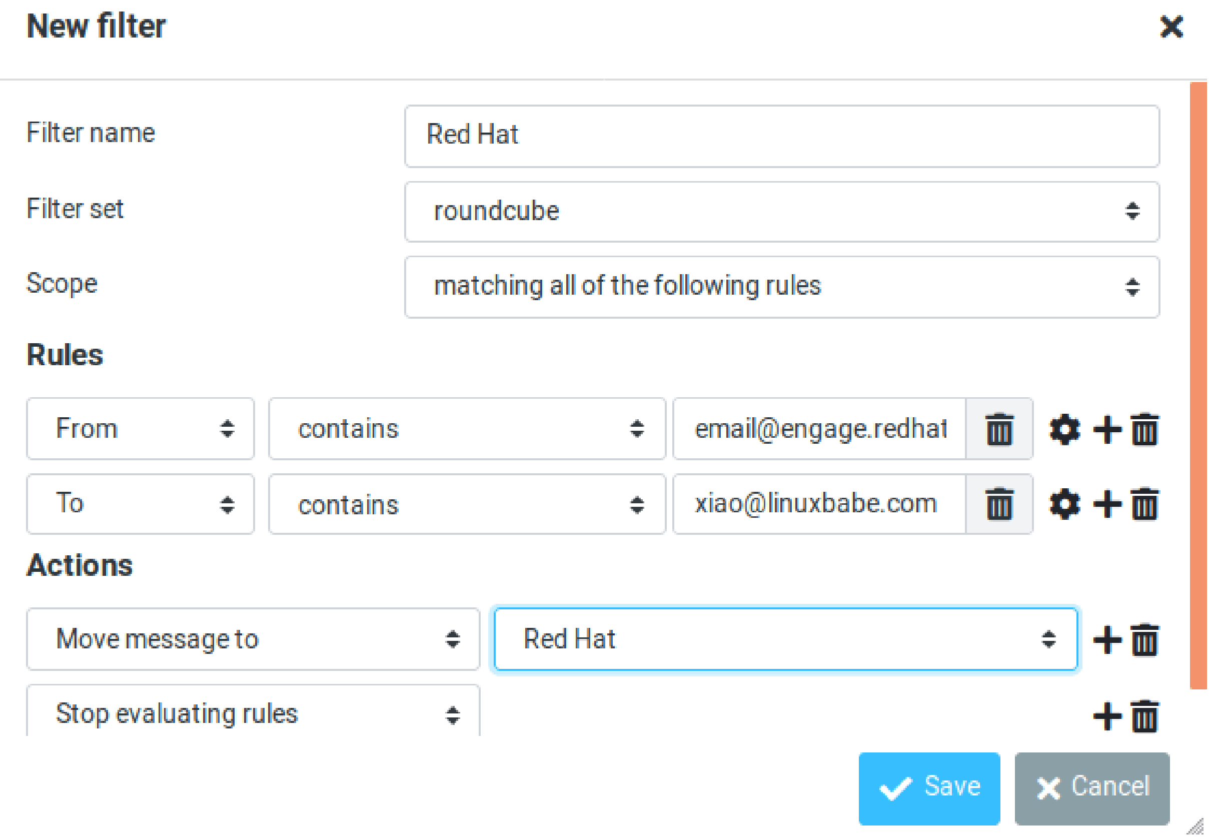
```
mail_home = /var/vmail/%d/%n
```

Save and close the file.

Finally, restart Postfix and Dovecot.

```
sudo systemctl restart postfix dovecot
```

Now you can go to Roundcube webmail, open an email message and click the more button, and select create filters to create message filters. For example, I create a filter that moves every email sent from redhat.com to the Red Hat folder.



New filter

Filter name: Red Hat

Filter set: roundcube

Scope: matching all of the following rules

Rules

From | contains | email@engage.redhat

To | contains | xiao@linuxbabe.com

Actions

Move message to | Red Hat

Stop evaluating rules

If you don’t have the create filter option, it’s probably because you didn’t enable the managesieve plugin. Edit the config.inc.php file.

```
sudo nano /var/www/roundcube/config/config.inc.php
```

At the end of this file, you will find a list of active plugins. add the managesieve plugin in the array. The plugin order doesn’t matter.

```
// ----------------------------------

// PLUGINS

// ----------------------------------

// List of active plugins (in plugins/ directory)

$config['plugins'] = ['acl', 'additional_message_headers', 'archive', 'attachment_reminder',
'autologon', 'database_attachments', 'debug_logger', 'emoticons', 'enigma',
'filesystem_attachments', 'help', 'hide_blockquote', 'http_authentication', 'identicon',
'identity_select', 'jqueryui', 'krb_authentication', 'managesieve', 'markasjunk', 'new_user_dialog',
'new_user_identity', 'newmail_notifier', 'password', 'reconnect', 'redundant_attachments',
'show_additional_headers', 'squirrelmail_usercopy', 'subscriptions_option', 'userinfo',
'vcard_attachments', 'virtuser_file', 'virtuser_query', 'zipdownload'];
```

Save and close the file.

Note that if you move a sieve filter set from an old mail server to your new mail server, you need to go to **Settings** -> **Filters**, then click **Actions** and enable the filter set, or Dovecot LMTP server won’t execute the sieve filter.

Step 9: Removing Sensitive Information from Email Headers

By default, Roundcube will add a User-Agent email header, indicating that you are using Roundcube webmail and the version number. You can tell Postfix to ignore it so recipient can not see it. Run the following command to create a header check file.

```
sudo nano /etc/postfix/smtp_header_checks
```

Put the following lines into the file.

```
/^User-Agent.*Roundcube Webmail/          IGNORE
```

Save and close the file. Then edit the Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

Add the following line at the end of the file.

```
smtp_header_checks = regexp:/etc/postfix/smtp_header_checks
```

Save and close the file. Then run the following command to rebuild hash table.

```
sudo postmap /etc/postfix/smtp_header_checks
```

Reload Postfix for the change to take effect.

```
sudo systemctl reload postfix
```

Now Postfix won’t include User-Agent: Roundcube Webmail in the headers when sending outgoing emails.

Step 10: Configure the Password Plugin in Roundcube

Roundcube includes a password plugin that allows users to change their passwords from the webmail interface. Edit the config.inc.php file.

```
sudo nano /var/www/roundcube/config/config.inc.php
```

Make sure the password plugin in the plugin list at the end of this file. The plugin order doesn’t matter.

```
$config['plugins'] = array('acl', 'additional_message_headers', 'password', .....);
```

Save and close the file.

However, we need to configure this plugin before it will work. Run the following command to copy the distributed password plugin config file to a new file.

```
sudo cp /var/www/roundcube/plugins/password/config.inc.php.dist
/var/www/roundcube/plugins/password/config.inc.php
```

Edit the password plugin configuration file.

```
sudo nano /var/www/roundcube/plugins/password/config.inc.php
```

Find the following line:

```
$config['password_db_dsn'] = '';
```

This parameter is used to tell the password plugin where the user passwords are stored. By default, the value is empty and it will query the roundcube database, which doesn't store user passwords. If you followed my PostfixAdmin tutorial, then user passwords are stored in the postfixadmin.mailbox table, so we need to change the value to:

```
$config['password_db_dsn'] =
'mysql://postfixadmin:postfixadmin_database_password@127.0.0.1/postfixadmin';
```

The tells the password plugin to connect to the postfixadmin database. If you don't remember your postfixadmin database password, you can find it in the /etc/dovecot/dovecot-sql.conf.ext file. If your PostfixAdmin password contains a single quote character, then you can use backslash (\') to escape it.

Then find the following line.

```
$config['password_query'] = 'SELECT update_passwd(%c, %u)';
```

Change it to the following.

```
$config['password_query'] = 'UPDATE mailbox SET password=%P,modified=NOW() WHERE
username=%u';
```

I recommend enabling a password strength checker to prevent users from setting weak passwords. Go to the beginning of this file, you can find the following line.

```
$config['password_strength_driver'] = null;
```

We can use the zxcvbn password strength driver, so change it to:

```
$config['password_strength_driver'] = 'zxcvbn';
```

Add the following line in this file to allow strong passwords only.

```
$config['password_zxcvbn_min_score'] = 5;
```

Note: The $config['password_minimum_score'] parameter doesn't work with the zxcvbn driver, so leave it alone.

You can also set a minimum length for the password. Find the following line.

```
$config['password_minimum_length'] = 0;
```

Change it to:

```
$config['password_minimum_length'] = 8;
```

Recall that we used the ARGON2I password scheme in the PostfixAdmin tutorial, so we also need to configure the password plugin to use ARGON2I. Find the following lines in the file.

```
$config['password_algorithm'] = 'clear';
```

By default, the password will be stored as clear text, change the value to the following to use Dovecot's builtin password algorithm.

```
$config['password_algorithm'] = 'dovecot';
```

Then find the following line, which tells where the Dovecot's password hash generator is located.

```
$config['password_dovecotpw'] = '/usr/local/sbin/dovecotpw'; // for dovecot-1.x
```

Change it to the following.

```
$config['password_dovecotpw'] = '/usr/bin/doveadm pw -r 5';
```

Then find the following line, which tells which password scheme will be used.

```
$config['password_dovecotpw_method'] = 'CRAM-MD5';
```

Change it to:

```
$config['password_dovecotpw_method'] = 'ARGON2I';
```

Find the following line.

```
$config['password_dovecotpw_with_method'] = false;
```

Change false to true. This will add a {ARGON2I} prefix to the hashed password, so you will recognize which password scheme is used.

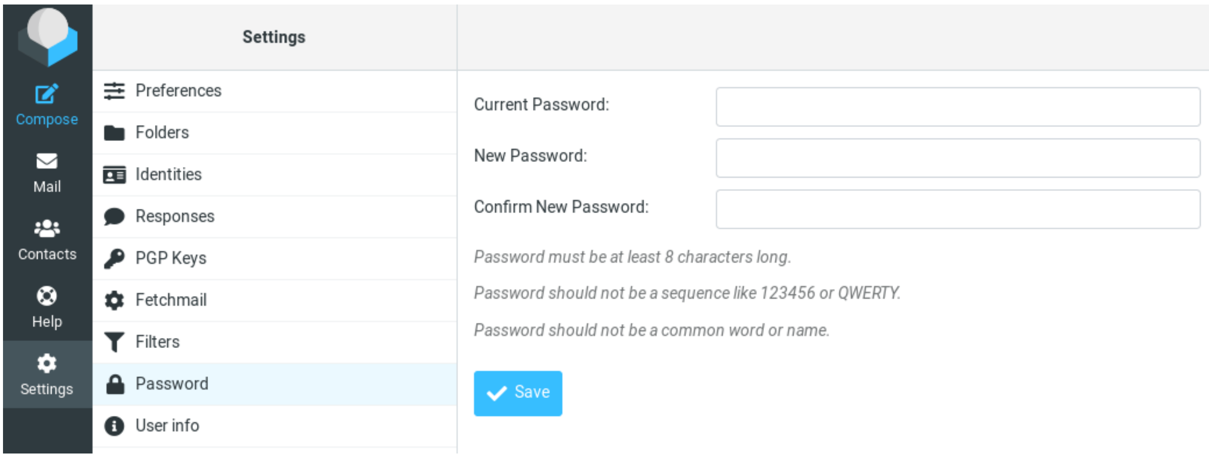
```
$config['password_dovecotpw_with_method'] = true;
```

Save and close the file. Since this file contains the database password, we should allow only the www-data user to read and write to this file.

```
sudo chown www-data:www-data /var/www/roundcube/plugins/password/config.inc.php
```

```
sudo chmod 600 /var/www/roundcube/plugins/password/config.inc.php
```

Now users should be able to change their passwords in the Roundcube webmail interface.



Current Password:

New Password:

Confirm New Password:

Password must be at least 8 characters long.

Password should not be a sequence like 123456 or QWERTY.

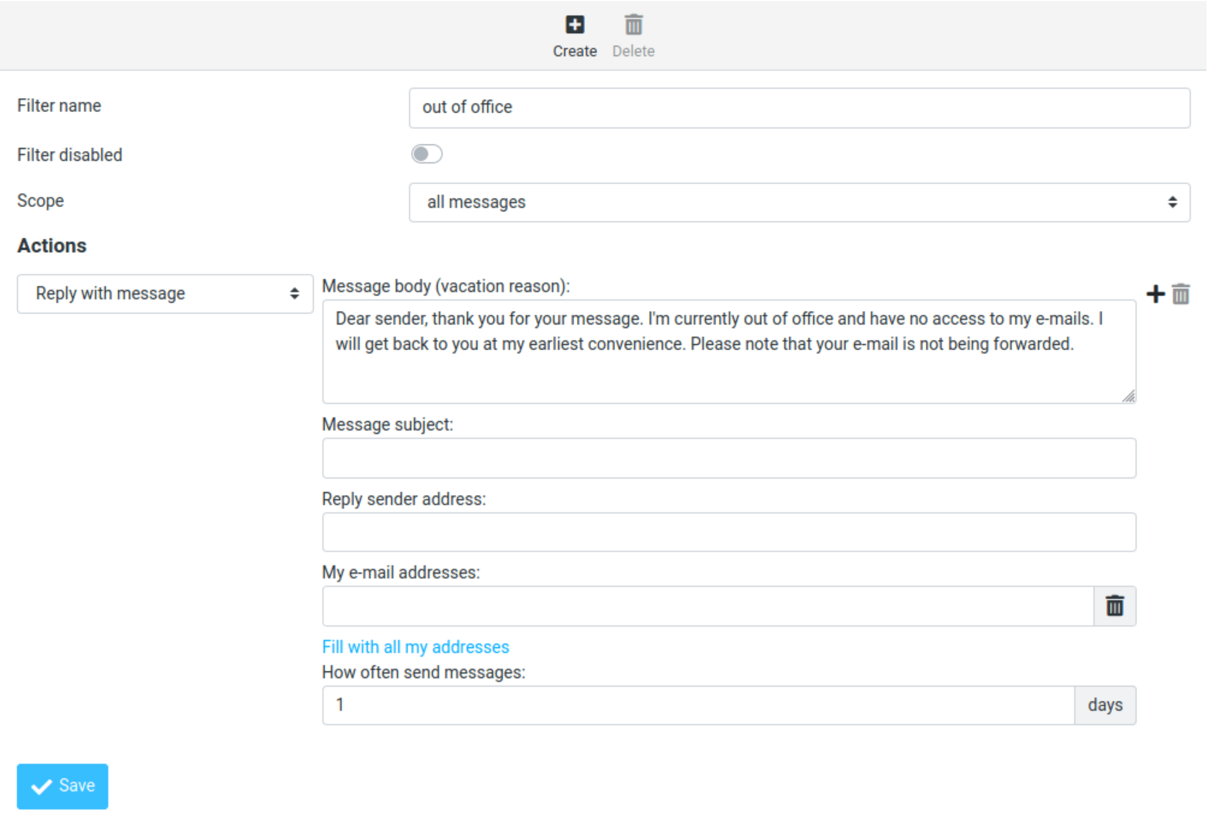
Password should not be a common word or name.

How to Set Up Vacation/Out-of-Office Messages

We can use the sieve filter to create vacation/out-of-office messages. Go to Roundcube **Settings** -> **Filters**. Then click the create button to create a filter.

- Give this filer a name like “out of office”.
- New filters are not disabled, so you can leave the button alone.
- In the **Scope** field, select all messages.
- Select **Reply with message** in the Actions settings, and enter the message that will be automatically sent.

- Enter **1** in **how often send messages**, so the auto-reply will be sent only once per day for each sender. If you set this value to **7**, then the auto-reply will be sent once per 7 days for each sender.
- Leave other text fields empty.
- Click the **Save** button and you are done.



Filter name: out of office

Filter disabled: ○

Scope: all messages

Actions

Reply with message

Message body (vacation reason): Dear sender, thank you for your message. I'm currently out of office and have no access to my e-mails. I will get back to you at my earliest convenience. Please note that your e-mail is not being forwarded.

Message subject:

Reply sender address:

My e-mail addresses:

Fill with all my addresses

How often send messages: 1 days

When you are back to office, you can toggle the “**Filter disabled**” button, and click the **Save** button to disable this filter.

Increase Upload File Size Limit

If you use PHP-FPM to run PHP scripts, then files such as images, PDF files uploaded to Roundcube can not be larger than 2MB. To increase the upload size limit, edit the PHP configuration file.

```
sudo nano /etc/php/8.1/fpm/php.ini
```

Find the following line (line 846).

```
upload_max_filesize = 2M
```

Change the value like below. Note that this value should not be larger than the attachment size limit set by Postfix SMTP server.

```
upload_max_filesize = 50M
```

Then find the following line (line 694).

```
post_max_size = 8M
```

Change the maximum size of POST data that PHP will accept.

```
post_max_size = 50M
```

Save and close the file. Alternatively, you can run the following two commands to change the value without manually opening the file.

```
sudo sed -i 's/upload_max_filesize = 2M/upload_max_filesize = 50M/g' /etc/php/8.1/fpm/php.ini
```

```
sudo sed -i 's/post_max_size = 8M/post_max_size = 50M/g' /etc/php/8.1/fpm/php.ini
```

Then restart PHP-FPM.

```
sudo systemctl restart php8.1-fpm
```

Nginx also sets a limit of upload file size. The default maximum upload file size limit set by Nginx is 1MB. If you use Nginx, edit the Nginx configuration file.

```
sudo nano /etc/nginx/conf.d/mail.example.com.conf
```

Add the following line in the SSL virtual host.

```
client_max_body_size 50M;
```

Save and close the file. Then reload Nginx for the changes to take effect.

```
sudo systemctl reload nginx
```

There are 3 plugins in Roundcube for attachments/file upload:

- database_attachments
- filesystem_attachments
- redundant_attachments

Roundcube can use only one plugin for attachments/file uploads. I found that the database_attachment plugin can be error_prone and cause you trouble. To disable it, edit the Roundcube config file.

```
sudo nano /var/www/roundcube/config/config.inc.php
```

Scroll down to the end of this file. You will see a list of active plugins.
Remove 'database_attachments' from the list. Note that you need to activate at least one other attachment plugin, for example, *filesystem_attachments*.

```
// ----------------------------------

// PLUGINS

// ----------------------------------

// List of active plugins (in plugins/ directory)

$config['plugins'] = ['acl', 'additional_message_headers', 'archive', 'attachment_reminder',
'autologon', 'debug_logger', 'emoticons', 'enigma', 'filesystem_attachments', 'help',
'hide_blockquote', 'http_authentication', 'identicon', 'identity_select', 'jqueryui',
'krb_authentication', 'managesieve', 'markasjunk', 'new_user_dialog', 'new_user_identity',
```

'newmail_notifier', 'password', 'reconnect', 'redundant_attachments', 'show_additional_headers', 'squirrelmail_usercopy', 'subscriptions_option', 'userinfo', 'vcard_attachments', 'virtuser_file', 'virtuser_query', 'zipdownload'];

Save and close the file.

Setting Up Multiple Mail Domains

To host multiple mail domains, please read the following article:

- How to Host Multiple Mail Domains in PostfixAdmin on Ubuntu

Troubleshooting Tips

If you encounter errors, you can check the web server error logs at /var/log/apache2/roundcube_error.log (if you are using Apache), or /var/log/nginx/roundcube.error (if you are using Nginx.), also the Roundcube error logs in /var/www/roundcube/logs/ directory.

Connection to Storage Server Failed

If you see the **Connection to storage server failed** error when trying to log into RoundCube, it's probably because

- Dovecot server isn't running. You can restart Dovecot with sudo systemctl restart dovecot and check its status with systemctl status dovecot.
- You are using a self-signed TLS certificate. Roundcube requires a valid TLS certificate issued from a trusted certificate authority such as Let's Encrypt.
- Your TLS certificate expired. You can renew the Let's Encrypt TLS certificate with sudo certbot renew, then restart Postfix and Dovecot (sudo systemctl restart postfix dovecot).

You can also try adding a custom DNS entry in /etc/hosts file as described in step 8 on the Roundcube server, so Roundcube can properly resolve the mail server hostname.

Could Not Load Message From Server

If you see the "**Internal error: could not load message from server**" error, it's probabaly because you are trying to open an deleted email (invalid URL). Try going to the mail root domain (mail.example.com) to see if it works.

Sieve Message Filter Doesn't Work?

If you followed step 8 to set up sieve filter to the letter, but still can't get it to work, then you can enable debugging in Dovecot to find out what's wrong.

```
sudo nano /etc/dovecot/dovecot.conf
```

Add the following line at the end of this file to enable debugging in Dovecot.

```
mail_debug=yes
```

Save and close the file. Then restart Dovecot.

```
sudo systemctl restart dovecot
```

Next, send a test email to your domain email address and open the mail log file.

```
sudo nano /var/log/mail.log
```

You can find debugging information for Sieve message filter. For example, I found that Dovecot was unable to run my Sieve script.

```
Jan 10 11:35:24 mail dovecot: lmtp(xiao@linuxbabe.com) Debug: sieve: Aborted running script `/var/vmail/linuxbabe.com/xiao/.dovecot.svbin'
```

It turns out that my Sieve filter has too many rules and some of them are conflicting with each other. I delete those conflicting rules and it works again.

Temporary lookup failure (Code: 451)

If you encounter this error when trying to send an email in Roundcube, it's probably something wrong with your Postfix configuration. For example, some folks might have the following error in the /var/log/mail.log file.

```
warning: connect to pgsql server localhost: connection to server at "localhost" (127.0.0.1), port 5432 failed: FATAL: password authentication failed for user "postfixadmin"?connection to server at "localhost" (127.0.0.1), port 5432 failed: FATAL: password authentication failed for user "postfixadmin"?
```

This means your password authentication for the Postfixadmin database is not working.

How to Upgrade Roundcube

It's very simple. For example, here's how to upgrade to Roundcube 1.5.3 after it's released.

Download the Roundcube latest version to your home directory.

```
cd ~


wget https://github.com/roundcube/roundcubemail/releases/download/1.5.3/roundcubemail-1.5.3-complete.tar.gz
```

Extract the archive.

```
tar xvf roundcubemail-1.5.3-complete.tar.gz
```

Change the owner to www-data.

```
sudo chown www-data:www-data roundcubemail-1.5.3/ -R
```

Then run the install script.

```
sudo roundcubemail-1.5.3/bin/installto.sh /var/www/roundcube/
```

Once it's done, log in to Roundcube webmail and click the **About** button to check what version of Rouncube you are using.