Configure Postfix

> ❝ Postfix is a Mail Transfer Agent (MTA) that can act as an SMTP server or client to send or receive email. There are many reasons why you would want to configure Postfix to send email using Google Apps and Gmail. One reason is to avoid getting your mail flagged as spam if your current server's IP has been added to a blacklist.
>
> [Linode Postfix Tutorial](#)

Install postfix and mailutils -

```
sudo apt install postfix mailutils
```

Create Google App Token

When attempting to send mail from a new host, you may encounter errors with Google blocking or filtering your mail as spam. To prevent this, simply create a GMail account you wish to send the mail under, [Activate 2FA](#) on the new account, then [Generate App Tokens](#) to distribute to the hosts / apps you wish to send mail on your behalf. See below for further instructions once you have a GMail account created, and have generated an app password / token.

Postfix App Token Authentication

Once you have the app token, we'll need to add it to `/etc/postfix/sasl/sasl_passwd` - If this file doesn't already exist, create it and include the following lines, modified with your information

```
sudo echo "[smtp.gmail.com]:587 username@gmail.com:password" > /etc/postfix/sasl/sasl_passwd;
```

Instead of using the password you usually input when logging into the GMail account, add the app token generated after enabling 2FA following the links in the first step above. Below, we notify postfix that we've made these changes by running `sudo postmap /etc/postfix/sasl/sasl_passwd`. This will create a sasl_passwd.db file in the `/etc/postfix/sasl` directory.

Run postmap, and restrict access to our new file containing this password

```
sudo postmap /etc/postfix/sasl/sasl_passwd;
sudo chown root:root /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db;
```

```
sudo chmod 600 /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db;
```

Configure Relay Server

Configure postfix to relay mail through GMail's server by making the below changes to `/etc/postfix/main.cf` -

```
# Change / modify this line..
relayhost = [smtp.gmail.com]:587


# Add these lines...
# Enable SASL authentication
smtp_sasl_auth_enable = yes
# Disallow methods that allow anonymous authentication
smtp_sasl_security_options = noanonymous
# Location of sasl_passwd
smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
# Enable STARTTLS encryption
smtp_tls_security_level = encrypt
# Location of CA certificates
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Send Mail

That's it! Now restart postfix with `sudo systemctl restart postfix` and test sending mail using any of the commands below -

```
echo "This email confirms that Postfix is working" | mail -s "Testing Posfix" emailuser@example.com
```

or..

```
sendmail emailaddress@gmail.com
FROM: admin@sub.domain.com
SUBJECT: Hi
Body test text

.
```

Mailer Daemon

To change the email the system sends security alerts to, modify the `/etc/aliases` file to use your email address for the `root` field below. If this isn't already in the file, add it, and run `sudo newaliases` to update the system with the new information.

```
# See man 5 aliases for format
postmaster:    root
root: someone@somedomain.com
```

Now to test that his works correctly, attempt to sudo somewhere on the system where you'll be required to enter a password, and botch it - all three times. You'll get an email from your server warning you of the security event! Missing a password on an attempt to sudo is a security event

Revision #5
Created 31 August 2019 14:14:04 by Shaun Reed
Updated 18 December 2021 15:20:07 by Shaun Reed