

## 1. Install Postfix

- Update package lists:

Bash

```
sudo apt update
```

- Install Postfix:

Bash

```
sudo apt install postfix
```

- During Postfix installation:
  - Choose "Internet Site" as the configuration type.
  - Enter your domain name (e.g., `example.com` ) or use a placeholder.
  - Enter your system's fully qualified domain name (FQDN) if available.

## 2. Configure Postfix

- Edit the main Postfix configuration file:

Bash

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

- Modify the following lines (if necessary):
  - `myhostname = your_hostname.domain.name` : Replace with the FQDN of your server.
  - `mydomain = domain.name` : Replace with your domain name.
  - `relayhost = [mail.yourprovider.com]:587` : If you're using a relay server (optional).
  - `smtp_use_tls = yes` : Enable TLS encryption.
  - `smtp_tls_security_level = encrypt` : Require encryption.
  - `smtp_sasl_auth_enable = yes` : Enable authentication.
  - `smtp_sasl_password_maps = hash:/etc/postfix/sasl/smtpd_passwd` : Specify the password file.
- Create the password file:

Bash

```
sudo postmap hash:/etc/postfix/sasl/smtpd_passwd < <(echo "your_username:your_password")
```

- Replace `your_username` and `your_password` with the credentials for your email provider.
- Restrict access (optional):
  - If you only want to allow local users to send mail, uncomment and modify:

```
mynetworks = 127.0.0.0/8
```

- Save and close the `main.cf` file.

### 3. Restart Postfix

- Restart the Postfix service:

Bash

```
sudo systemctl restart postfix
```

### 4. Test the SMTP Server

- Use a command-line tool like `mail` or `sendmail` to send a test email:

Bash

```
echo "Test email body" | mail -s "Test Subject" recipient@example.com
```

### 5. Configure your email client

- Configure your email client (e.g., Thunderbird, Outlook) to use your server as the outgoing mail server (SMTP).
  - Server Address: Your server's IP address or hostname.
  - Port: 587 (or 25 if TLS is not enabled)
  - Authentication: Enable authentication and enter your username and password.
  - Encryption: Enable TLS/SSL encryption.

#### Important Notes:

- Security:
  - Use strong passwords.
  - Consider using TLS encryption for all email communication.
  - Regularly update Postfix to the latest version for security patches.
  - If you're using a relay server, ensure you have the necessary permissions.
- Firewall:
  - Make sure your firewall allows the necessary ports for SMTP communication (typically 25, 465, 587).
- This is a basic setup. You can further customize Postfix by configuring advanced options like:

- Virtual users: Create multiple users with separate mailboxes.
- Spam filtering: Integrate with spam filtering tools.
- Logging and monitoring.