

# Postfix. Dovecot. Danger.

you have a mailbox in your yard, why not a mail server in your closet?

- [Postfix MTA, with Dovecot for clients.](#)

# Postfix MTA, with Dovecot for clients.

One of the great dreams of the early internet, once it began to creep into regular peoples homes, was that everyone could stand up their own server and host whatever services they wanted.

Website? sure. Fileshare? yep. Email? absofuckinlutely.

Now, it was never expected to be easy. But neither was it expected that a handful of corporations would make popular services easy to use, put a moat around them once we were all inside, and turn the internet into an eyeball attracting advertising consumption machine.

But people might be slowly waking up from this sleep and remembering the bright future we almost had. Activitypub and the "Fediverse" remind people that you can do anything you want- its your internet- and you just dont have to pimp yourself and your eyeballs.

Postfix is a great way to explore some diy internetting. With your own mailserver and a domain registration, you can communicate with your friends, family, and the world without google snooping through your junk. at least half your junk, anyway. Postfix is old software and has been the backbone of many orgs mail systems for years. While its great for gigantic multiuser and multidomain systems, its fine for a single user vps, too.

I run Postfix 3.4.13 on a Ubuntu focal (20.04) vps. It has two single core sockets and 8gb ram. it has no trouble at all with email, a little website, and the occasional lab project. One advantage of using a vps is you usually get a static ip address. and they are dirt cheap.

First, youll want to install postfix with the usual apt method. you can get fancy and build from source, or compile with special features, but i found the the repo version to be just fine. Postfix has great documentation and the config file are pretty detailed so it seem like a waste to give a step by step. RTFM and stuff. you should pretty quickly be able to send and receive email from your server. *BEWARE:* Google and others will trash you outbound messages pretty much immediately if you dont configure SPF records and DMARC for your site. these are good things to do and you should do them anyway. Make sure you have a reverse dns record for your server in DNS, too.

with a working postfix you can receive email and the server will put it into your Maildir and tell you about it when you log in. postfix in the simplest configuration relies on pam and local users. if you hate yourself, you can use a database to have a lot of mail users that arents also local users. if you hate yourself. (hint: if you make a /etc/postfix/aliases file, you can have a million addresses at your domain and get them all in one /Maildir)

<http://www.postfix.org/documentation.html>

A terrific mail client for interacting with postfix is s-nail. its a hard to use as vim. nerds like it.

<https://wiki.archlinux.org/title/S-nail> . Maybe thats enough for you. i used s-nail for a long time with joy. But truth is, if you really want to dig out of hotmails clutches, you need to be able to use your homebrew email server with mobile. mfa, password resets, rickrolling and memes require something more.

you could install squirrelmail or some other websitey front end- but that again seems like self-hate. Dovecot has what you need. good old imap. Getting dovecot to play with postfix is pretty easy. in the dovecot conf.d/10-master.conf, enable the auth service:

```
service auth {
...
unix_listener /var/spool/postfix/private/auth {
mode = 0660
# Assuming the default Postfix user and group
user = postfix
group = postfix
}
...
}# Outlook and Windows Mail works only with LOGIN mechanism, not the
standard PLAIN:
auth_mechanisms = plain login
```

Example Postfix main.cf excerpt

```
smtpd_sasl_type = dovecot

# Can be an absolute path, or relative to $queue_directory
# Debian/Ubuntu users: Postfix is setup by default to run chrooted, so it is best to leave it as
smtpd_sasl_path = private/auth

# On Debian Wheezy path must be relative and queue_directory defined
#queue_directory = /var/spool/postfix

# and the common settings to enable SASL:
smtpd_sasl_auth_enable = yes
# With Postfix version before 2.10, use smtpd_recipient_restrictions
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
```

Using SASL with Postfix submission port

When Dovecot is used as the authentication backend for Postfix it is good practice to use a dedicated submission port for the MUAs (TCP 587). Not only can you specify individual parameters in **master.cf** overriding the global ones but you will not run into internet mail rejection while the Dovecot Auth Mechanism is unavailable. In this example Postfix is configured to accept TLS encrypted sessions only, along with several other sanity checks:

- Verification of alias ownership via Login Maps
- Domainname and recipient plausibility

master.cf

```
submission inet n - n - - smtpd
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_sasl_security_options=noanonymous
  -o smtpd_sasl_local_domain=$myhostname
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o smtpd_sender_login_maps=hash:/etc/postfix/virtual
  -o smtpd_sender_restrictions=reject_sender_login_mismatch
  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_do
```

[https://doc.dovecot.org/configuration\\_manual/howto/postfix\\_and\\_dovecot\\_sasl/](https://doc.dovecot.org/configuration_manual/howto/postfix_and_dovecot_sasl/)

you're also going to want to enable encryption in postfix using real certs. Your client will complain when you try to send via smtp. I just used some letsencrypt certs for my domain.

---

The following settings enable encryption, set the key and certificate paths for Postfix. Just run these commands:

```
postconf smtpd_tls_security_level=may
postconf smtpd_tls_auth_only=yes
postconf smtpd_tls_cert_file=/etc/letsencrypt/live/webmail.example.org/fullchain.pem
postconf smtpd_tls_key_file=/etc/letsencrypt/live/webmail.example.org/privkey.pem
postconf smtpd_tls_security_level=may
```

you might need to adjust your firewall to allow inbound imap and smtp. UFW makes it so easy:

```
sudo ufw app list
```

to see what apps are configured.  
add a new one with:

```
sudo ufw add "dovecot"
```

it's that easy

<https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands>