Universal Acceptance

EAI Self-Hosting Kit for Linux

Instructions on how to set up and use it

30 June 2025

Universal Acceptance - **Report UASG052B**

TABLE OF CONTENTS

EAI Self-Hosting Kit for Linux

Overview

This package creates a running mail server on a Debian or Ubuntu Linux system. It installs widely used open-source software packages and configures them to run a small EAI mail system, including inbound and outbound SMTP mail including inbound spam filtering and outbound mail submission, a POP and IMAP server, and web mail that uses the submission and IMAP servers.

Once the system is set up, users are encouraged to experiment with it both to see how an EAI mail server works, and how it exchanges mail with other mail systems.

Preparation

Before installing any software on your new mail server, you need to do several preparatory steps.

Select a hosting provider

The software runs on a Linux server, most often a virtual server at a hosting provider. The provider must:

- Provide one of these three versions of Linux: Debian 12, Ubuntu 22 LTS Jammy Jellyfish, or Ubuntu 24 LTS Noble Numbat. Other versions of Linux may work but these are the only ones we have tested. If you have a choice, use Debian 12.
- Assign a dedicated IPv4 address for the server, and if possible an IPv6 address
- Allow access to ports 25, 465, and 587 for mail, as well as 80 and 443 for web mail. At some providers, port 25 is normally blocked but can be opened on request.
- Provide configurable reverse DNS for the IPv4 and if assigned IPv6 address. (Not essential, but without proper reverse DNS mail delivery is often rejected.)

Providers offer a variety of server sizes, on Intel x86 or ARM servers. For a test installation, the smallest server is adequate, on either x86 or ARM.

Select domain names

Choose a domain name for the new server, and a domain name for the mail addresses. For simplicity we suggest using the same name for both, but in production systems it is more common for them to be different, e.g., example.com for mail addresses and mailhost.example.com for the mail server.

The domain names can be ASCII names, internationalized (IDN) names, or a combination, e.g. 邮件测试`.example.com`, which is equivalent to `xn--5nq625ee4u0je.example.com`. EAI

mail works equally well to and from ASCII and IDN domains, so it may be easier to start with an ASCII domain.

It is not necessary to register a new domain. A subdomain of an existing domain works equally well. Either way, be sure that you know how to change the DNS for the domain, so you can add the new records the mail server will need.

Select mailbox names

A mail server usually handles many mailboxes. In theory the mailbox names can include any UTF-8 characters but in practice, they should be easy to type. The mailbox need not be in the same script as the domain name so test@信息测试.中国 and 测试@example.com are both valid mailbox names.

If your mail domain uses IDNs, it can be written in either U-labels or A-labels. The Postfix mail server does not automatically make the two versions of the domain equivalent, but the setup scripts configure both versions to deliver to the same mailbox so you can use either or both.

Note: the current version of Dovecot, which handles the login credentials for POP, IMAP, and mail submission, does not yet have EAI extensions, which means that the internal usernames and passwords used to log in to send or receive mail have to be ASCII. For simplicity, the username for the first created mailbox is `mailbox1`, the second mailbox `mailbox2`, and so forth, with an ASCII password chosen at setup time. These usernames are only used to log in via webmail or mail client programs, and are not visible in sent or received mail. (We expect that Dovecot will eventually add EAI support so we can relax these restrictions.)

Set up an ssh client and create keys

Linux virtual machines are managed using *ssh*, the secure shell. With an ssh client you can log into the virtual machine and type linux shell commands. Ssh clients can create *key pairs*, with a private and public key. When you set up a remote virtual machine, you provide your public key to configure into the newly created machine. Then when you use ssh to log in, your SSH client uses the matching private key to authenticate without needing a password.

MacOS and linux systems include ssh as part of the basic system. To run ssh, open a terminal window and type “ssh *user@hostname*”. To create a key pair, type “ssh-keygen” and press Enter to accept the defaults. Note where it puts the created keys, usually in the directory `~/.ssh`.

Windows 10 and 11 include a version of OpenSSH, the same ssh package that Mac and Linux uses. Another option is PuTTY, a popular freeware ssh client. For either, see the documentation to find out how to create a key pair.

Create the Linux virtual machine

Log into the selected hosting provider and create a virtual machine. As noted above the smallest available configuration should be adequate. Ensure that the machine has a public IPv4 address, and if possible an IPv6 address.

If the provider allows you to specify the server's name, use the full host name you selected above. If the provider allows you to specify an initial user name, use "mailuser". (If you can't specify the name, the setup scripts will create the mailuser later.) It may also ask you to pick a login password for the username.

If possible, have the provider set the reverse DNS for the IPv4 and IPv6 addresses to the hostname. If you have told the provider to set the server's name to the hostname, some providers will set the rDNS automatically. Others have a "set reverse DNS" or "set rDNS" option to do it manually.

Make a note of the IP addresses to use in the next section.

DNS configuration

Before installing the software, set up the DNS configuration. This will require logging in to your DNS provider (often the same as your domain registrar) and add the following DNS records.

A record for server domain name

Add an A record for the domain name you chose for the server, and the IP address the hosting provider assigned. For example, if your server name is `mailhost.example.com` and the IP address is `11.22.33.44`, the A record will look like:

```
mailhost.example.com A 11.22.33.44
```

If your domain name uses IDNs, use the A-label version of the name, that is, if the name is `邮件测试.example.com`, enter it as `xn--5nq625ee4u0je.example.com` since DNS configuration software is generally unaware of IDNs and handles U-labels poorly if at all.

For this and all other records, if it asks you to select a TTL (Time To Live), select 300 seconds or 5 minutes. With a short TTL any updates you make later will take effect more quickly.

AAAA record for server domain

If the provider assigned an IPv6 address, add an AAAA record. For example, if the IP address is 2123:4567::89:abcd, the AAAA record will look like:

```
mailhost.example.com AAAA 2123:4567::89:abcd
```

MX record for mail domain

Add an MX (Mail Exchanger) record to link the mail host domain to the mail domain. If the two domains are the same this record is technically optional, but it's good practice to add it anyway for clarity.

If the domains are different, say `mailhost.example.com` and `example.com`, the MX record would look like:

```
example.com MX 0 mailhost.example.com.
```

The number 0 is the "priority" of the mail server which doesn't matter if there is only one server, but has to be present anyway.

If the mail domain and server domain are the same, the MX record has that domain in both places:

```
example.com MX 0 example.com.
```

SPF record for mail domain

SPF (Sender Policy Framework) is a mail security scheme that describes the hosts that are supposed to send a domain's mail. Many mail providers require that you publish an SPF record if you want them to accept your mail. The SPF record is a TXT record at the mail domain (the same domain as the MX record.) Install this SPF record at the mail domain:

```
example.com TXT "v=spf1 mx ~all"
```

In this SPF record, "mx" means that the MX host will send mail, and "~all" means that other hosts might also send mail, e.g., if a message is forwarded.

Once these DNS records are installed, you can proceed to install the software. The installation script will create a DKIM DNS record that you'll need to install later.

Install and set up software

Log into the server you created using ssh. Depending on the way the hosting provider set up the virtual machine, you may ssh to "root@*hostname*" or a different user name. If you provided an ssh public key you should be logged in directly. If not you may have to enter the password you chose. Consult your provider's documentation for details.

Once you are logged in you should see a shell prompt like this:

```
Last login: Thu Dec 19 04:25:40 2024 from 12.34.56.78
root@torn:~#
```

If the user name was not "root", the prompt will end with $ rather than # to indicate that you are not a system super-user. Use the "wget" command to download the installation script. Check the archive where the package is located to see if the URL to get has changed:

```
root@torn:~# wget
https://raw.githubusercontent.com/icann/eaiselfhost/refs/heads/main/
eaiselfhost.sh

--2025-07-09 09:27:22--
https://raw.githubusercontent.com/icann/eaiselfhost/refs/heads/main/
eaiselfhost.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)...
2606:50c0:8002::154, 2606:50c0:8003::154, 2606:50c0:8000::154, ...
Connecting to raw.githubusercontent.com
(raw.githubusercontent.com)|2606:50c0:8002::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13884 (14K) [text/plain]
Saving to: 'eaiselfhost.sh'
eaiselfhost.sh
100%[=========================================>]  13.56K  --.-KB/s
in 0s
2025-07-09 09:27:22 (70.0 MB/s) - 'eaiselfhost.sh' saved
[13884/13884]
```

Starting the setup script

Now use the linux shell to run the downloaded script. It should identify the system it is running on, Ubuntu or Debian, and then update the preinstalled software to the most recent versions.

```
root@torn:~# sh eaiselfhost.sh
Installing on debian.
Installing initial software
=== update software catalog
 --- lengthy update output here ---

=== upgrade preinstalled packages
--- lengthy upgrade output here ---

=== install idn2 ...

This computer's domain name is xn--5nqv22n (郵件)
Is that the correct name you wish to use for this computer? (y)
```

If this is not the correct domain name, say n and enter the correct name.

```
Is that the correct name you wish to use for this computer? (y) n
Enter the correct full domain name using A-labels:
torn.xn--vuq861bgvjrx4a.xn--fiqs8s

This computer's domain name is torn.xn--vuq861bgvjrx4a.xn--fiqs8s
(torn.信息测试.中国)
Is that the correct name you wish to use for this computer? (y)
```

Then it will ask if the mail domain is the same. If not, say n and enter the mail domain you chose above.

```
Do you want to use the same domain name for your mail addresses? (y)
Mail domain is torn.xn--vuq861bgvjrx4a.xn--fiqs8s (torn.信息测试.中
国)
```

Check the DNS configuration

Now the script will check that the initial DNS setup is correct.

```
Check for DNS records

Found valid A record 'torn.xn--vuq861bgvjrx4a.xn--fiqs8s. A
71.19.148.118'
Found valid IPv4 PTR record 'torn.xn--vuq861bgvjrx4a.xn--fiqs8s.'
found valid AAAA record 'torn.xn--vuq861bgvjrx4a.xn--fiqs8s. AAAA
2605:2700:0:2:a800:ff:fe72:8531'
Found valid IPv6 PTR record 'torn.xn--vuq861bgvjrx4a.xn--fiqs8s.'
Found valid MX record 'torn.xn--vuq861bgvjrx4a.xn--fiqs8s. 10
torn.xn--vuq861bgvjrx4a.xn--fiqs8s.'
Found valid SPF record 'v=spf1 mx ~all'
DNS set up correctly, continuing
```

If the setup is not correct, it will encourage you to stop and correct the DNS entries, then restart installation.

```
Error: no valid DNS SPF record for this server.  Add this record in your DNS and
then rerun this script.

   torn.xn--vuq861bgvjrx4a.xn--fiqs8s. IN TXT "v=spf1 mx ~all"

This mail server will not work until the DNS is set up,
so you should stop, make the DNS changes, and then rerun this script.
Do you want to continue anyway, even though the server will not work? (n)
```

If you continue anyway, it will install most of the software but it will be unable to configure SSL certificates (see below.)

Then it will create the mailuser account if it does not already exist.

Create mailbox(es)

The next step is to create one or more mailboxes in the mail domain.

The mailbox names can be any UTF-8 text, but as described above, due to limitations in the Dovecot software, each mailbox is associated with an internal ASCII name like `mailbox1` and `mailbox2`, and has an ASCII password.

Enter the mailbox name and password for each mailbox.

```
Updating mail configuration
Enter mailbox name for mailbox 1: bjørn
Password for mailbox 1: bjørn
Password must be ASCII printing characters and cannot contain colons, try again
Password for mailbox 1: sekret123
Do you want to add another mailbox? (n)
```

Once you have created the mailboxes, it will display a summary of the internal user names, passwords, and mail addresses, and create the internal directories for each mailbox:

```
Mailbox   Password   Mail address
mailbox1  sekret123  bjørn@torn.信息测试.中国

Creating mailbox directories
```

You can add more mailboxes later and manually edit the mailbox names and passwords, as described below.

Create a DKIM key

DKIM is a mail authentication scheme that puts cryptographic signatures on messages. Recipient systems check the signature using a verification key stored in the DNS. The installation script creates DKIM signing and verification keys. You must install the verification key in the DNS so other systems can find it and verify the mail the mail server sends.

```
=== Create DKIM keys

You must add this DKIM record to your DNS if you have not already.  Copy it to a
safe place before proceeding

s1._domainkey.torn.xn--vuq861bgvjrx4a.xn--fiqs8s.   IN    TXT    ( "v=DKIM1;
h=sha256; k=rsa; "
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQyor116qAn+w7rtd4Sgcsm1z4go6ENv2+eAfQy3x
E+1GTMueARiUM2sEiHXW++qE/TqCioXc23F9S77oNo+AkQFmqEBVBX8COHz9qxcHJijNThXMs20nEXhiNc
FppW3/PbxgcIpQ6M57A7FGNaYH+Lrcf9KMlJcGfwYx/VPRYIwIDAQAB" )  ; ----- DKIM key s1
for torn.xn--vuq861bgvjrx4a.xn--fiqs8s
```

```
Press Enter when you have copied those records to add to your DNS:
```

Copy and paste this DKIM key to your DNS. Note that the name of the key record is

`s1._domainkey.`*`mailname`*

The DNS TXT record contains two strings, one starting with v=DKIM1 and the other with p= and the key. Both strings need to be copied separately into the DNS record.

If you need to do the DNS update later, the key record is stored in a file on your server for later reference.

Set up webmail and finish

Once the DKIM key is generated and installed, press enter to finish the setup. The rest of the process is automatic, starting the web server and installing a TLS certificate for the web, SMTP, and POP/IMAP servers:

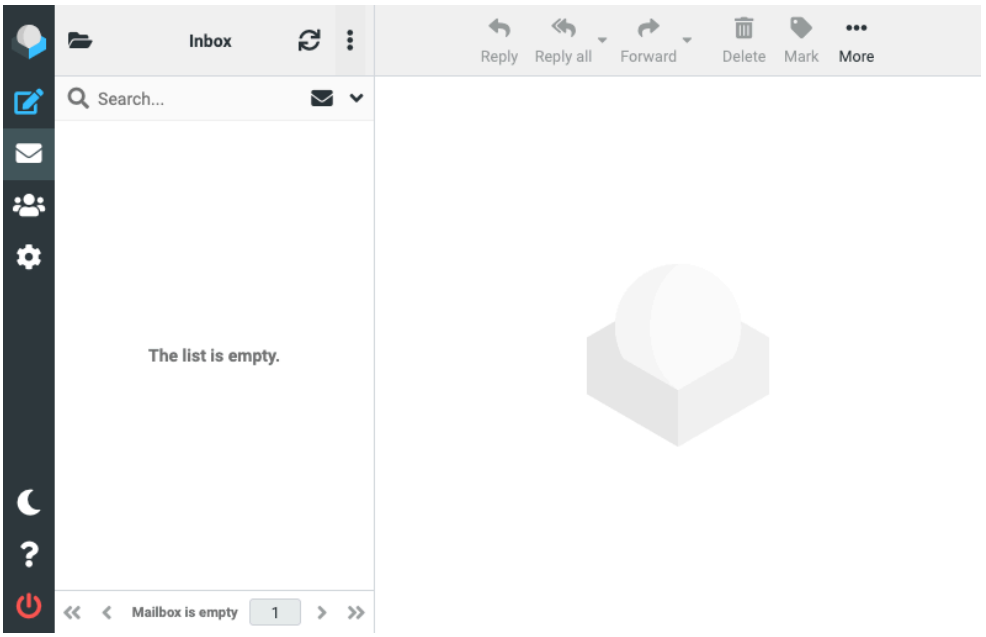
```
=== configure web server
Start web server.
Get signed TLS certificate for web server.
Install TLS certificate into mail server.

=== System should be running.
Try the webmail at https://torn.xn--vuq861bgvjrx4a.xn--fiqs8s
The DKIM key record is at /etc/dkimkeys/s1.txt
The postfix mailbox map is at /etc/postfix/vmailbox
The dovecot password file is at /etc/dovecot/users
In case of trouble, see installation log file at /tmp/install-log
```

If the DNS checks above failed, rather than getting signed certificates, it will say `Using self-signed certs` which will provoke warnings in most web browsers when you try to use the webmail. If you later fix the DNS records, you can rerun the setup script and it will install the signed certificates.

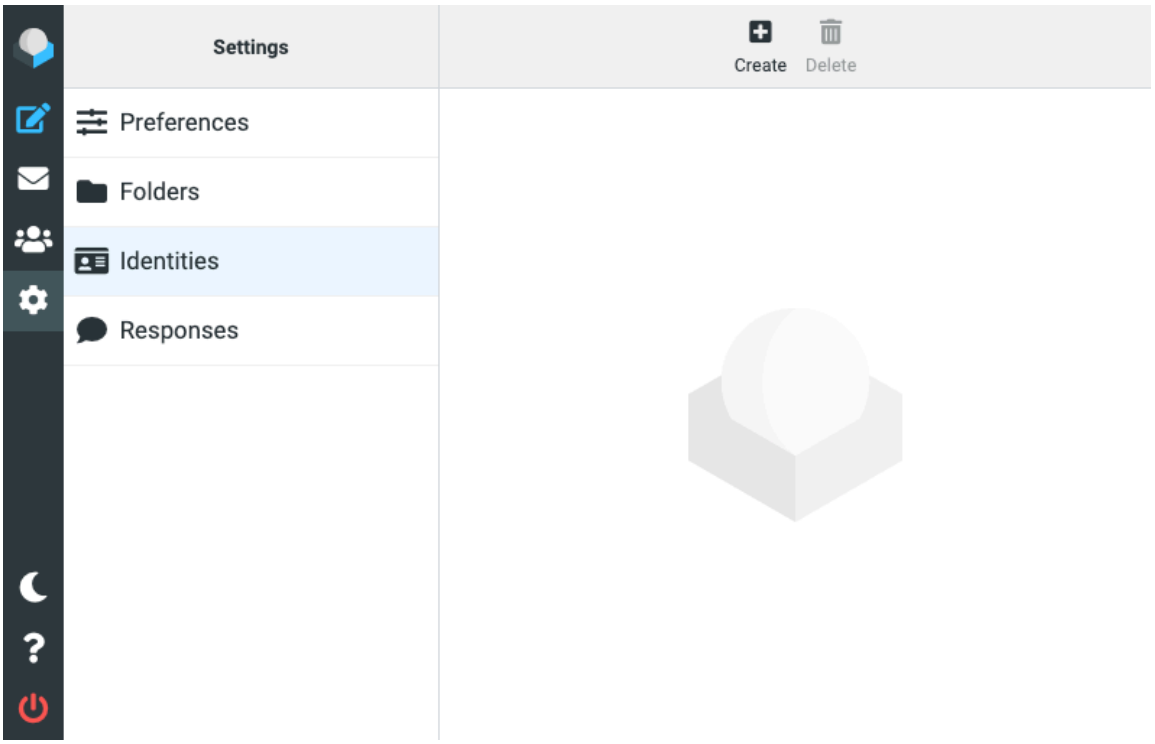
Use the web mail

The mail and web servers should now be running. Open the web server in a browser and you should see the Roundcube webmail login page. Enter the internal username, usually mailbox1, and the password you selected and click LOGIN:

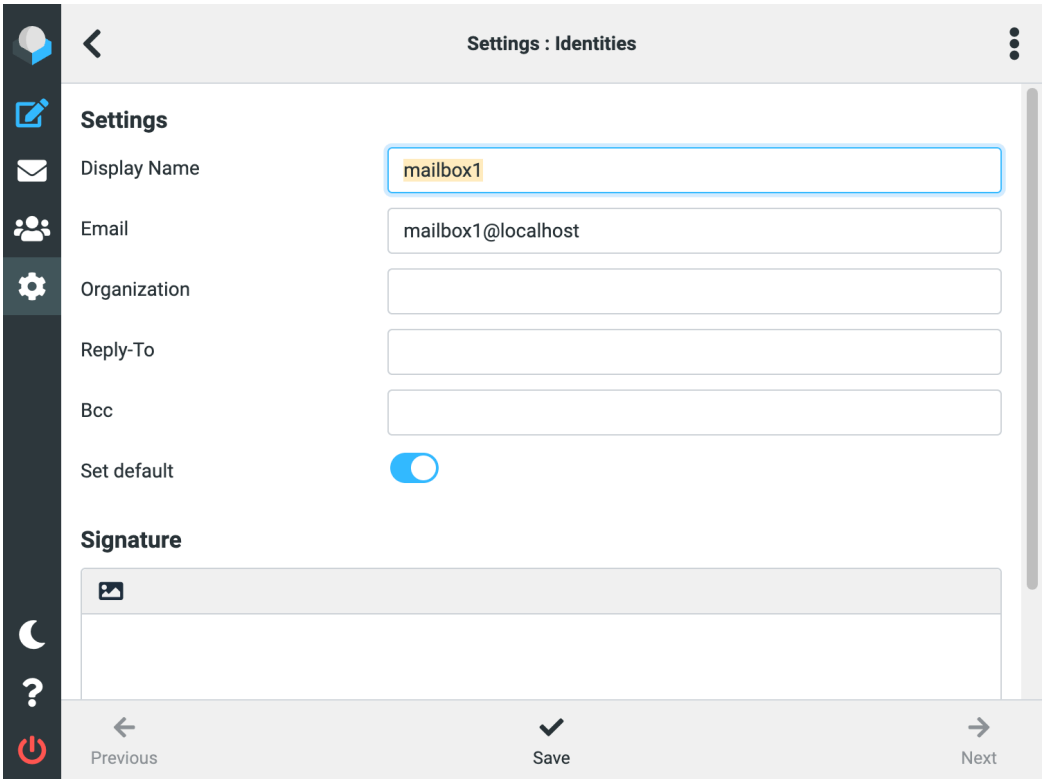
It should log you in and show you an empty mailbox.



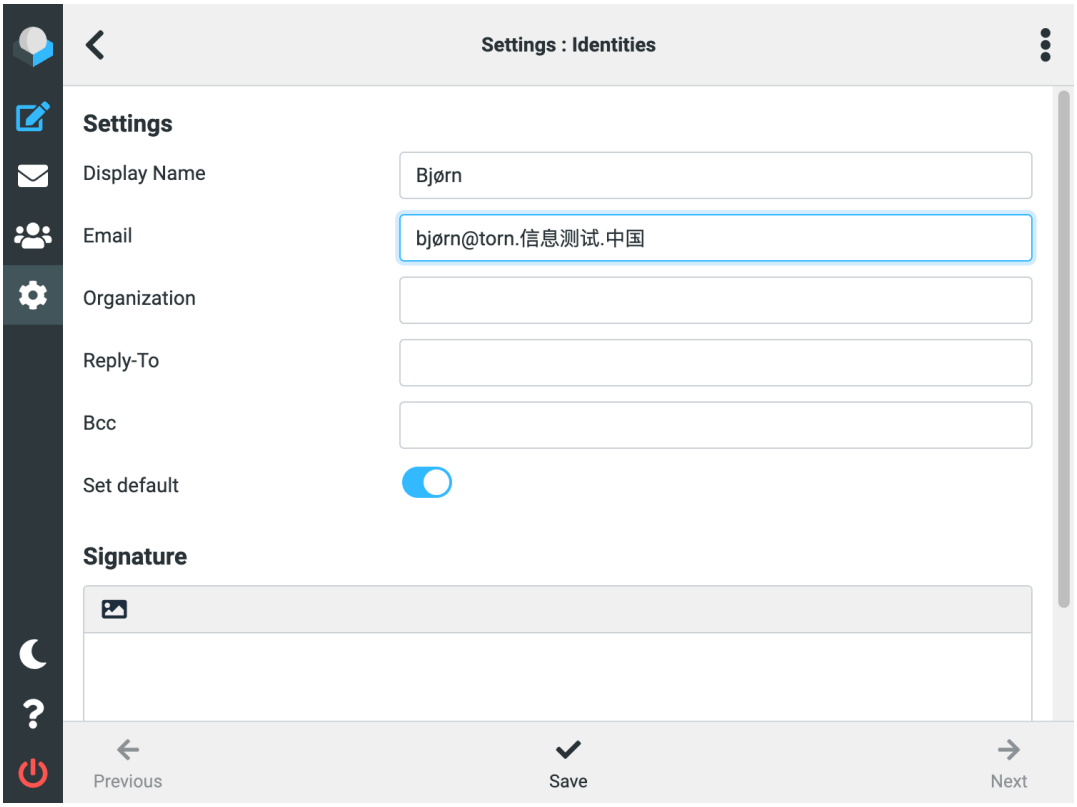
Before you can send any mail, you need to configure the correct mailbox name into Roundcube. Click the little gear at the left:



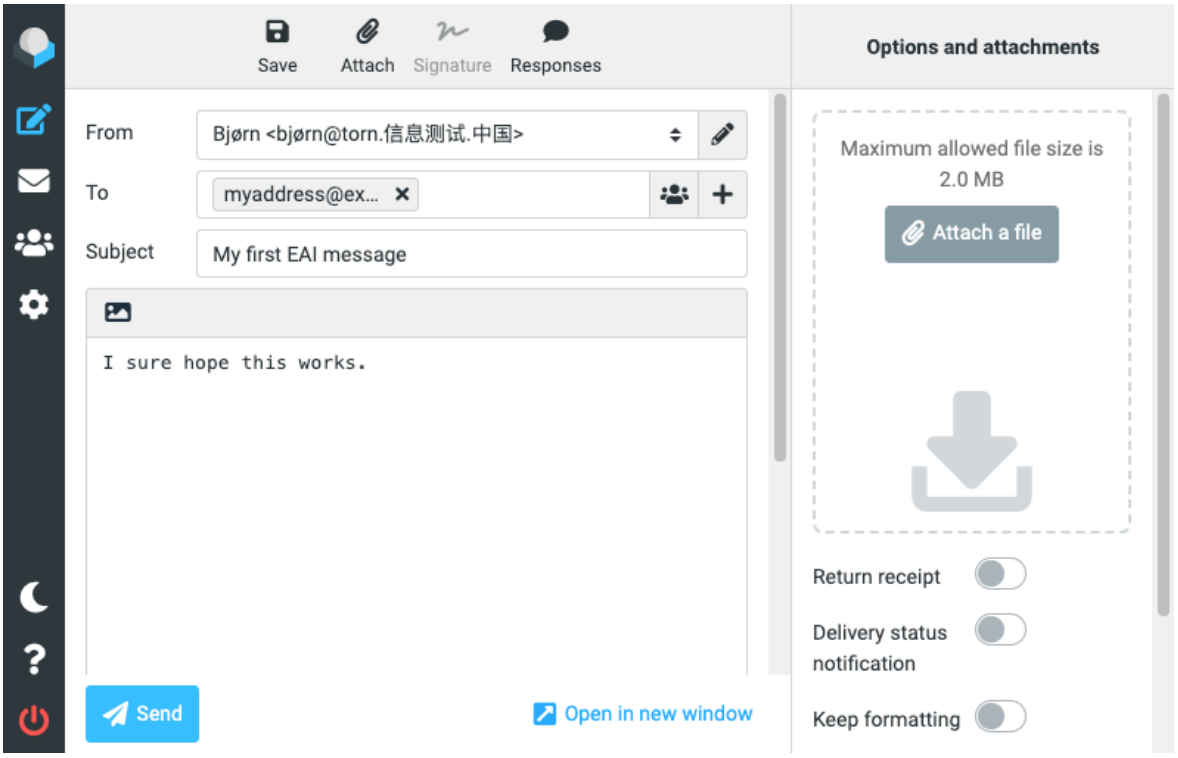
Click Identities and then click on the mailbox1 identity:



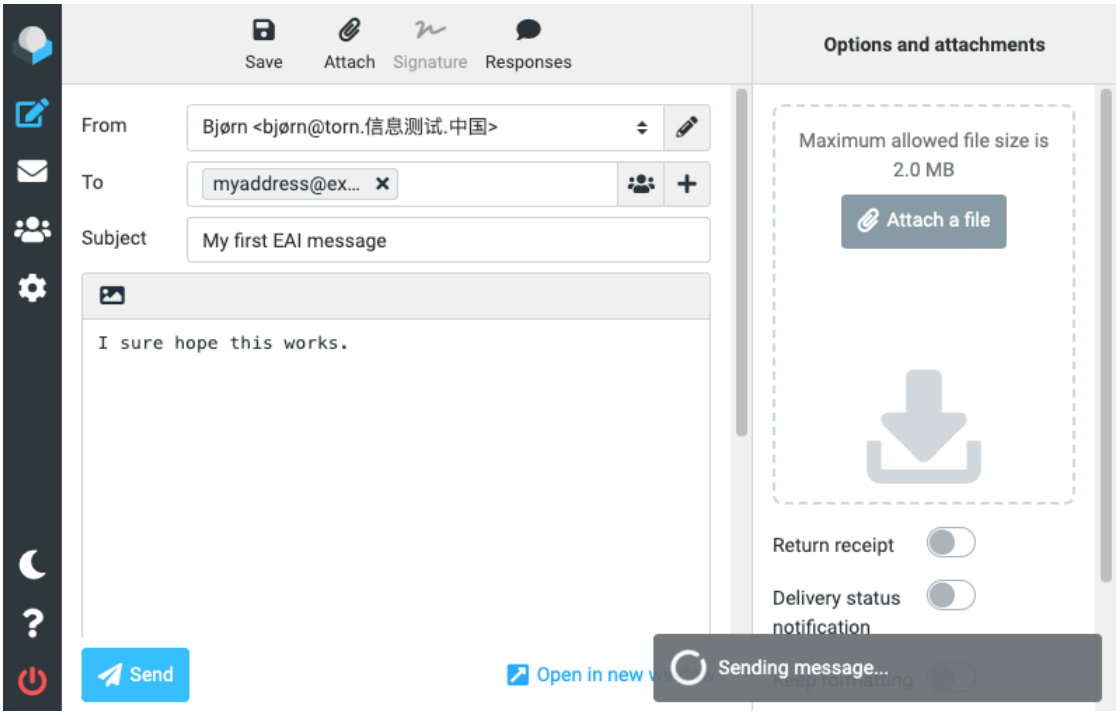
Update the display name and Email to the account's actual name, as shown earlier in the list of mailboxes you set up:



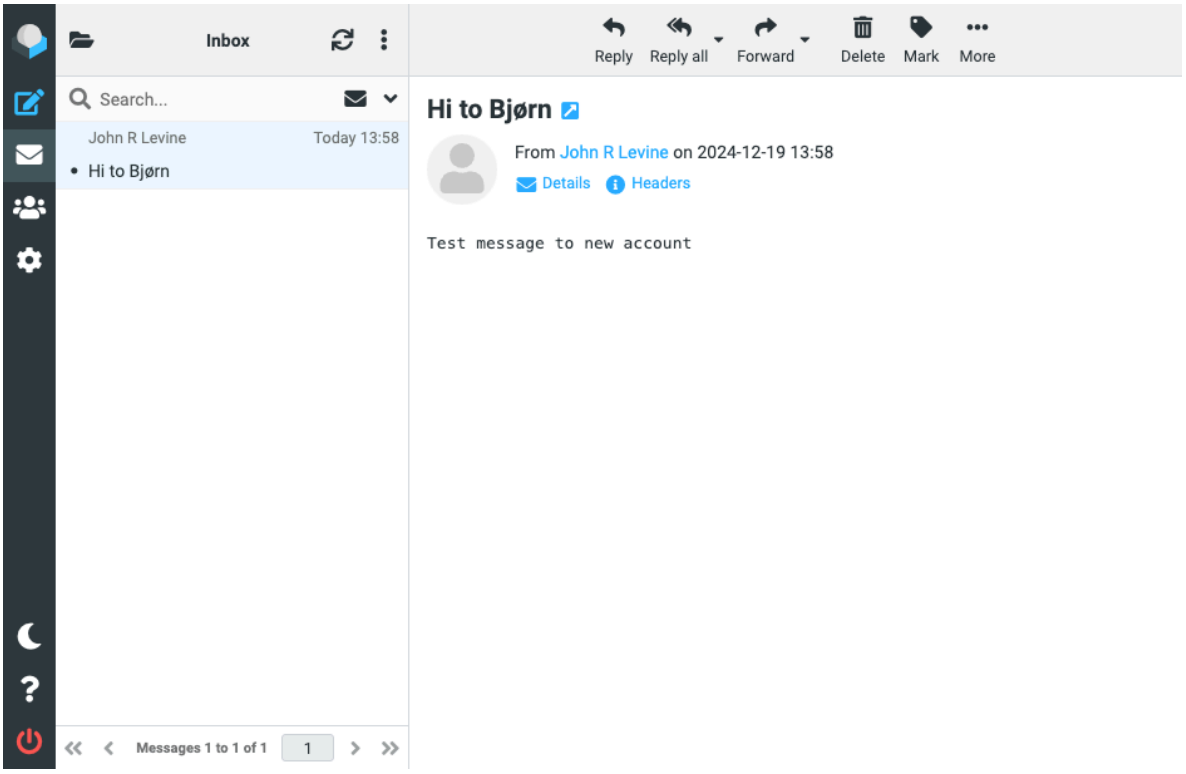
Then click Save, and click the pencil icon at the upper left to compose your first message:



Note that the From: address is set to the EAI address you just configured. Enter the recipient's address, subject, and a message, and click Send. It should say Sending Message, and then report success.



Now you can send and receive mail at your new address. Click the little envelope to see incoming mail.



Set up mail in a separate mail program

You can also send and receive mail in a separate mail program such as Outlook or Thunderbird. Provide this information to set up the account:

Mail address: the address you configured

Incoming mail server: the hostname of your mail server, select IMAP, preferably with TLS. If it asks for a port number, select 995 or 143.

Outgoing mail server: the hostname of your mail server, If it asks for a port number, select 465 or 587

Username and password: the same name and password you used for webmail.

Troubleshooting hints

The initial software update can be quite complicated, for example:

```
=== update software catalog

Hit:1 http://ports.ubuntu.com/ubuntu-ports jammy InRelease
Get:2 http://ports.ubuntu.com/ubuntu-ports jammy-updates InRelease [128 kB]
...

Fetched 6,200 kB in 2s (2,929 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done56 packages can be upgraded. Run 'apt list
--upgradable' to see them.

=== upgrade preinstalled packages
Reading package lists... Done
Building dependency tree... Done
...

# Patches available for the local privilege escalation issue ...
The following NEW packages will be installed:
linux-headers-5.15.0-128 linux-headers-5.15.0-128-generic ...

...

55 upgraded, 7 newly installed, 0 to remove and 1 not upgraded.
1 standard LTS security update
Need to get 468 MB/469 MB of archives.
After this operation, 626 MB of additional disk space will be used.
```

If it asks whether you want to continue to upgrade, say Y to start the potentially lengthy upgrade process. In some cases it may pop up a screen warning you that a new linux kernel

is available and you will need to reboot, or a list of system services to restart. Press enter to acknowledge each.

If it says that a reboot is required, you can wait to reboot until after the software installation is complete. Then type “reboot” or “sudo reboot” to reboot the system, wait a few minutes for the reboot to complete, and then log back in with ssh.

Installation without Dovecot

If you want to install a subset of the packages without Dovecot and the other components that depend on it, pass the “nodovecot” argument to the setup script.

```
# sh eaiselfhost.sh nodovecot
```

The subset includes Postfix for incoming and outgoing mail, but no POP or IMAP and no authentication for mail submission.

Managing your mail server

For the most part your mail server should run automatically. You can inspect and edit the control files and mail messages using linux shell commands.

The mailboxes

All mailboxes belong to the linux “mailuser” account, under the directory `/home/mailuser/users`. Each mailbox is in a directory with its internal name such as user1. Under that directory is a standard Maildir mailbox, with three subdirectories, new, cur, and tmp, with each message in a file. Incoming mail is delivered to files in new, and moved to cur once Dovecot has seen them. A typical layout is:

```
root@torn:/home/mailuser/users# ls -R user1
User1:
Maildir

user1/Maildir:
cur    dovecot.index.log dovecot.mailbox.log dovecot-uidvalidity new tmp
dovecot.index.cache  dovecot.list.index.log  dovecot-uidlist
dovecot-uidvalidity.6764696d     subscriptions

user1/Maildir/cur:

1734634698.Vca01I637c4M400024.torn.xn--vuq861bgvjrx4a.xn--fiqs8s:2,S
1734635917.Vca01I63b59M561171.torn.xn--vuq861bgvjrx4a.xn--fiqs8s:2,

user1/Maildir/new:

user1/Maildir/tmp:
```

The dovecot files are used by Dovecot to keep indexes of messages. Within the new and cur directories, each message is a file. The filenames start with a number which is the time the message arrived, as a Unix timestamp. The contents of each message file is just the message itself.

Managing user names and addresses

The information about the mailboxes are in two files. One file, `/etc/postfix/vmailbox`, is used by Postfix to say where to deliver mail sent to each address. Each line has the mailbox, a space, and the location of the Maildir relative to the mailuser home directory:

```
root@torn:~# cat /etc/postfix/vmailbox
bjørn@torn.xn--vuq861bgvjrx4a.xn--fiqs8s users/user1/Maildir/
postmaster@torn.xn--vuq861bgvjrx4a.xn--fiqs8s users/user1/Maildir/

bjørn@torn.信息测试.中国 users/user1/Maildir/
postmaster@torn.信息测试.中国 users/user1/Maildir/
```

Postfix does not automatically treat A-labels and U-labels as equivalent, so the file has an entry for both versions of the address. Internet mail requires that every mail domain have a *postmaster* address, so the setup script automatically makes postmaster deliver to the first user's mailbox.

The other file, `/etc/dovecot/users`, has the local username and password for each user, and the location of the directory Dovecot uses for the mailbox.

Each line of this file has colon separated fields with the local username, then the password, then three unused fields, and the directory. The passwords are stored as plain text which would be a poor choice for security purposes, but makes it easier to read and edit the file in this test system. (If you want to use encrypted passwords, see the references at the end of this document.)

```
root@torn:~# cat /etc/dovecot/users
user1:{PLAIN}sekret123::::/home/mailuser/users/user1
```

To add a new user, rerun the installation script with "addmbox" as an argument, and it will run the same script used to add users initially:

```
root@torn:~# sh eaiselfhost.sh addmbox
Installing on debian.
--- existing users ---
User   Password   Mail address
user1  sekret123  bjørn@torn.信息测试.中国

Do you want to add another user? (n) y
Enter mailbox name for user 2: rené
```

```
Password for user 2: reeney
Do you want to add another user? (n)
User   Password   Mail address
user1  sekret123  bjørn@torn.信息测试.中国
user2  reeney     rené@torn.信息测试.中国

Creating mailbox directories
Mailbox(es) added.
```

Now you can find the new user(s) in those files.

```
root@torn:~# cat /etc/postfix/vmailbox
bjørn@torn.xn--vuq861bgvjrx4a.xn--fiqs8s users/user1/Maildir/
postmaster@torn.xn--vuq861bgvjrx4a.xn--fiqs8s users/user1/Maildir/
rené@torn.xn--vuq861bgvjrx4a.xn--fiqs8s users/user2/Maildir/

bjørn@torn.信息测试.中国 users/user1/Maildir/
postmaster@torn.信息测试.中国 users/user1/Maildir/
rené@torn.信息测试.中国 users/user2/Maildir/

root@torn:~# cat /etc/dovecot/users
user1:{PLAIN}sekret123::::/home/mailuser/users/user1
user2:{PLAIN}reeney::::/home/mailuser/users/user2
```

To use the new user(s) in webmail, log in and configure the mail address(es) as described above.

To change a user's password, edit the password in the users file with any linux editor such as vi or ed, then type "dovecot reload" to reload the password table.

Mail system components

This package is constructed of the following major software packages. Debian has created installable packages for all of them which are also used by Ubuntu. Each package includes documentation files installed on the server. Most packages install manual pages you can read with the "man" command, such as "man postfix" or "man opendkim".

Postfix

Postfix is the mail server that handles inbound and outbound SMTP and mail submission. Its configuration files are in `/etc/postfix`.

General Postfix documentation is on the web at https://postfix.org., Debian package information is on the server in `/usr/share/doc/postfix`.

Opendkim

Opendkim creates and verifies DKIM signatures, and also has tools to create DKIM signing keys. It has one configuration file `/etc/default/opendkim`.

General (rather outdated) information is on the web at http://www.opendkim.org/. Debian package information is in `/usr/share/doc/opendkim` and `/usr/share/doc/opendkim-tools`.

Dovecot

Dovecot includes the POP and IMAP servers, and also handles login authentication for mail submission. Its configuration files are in /etc/dovecot.

General information is on the web at https://doc.dovecot.org/. Debian package information is in `/usr/share/doc/dovecot-core`, `/usr/share/doc/dovecot-imapd`, and `/usr/share/doc/dovecot-pop3d`.

SpamAssassin and Spamass-milter

Spamassassin is a spam filtering package that looks at messages as they arrive and assigns them a spam score. Spamassassin itself does the filtering, while spamass-milter is a “milter” (mail filter) that passes the messages from Postfix to SpamAssassin and back. Configuration files for spamassassin are in `/etc/spamassassin`. The configuration file for spamass-milter is `/etc/default/spamass-milter`.

General information about SpamAssassin is at https://spamassassin.apache.org/. Debian package info is in `/usr/share/doc/spamassassin`. General information about spamass-milter is at https://savannah.nongnu.org/projects/spamass-milt/. Debian package info is in `/usr/share/doc/spamass-milter`.

Apache and PHP

Apache is a widely used web server package. PHP is a scripting language primarily used to write applications that run in web servers.

General information about Apache is at https://httpd.apache.org/. Debian package info is in `/usr/share/doc/apache2` and `/usr/share/doc/apache2-utils`.

Roundcube and sqlite3

Roundcube is a webmail application written in PHP that runs on web servers including Apache. Its configuration files are in `/etc/roundcube`. User information is stored in a database managed by the Sqlite3 database package.

General information about Roundcube is at https://roundcube.net/. Debian package info is in `/usr/share/doc/roundcube` and `/usr/share/doc/roundcube-core`. General information on Sqlite is at https://www.sqlite.org/index.html, and Debian package info describing the way Roundcube uses Sqlite is in `/usr/share/doc/roundcube-sqlite3`.

Certbot

Certbot is a package sponsored by the Electronic Frontier Foundation that creates and installs free signed SSL certificates from the Let's Encrypt project. It gets a certificate for the Apache web server, which the install script then also configures into the Dovecot for IMAP and POP and Postfix for SMTP STARTTLS and submission. Certificates expire after 90 days so Certbot schedules a periodic re-signing to keep the certificate valid. Its configuration files are in `/etc/letsencrypt`, with the current SSL key in `/etc/letsencrypt/live`.

General information is at https://certbot.eff.org/. Debian package info is in /usr/share/doc/certbot, `/usr/share/doc/python3-certbot`, and `/usr/share/doc/python3-certbot-apache`.

Further reading

Here are some online resources that may be helpful when setting up and managing the mail server.

Using SSH

https://linuxhandbook.com/ssh-basics/ (Using ssh on Linux)

https://www.ssh.com/academy/ssh (General information about ssh)

https://learn.microsoft.com/en-us/windows/terminal/tutorials/ssh (Windows 10 and 11 ssh)

https://www.putty.org/ (PuTTY, a popular Windows ssh client)

Using Linux commands

https://ubuntu.com/tutorials/command-line-for-beginners#1-overview (Linux shell tutorial)

Managing Dovecot

https://doc.dovecot.org/2.3/configuration_manual/authentication/passwd_file/ (How to manage the password file)

https://doc.dovecot.org/2.3/configuration_manual/authentication/password_schemes/#authentication-password-schemes (How to use encrypted rather than plain text passwords)