

How to Quickly Set up a Mail Server on Ubuntu 18.04 with Modoboa

This tutorial is going to show you how to quickly set up your own email server on Ubuntu 18.04 with [Modoboa](#), which is a free and open source mail hosting and management platform designed to work with Postfix SMTP server and Dovecot IMAP/POP3 server.

Modoboa is written in Python, released under the terms of ISC license. The latest version is v1.12.2, released on October 19, 2018. Main features of Modoboa are as follows:

- Modoboa by default uses **Nginx** web server to serve the webmail client and web-based admin panel.
- Compatible with Postfix and Dovecot.
- Support MySQL/MariaDB, or PostgreSQL database.
- Easily create **unlimited mailboxes** and **unlimited mail domains** in a web-based admin panel.
- Easily create email alias in the web-based admin panel.
- The webmail client provides an easy-to-use message filter to help you organize messages to different folders.
- It can help you protect your domain reputation by monitoring email blacklists and generating DMARC report, so your emails have better chance to land in inbox instead of spam folder.
- Includes amavis frontend to block spam and detect virus in email.
- Calendar and address book.
- Integration with Let's Encrypt.
- Includes AutoMX to allow end users to easily configure mail account in a desktop or mobile mail client.

Step 1: Choose the Right Hosting Provider and Buy a Domain Name

To set up a complete email server with Modoboa, you need a server with at least 2GB RAM, because after the installation, your server will use more than 1GB of RAM. This tutorial is done on a [\\$10/month Vultr VPS \(virtual private server\)](#). I recommend Vultr because it allows you to send emails via port 25, so you can send unlimited emails (transactional email and newsletters) without spending money on SMTP relay.

Step 2: Creating DNS MX Record

The MX record specifies which host or hosts handle emails for a particular domain name. For example, the host that handles emails for `linuxbabe.com` is `mail.linuxbabe.com`. If someone with a Gmail account sends an email to `somebody@linuxbabe.com`, then Gmail server will query the MX record of `linuxbabe.com`. When it finds out that `mail.linuxbabe.com` is responsible for accepting email, it then query the A record of `mail.linuxbabe.com` to get the IP address, thus the email can be delivered.

In your DNS manager, create a MX record for your domain name. Enter `@` in the Name field to represent the main domain name, then enter `mail.your-domain.com` in the Value field.

Edit DNS Record

DNS Record Type	MX - Mail exchange ▼
Name	@
Value	mail.linuxbabe.com
Time to Live (TTL)	90 seconds ▼

CloseSave Changes

Note: The hostname for MX record can not be an alias to another name. Also, It's highly recommended that you use hostnames, rather than bare IP addresses for MX record.

Your DNS manager may require you to enter a preference value (aka priority value). It can be any number between 0 and 65,356. A small number has higher priority than a big number. You can enter 0 for your email server, or accept the default value.

After creating MX record, you also need to create an A record for `mail.your-domain.com`, so that it can be resolved to an IP address. If your server uses IPv6 address, be sure to add AAAA record.

If you uses Cloudflare DNS service, you should not enable the CDN feature when creating A record for your mail server.

Step 3: Set up Mail Server on Ubuntu 18.04 with Modoboa Installer

Log into your server via [SSH](#), then run the following commands to update software packages.

```
sudo apt update
```

```
sudo apt upgrade
```

Download modoboa installer from Github.

```
git clone https://github.com/modoboa/modoboa-installer
```

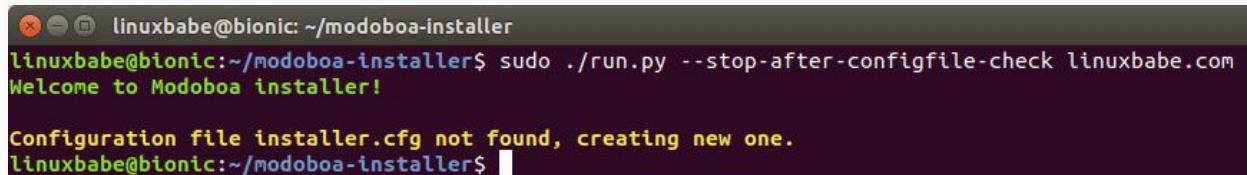
Modoboa is written in Python. Run the following command to install the necessary Python software.

```
sudo apt-get install python-virtualenv python-pip
```

Then navigate to the `modoboa-installer` directory and create a configuration file. Replace `example.com` with your own domain name.

```
cd modoboa-installer
```

```
sudo ./run.py --stop-after-configfile-check example.com
```

A terminal window screenshot showing the execution of the modoboa-installer script. The prompt is 'linuxbabe@bionic: ~/modoboa-installer'. The command entered is 'sudo ./run.py --stop-after-configfile-check linuxbabe.com'. The output shows 'Welcome to Modoboa installer!' followed by 'Configuration file installer.cfg not found, creating new one.' and the prompt returns to 'linuxbabe@bionic:~/modoboa-installer\$'.

```
linuxbabe@bionic: ~/modoboa-installer
linuxbabe@bionic:~/modoboa-installer$ sudo ./run.py --stop-after-configfile-check linuxbabe.com
Welcome to Modoboa installer!

Configuration file installer.cfg not found, creating new one.
linuxbabe@bionic:~/modoboa-installer$
```

Edit the configuration file `installer.cfg` with a command line text editor like nano.

```
sudo nano installer.cfg
```

To obtain a valid TLS certificate from Let's Encrypt for your mail server, in `[certificate]` section, change the value of type from `self-signed` to `letsencrypt`.

```
type = letsencrypt
```

And change the email address from `admin@example.com` to your real email address, which will be used for account recovery and important notifications.

```
[certificate]
generate = true
type = letsencrypt

[letsencrypt]
email = xiao@linuxbabe.com
```

By default, Modoboa installer will install PostgreSQL database server, as indicated by the following lines in the config file.

```
[database]
engine = postgres
host = 127.0.0.1
install = true
```

If you would like to use MariaDB database server, then change the engine from `postgres` to `mysql`. (Modoboa will install MariaDB instead of MySQL.)

```
[database]
engine = mysql
host = 127.0.0.1
install = true
```

Save and close the file. (To save a file in Nano text editor, press `Ctrl+O`, then press `Enter` to confirm. To exit, press `Ctrl+X`.)

Now run the following command to start the installation.

```
sudo ./run.py --interactive example.com
```

```
linuxbabe@bionic:~/modoboa-installer$ sudo ./run.py --interactive linuxbabe.com
Welcome to Modoboa installer!

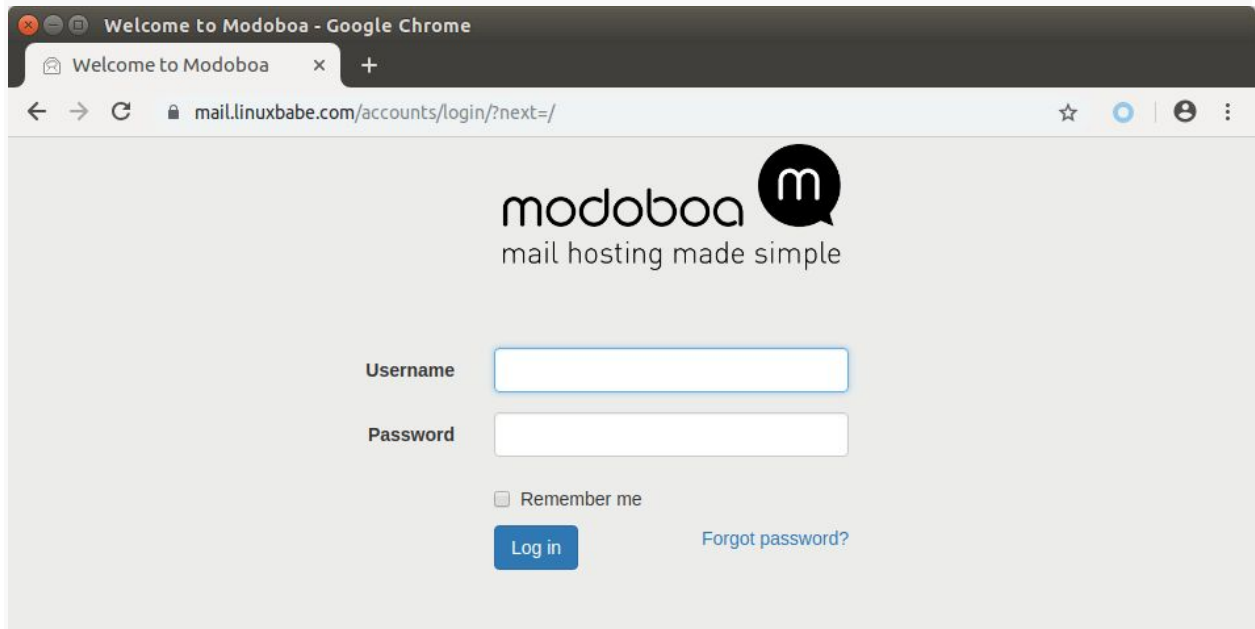
Warning:
Before you start the installation, please make sure the following DNS records exist for domain 'linuxbabe.com':
  mail IN A   <IP ADDRESS OF YOUR SERVER>
        IN MX mail.linuxbabe.com.

Your mail server will be installed with the following components:
modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n) y
The process can be long, feel free to take a coffee and come back later ;)
Starting...
Generating new certificate using letsencrypt
Installing amavis
Installing spamassassin
Installing razor
Installing clamav
Installing modoboa
Installing automx
Installing radicale
Installing uwsgi
Installing nginx
Installing opendkim
Installing postfix
Installing postwhite
Installing dovecot
Congratulations! You can enjoy Modoboa at https://mail.linuxbabe.com (admin:password)
```

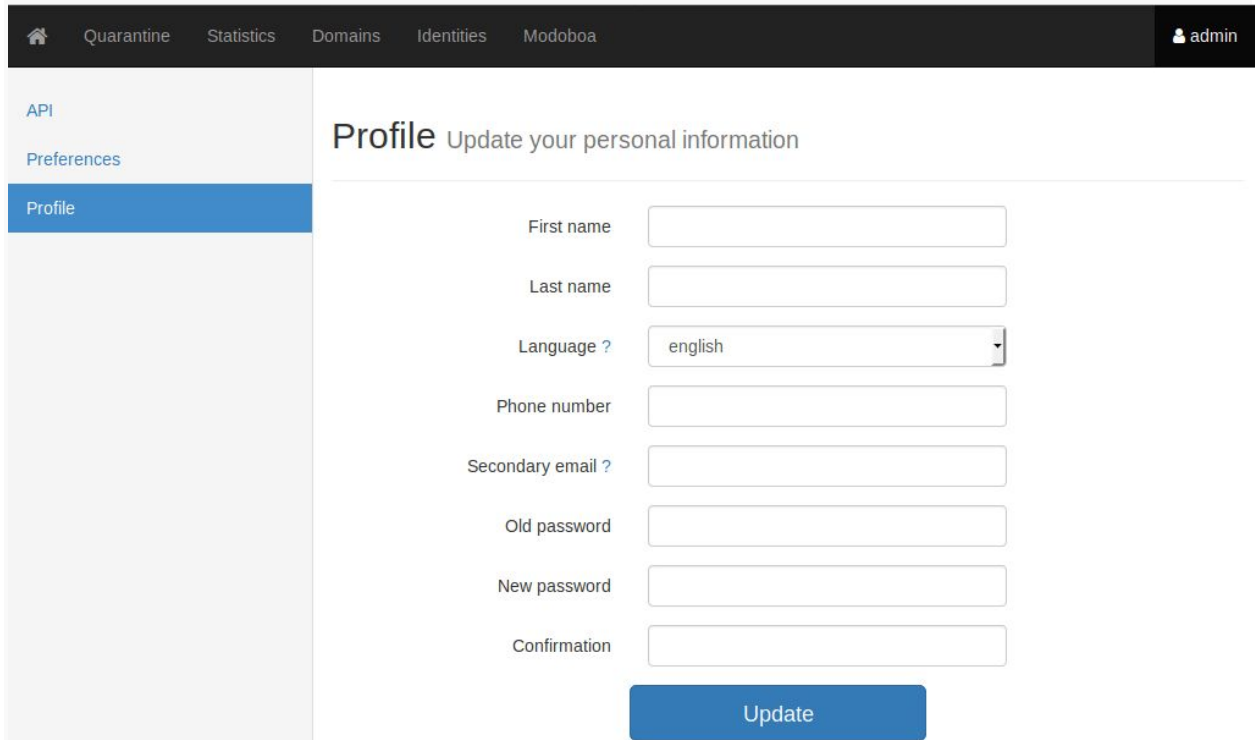
The installation process can take a while. It took 10 minutes on my Vultr server. If you see an error during the installation, you can use the `--debug` option to see more detailed output.

```
sudo ./run.py --interactive --debug example.com
```

After Modoboa finishes installation, you can log into the admin panel with username `admin` and password `password`.



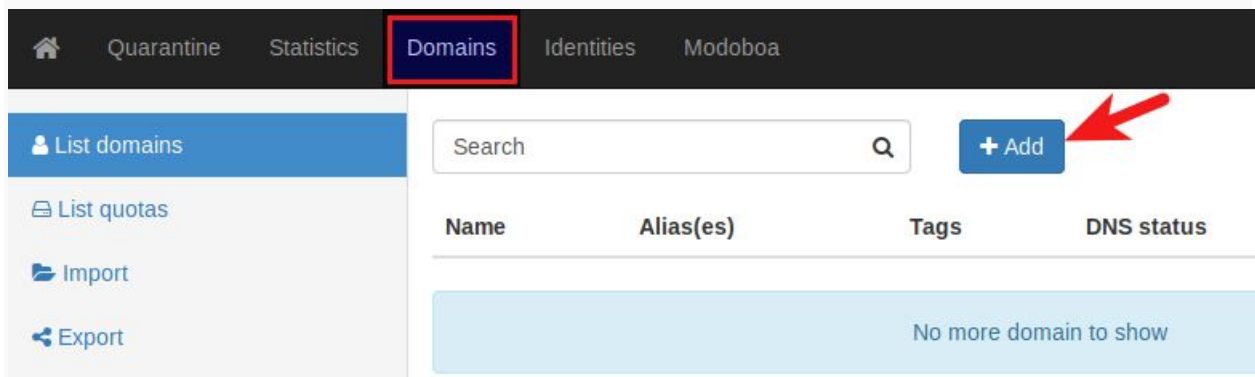
Once you are logged in, you should go to `Admin` -> `Settings` -> `Profile` to change the password.



The screenshot shows the 'Profile' page in the Modoboa Admin Panel. The top navigation bar includes 'Quarantine', 'Statistics', 'Domains', 'Identities', and 'Modoboa'. The left sidebar has 'API', 'Preferences', and 'Profile' (selected). The main content area is titled 'Profile Update your personal information' and contains several form fields: 'First name', 'Last name', 'Language ?' (set to 'english'), 'Phone number', 'Secondary email ?', 'Old password', 'New password', and 'Confirmation'. A blue 'Update' button is at the bottom right.

Step 4: Adding Mailboxes in Modoboa Admin Panel

Go to **Domains** tab and click **Add** button to add a new domain.



The screenshot shows the 'Domains' page in the Modoboa Admin Panel. The top navigation bar has 'Domains' highlighted with a red box. The left sidebar has 'List domains' (selected), 'List quotas', 'Import', and 'Export'. The main content area has a search bar and a blue '+ Add' button with a red arrow pointing to it. Below the button is a table with columns 'Name', 'Alias(es)', 'Tags', and 'DNS status'. The table is currently empty, showing 'No more domain to show'.

Then enter your main domain name in the Name field. It is highly recommended that you enable DKIM signing, which can help with your domain reputation. In **Key**

selector filed, you can enter a random word like modoboa. Choose 2048 as the key length.

New domain / General

Name ?

linuxbabe.com

Type

Domain

Quota ?

0

Default mailbox quota ?

0

Alias(es) ?

Enabled ?

☒

Enable DNS checks ?

☒

Enable DKIM signing ?

☒

Key selector

modoboa

Key length

2048

Close

Next

In the next screen, you can choose to create an admin account for your domain. The SMTP protocol requires that a mail server should have a `postmaster@example.com` address.

New domain / Options

Create a domain administrator ?☒ Yes ☐ No

Name ?

postmaster@linuxbabe.com

Random password ?☒ Yes ☐ No

With a mailbox ?☒ Yes ☐ No

Create aliases ?☒ Yes ☐ No

Close

Previous

Submit

Click the Submit button and your domain name will be added in Modoboa.

To add email addresses, go to **Domains** tab and click your domain name.

Home

Quarantine

Statistics

Domains

Identities

Modoboa

admin

List domains

List quotas

Import

Export

Search

+ Add

Name	Alias(es)	Tags	DNS status	Actions
linuxbabe.com	---	Domain	MX DNSBL	<div></div>

Then click mailboxes.

linuxbabe.com

Summary

Creation date	Oct. 24, 2018, 6:37 a.m.
Last modification date	Oct. 24, 2018, 6:37 a.m.
Domain aliases	0
Mailboxes	0
Mailbox aliases	0
Quota	0 MB
Default mailbox quota	0 MB

DNS

Status	MX DNSBL
DKIM key	Show key

Administrators

Username	Name
No domain administrator defined yet.	

Click **Add** button and choose **Account**.

Add

Account

Alias

Name	Fullname/Recipient	Tags	Actions
------	--------------------	------	---------

Then choose **Simple user** as the role. Enter an email address in Username field and enter a password.

New account / General



Role ?

Simple user

Username ?

user1@linuxbabe.com

First name

Xiao

Last name

Guoan

Random password ?

☐

Password

.....

Confirmation ?

.....

Enabled



Close

Next

In the next screen, you can optionally create an alias for this email address.

New account / Mail

E-mail

user1@linuxbabe.com

Quota ?

☒ Use domain default value

Alias(es) ?

Sender addresses ?

Close

Previous

Submit

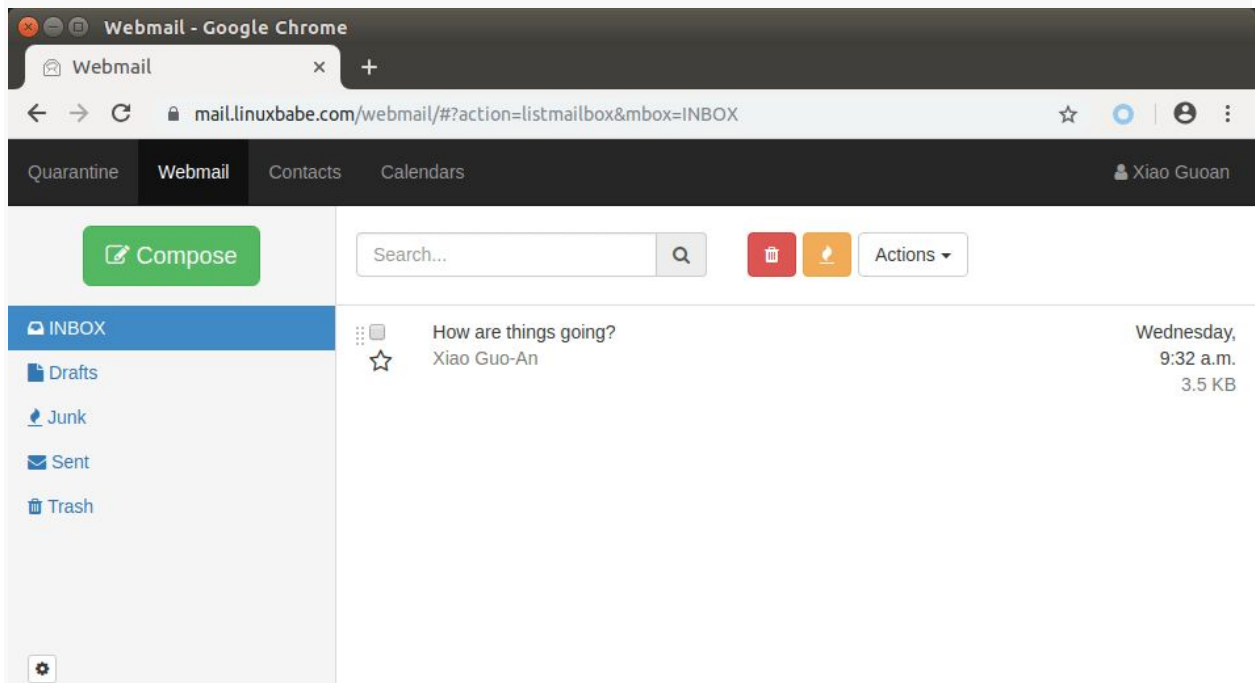
After clicking the submit button, the email address is created.

Step 5: Sending Test Emails

To login to the webmail, you need to log out the admin account first and then enter the user credentials.



Once you are logged into Modoboa webmail, you can send a test email from your private email server to your other email address and vice versa.



Inbound emails will be delayed for a few minutes, because by default Modoboa enables greylisting, which tells other sending SMTP server to try again in a few minutes. This is

useful to block spam. The following message in `/var/log/mail.log` indicates greylisting is enabled.

```
postfix/postscreen[20995]: NOQUEUE: reject: RCPT from  
[34.209.113.130]:36980: 450 4.3.2 Service currently unavailable;
```

Step 6: Unblocking Port 25 for Your Vultr Server

Your ISP or hosting provider won't block incoming connection to port 25 of your server, which means you can receive emails from other mail servers. However, many ISP/hosting providers block outgoing connection to port 25 of other mail servers, which means you can't send emails.

If your email didn't arrive at your other email address such as Gmail, then run the following command on your mail server to check if port 25 is blocked.

```
telnet gmail-smtp-in.l.google.com 25
```

If it's not blocked, you would see messages like below, which indicates a connection is successfully established. (Hint: Type in `quit` and press Enter to close the connection.)

```
Trying 74.125.68.26...  
Connected to gmail-smtp-in.l.google.com.  
Escape character is '^]'.  
220 mx.google.com ESMTP y22si1641751p1l.208 - gsmtip
```

If port 25 is blocked, you would see something like:

```
Trying 2607:f8b0:400e:c06::1a...  
Trying 74.125.195.27...  
telnet: Unable to connect to remote host: Connection timed out
```

If port 25 is blocked for outgoing connections on your Vultr server, then you should open a support ticket in your Vultr account. They will unblock port 25 for you. Here's what I said to the support stuff.

Hi

I'm setting up a mail server. Looks like port 25 is blocked on this server. Please open it for me.

Thanks :)

The support stuff replied very quickly:

Hello XIAO GUOAN,

Thank you for your SMTP unblock request!

In order to combat spam and spam-like activities, we will need to review some additional information prior to removing the SMTP filter.

Please reply to this ticket with the following information:

1. The business name and organization URL(s) under which you offer services.
2. Describe, in as much detail as possible, the nature of the emails you intend to send.
3. The volume of email that you plan to deliver on a daily/monthly basis.

We need to know this in order to make an informed decision regarding your account settings and resource limits to ensure the integrity of our network/systems/online reputation.

Customer Support
www.Vultr.com

So you just need to answer 3 simple questions. You can use the following as a template. Note that if you are going to send newsletters, you need to tell that you will send newsletter and how your email list addresses are collected.

Hi

My business name is LinuxBabe and website is <https://www.linuxbabe.com>,

I'm setting up this mail server for my website, so I would be able to send registration emails and notification emails to my users.

The volume of outgoing email is below 100 emails per day.

Thanks.

And then the stuff replied:

Hello,

Thank you for the information provided!

We have removed the default SMTP block on your account. Please restart any active instances via <https://my.Vultr.com> for the change to take effect (restarting via the server itself `_will_not_` work).

Also, keep in mind that marketing and bulk email is restricted in our platform. For reference, our ANTI-SPAM policy is listed here: https://www.Vultr.com/legal/antispam_policy.php

If you have any additional questions our team is happy to assist you further. Thank you for choosing Vultr!

Kind Regards,
Customer Support

Once they removed the SMTP block on your account, you need to restart your server via the Vultr control panel for the change to take effect. Note that [you can use Vultr server so send newsletters](#), as long as the recipients subscribed for it, but you are not allowed to send spam.

If your ISP or hosting provider (such as [DigitalOcean](#)) refuses to unblock port 25, then you can't send emails directly, you also need to [set up SMTP relay](#) to solve this problem.

Step 7: Using Mail Clients on Your Computer or Mobile Device

Fire up your desktop email client such as Mozilla Thunderbird and add a mail account.

- In the incoming server section, select IMAP protocol, enter `mail.your-domain.com` as the server name, choose port 993 and SSL/TLS. Choose `normal password` as the authentication method.
- In the outgoing section, select SMTP protocol, enter `mail.your-domain.com` as the server name, choose port 587 and STARTTLS. Choose `normal password` as the authentication method.

Set Up an Existing Email Account

Your name: Your name, as shown to others

Email address: Your existing email address

Password: ☒ Remember password

	Server hostname	Port	SSL	Authentication
Incoming: <input type="button" value="IMAP"/>	<input type="text" value="mail.linuxbabe.com"/>	<input type="text" value="993"/>	<input type="button" value="SSL/TLS"/>	<input type="button" value="Normal password"/>
Outgoing: <input type="button" value="SMTP"/>	<input type="text" value="mail.linuxbabe.com"/>	<input type="text" value="587"/>	<input type="button" value="STARTTLS"/>	<input type="button" value="Normal password"/>
Username: Incoming:	<input type="text" value="user1"/>	Outgoing:	<input type="text" value="user1"/>	

You can also use IMAP on port 143 with STARTTLS encryption.

Step 8: Improving Email Deliverability

To prevent your emails from being flagged as spam, you should set PTR, SPF, DKIM and DMARC records.

PTR record

A pointer record, or PTR record, maps an IP address to a FQDN (fully qualified domain name). It's the counterpart to the A record and is used for reverse DNS lookup, which can help with blocking spammers. Many SMTP servers reject emails if no PTR record is found for the sending server.

To check the PTR record for an IP address, run this command:

```
dig -x IP-address +short
```

or

host **IP-address**

Because you get IP address from your hosting provider or ISP, not from your domain registrar, so you must set PTR record for your IP in the control panel of your hosting provider or ask your ISP. Its value should be your mail server's hostname:

`mail.your-domain.com`. If your server uses IPv6 address, be sure to add a PTR record for your IPv6 address as well.

To edit the reverse DNS record for your [Vultr server](#), log into Vultr control panel, select your server and the **Settings** tab. Then you can edit the reverse DNS record for both IPv4 and IPv6 address.

Usage Graphs	Settings	Snapshots	Backups	DDOS
Public Network				
Need assistance? View our networking configuration tips and examples.				
Address	Netmask	Gateway	Reverse DNS	
108.160.131.149 Main IP	255.255.254.0	108.160.130.1	mail.linuxbabe.com	

SPF Record

SPF (Sender Policy Framework) record specifies which hosts or IP address are allowed to send emails on behalf of a domain. You should allow only your own email server or

your ISP's server to send emails for your domain. In your DNS management interface, create a new TXT record like below.

Edit DNS Record

DNS Record Type	<div>TXT - Text</div>
Name	<div>@</div>
Value	<div>v=spf1 mx ~all</div>
Time to Live (TTL)	<div>90 seconds</div>

Close

Save Changes

Explanation:

- **TXT** indicates this is a TXT record.
- Enter **@** in the name field to represent the main domain name.
- **v=spf1** indicates this is a SPF record and the version is SPF1.
- **mx** means all hosts listed in the MX records are allowed to send emails for your domain and all other hosts are disallowed.
- **~all** indicates that emails from your domain should only come from hosts specified in the SPF record. Emails that are from other hosts will be flagged as forged.

To check if your SPF record is propagated to the public Internet, you can use the dig utility on your Linux machine like below:

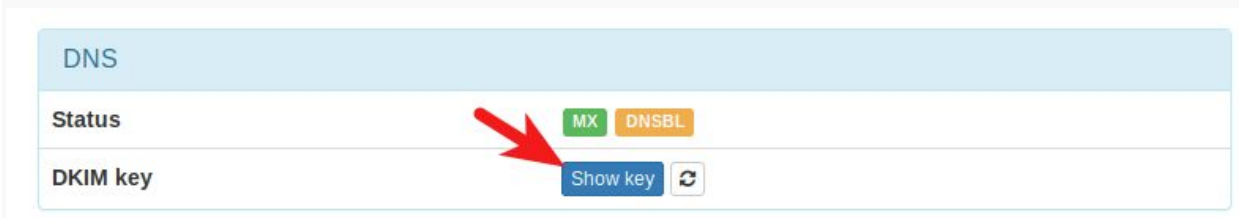
```
dig your-domain.com txt
```

The `txt` option tells `dig` that we only want to query TXT records.

DKIM Record

DKIM (DomainKeys Identified Mail) uses a private key to digitally sign emails sent from your domain. Receiving SMTP servers verify the signature by using the public key, which is published in the DNS DKIM record.

When we were adding domain name in Moboboa admin panel earlier, we enabled DKIM signing, so the signing part is taken care of. The only thing left to do is creating DKIM record in DNS manager. First go to Modoboa admin panel and select your domain name. In the DNS section, click `Show key` button.



The public key will be revealed. There are two formats. We only need the Bind/named format.

DKIM public key for linuxbabe.com

Raw format

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwm4rdttj9tvhb9r6jLAacHnOGQAqXaJOIdFm3yWe/em41MgWsinVIC74acaQ8saD7kT7rjz/5rfO9lhQTgW04BRRMjlcNyYAY2YWFsWy1hv7oJcbHPHgA/epCPw15FTFA0lLk+hGXc723F5xfFlueScwLr+vtyhr6XNxWHLd2FIWheaqEibN1wk+lubJaqRW+zjEvqfq32fSNwkW9aNH19MsHJpjFLAPb3vnMLmA81bwOpUUagHZchSHRUf7fW3rgWiSq17mEjeX2tWJeAP6cngEKB9juGSQuAtjGGsLA5OhzbKY+dwODzdioKABXBv3MDzJ86ECp2UC5KKk29G0NwIDAQAB
```

Bind/named format

```
modoboa._domainkey.linuxbabe.com. 10800 IN TXT (  
"v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwm4rdttj9tvhb9"  
"r6jLAacHnOGQAqXaJOIdFm3yWe/em41MgWsinVIC74acaQ8saD7kT7rjz/5rfO9lhQTgW04BRR"  
"MjlcNyYAY2YWFsWy1hv7oJcbHPHgA/epCPw15FTFA0lLk+hGXc723F5xfFlueScwLr+vtyhr6X"  
"NxWHLd2FIWheaqEibN1wk+lubJaqRW+zjEvqfq32fSNwkW9aNH19MsHJpjFLAPb3vnMLmA81bw"  
"OpUUagHZchSHRUf7fW3rgWiSq17mEjeX2tWJeAP6cngEKB9juGSQuAtjGGsLA5OhzbKY+dwODz"  
"dioKABXBv3MDzJ86ECp2UC5KKk29G0NwIDAQAB")
```

Go to your DNS manager, create a TXT record, enter `modoboa._domainkey` in the Name field. (Recall that we used modoboa as the selector when adding domain name in the admin panel.) Copy everything in the parentheses and paste into the value field. Delete all double quotes. Your DNS manager may require you to delete other invalid characters, such as carriage return.

Edit DNS Record

DNS Record Type

TXT - Text

Name

modoboa._domainkey

Value

v=DKIM1;k=rsa;p=MIIBIJANBgkqhkiG9w0BAQEFAAO

Time to Live (TTL)

90 seconds

Close

Save Changes

For those who are interested, Modoboa uses OpenDKIM to generate private key for your domainkey and verify signatures of inbound emails.

DMARC Record

DMARC stands for Domain-based Message Authentication, Reporting and Conformance. DMARC can help receiving email servers to identify legitimate emails and prevent your domain name from being used by email spoofing.

To create a DMARC record, go to your DNS manager and add a **TXT** record. In the name field, enter `_dmarc`. In the value field, enter the following:

```
v=DMARC1; p=none; pct=100;  
rua=mailto:dmarc-reports@your-domain.com
```


Edit DNS Record

DNS Record Type	<div>TXT - Text</div>
Name	<div>_dmarc</div>
Value	<div>v=DMARC1; p=none; pct=100; rua=mailto: dmarc@li</div>
Time to Live (TTL)	<div>5 mins</div>

Close

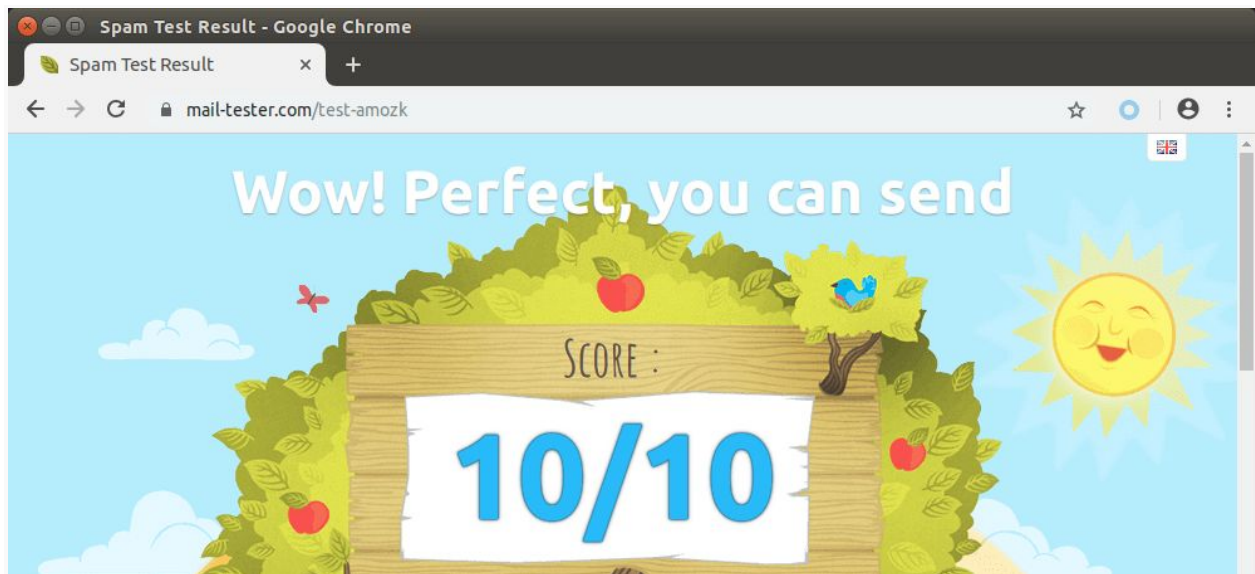
Save Changes

The above DMARC record is a safe starting point. To see the full explanation of DMARC, please check the following article.

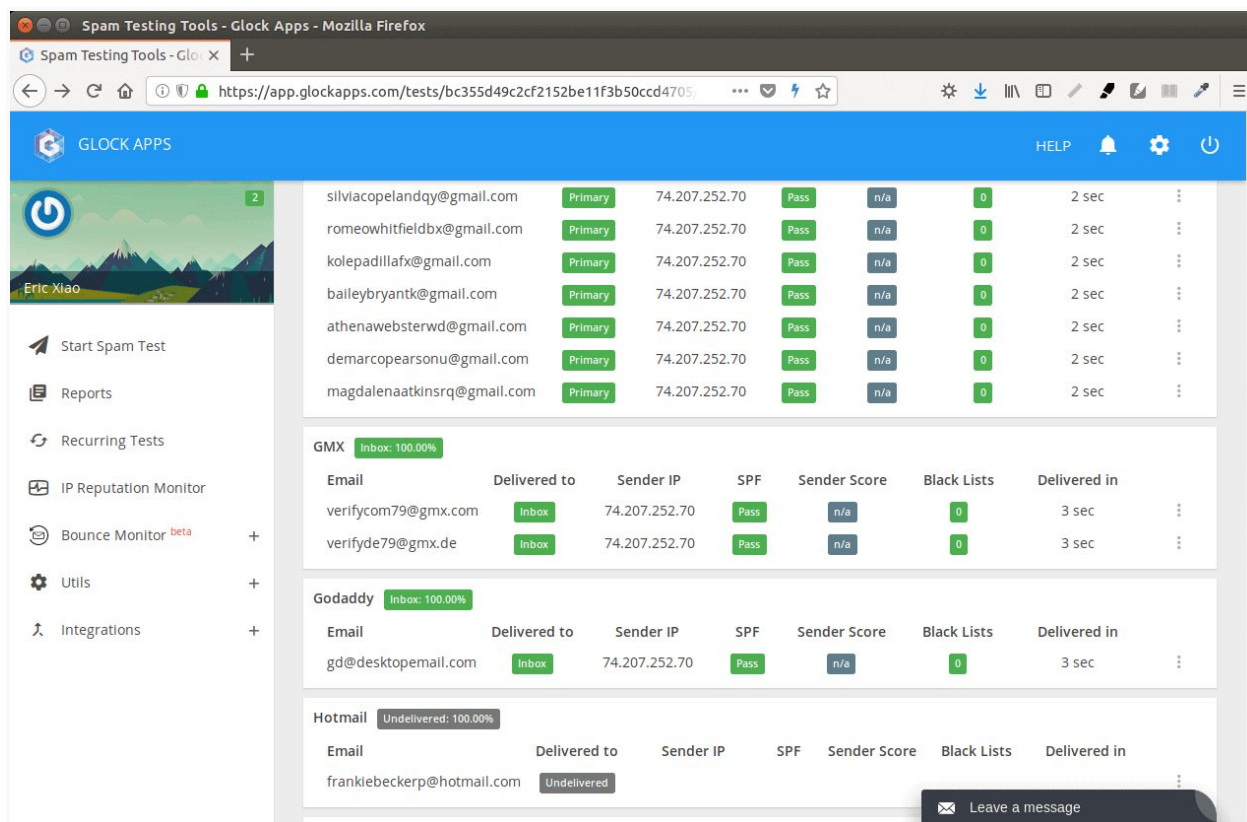
- [Creating DMARC Record to Protect Your Domain Name From Email Spoofing](#)

Step 7: Testing Email Score and Placement

After creating PTR, SPF, DKIM record, go to <https://www.mail-tester.com>. You will see a unique email address. Send an email from your domain to this address and then check your score. As you can see, I got a perfect score.



Mail-tester.com can only show you a sender score. There's another service called [GlockApps](#) that allow you to check if your email is placed in the recipient's inbox or spam folder, or rejected outright. It supports many popular email providers like Gmail, Outlook, Hotmail, YahooMail, iCloud mail, etc



What if Your Emails Are Still Being Marked as Spam?

I have more tips for you in this article: [How to stop your emails being marked as spam](#). Although it will take some time and effort, your emails will eventually be placed in inbox after applying these tips.

Auto-Renew Let's Encrypt TLS Certificate

Modoboa installed the latest version of Let's Encrypt client (certbot) as `/opt/certbot-auto`. You can find the location of certbot binary by executing the following command.

```
sudo find / -name "*certbot*"
```

Let's Encrypt TLS certificate is valid for 90 days. To automatically renew the certificate, edit root user's crontab file.

```
sudo crontab -e
```

Add the following line at the end of this file.

```
@daily /opt/certbot-auto renew -q && systemctl reload nginx  
postfix dovecot
```

Save and close the file. This tells Cron to run the certbot renew command every day. If the certificate has 30 days left, certbot will renew it. It's necessary to reload Nginx web server, Postfix SMTP server and Dovecot IMAP server so they can pick up the new certificate.

Enabling SMTPS Port 465

If you are going to use Microsoft Outlook client, then you need to [enable SMTPS port 465 in Postfix SMTP server](#).

(Optional) Set Up Autodiscover and AutoConfig to Automate Mail Client Configuration

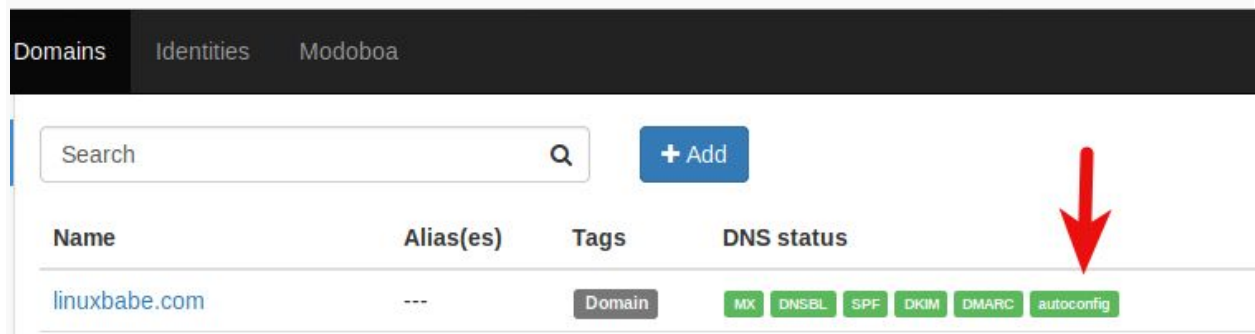
Autodiscover and AutoConfig make it easy to configure a desktop or mobile mail client. The end user just need to enter a name, email address and password to set up his/her mail account, without having to enter the SMTP or IMAP server details. Autodiscover is

supported by Microsoft Outlook mail client and AutoConfig is supported by Mozilla Thunderbird mail client.

Modoboa uses AutoMX to implement this feature on your mail server. All we need to do now is add CNAME records in DNS. In your DNS manager, create two CNAME records.

```
autoconfig.yourdomain.com      CNAME
mail.yourdomain.com
autodiscover.yourdomain.com    CNAME
mail.yourdomain.com
```

Go to the **Domains** tab in your Modoboa admin panel, if the **autoconfig** is in green, that means your CNAME records are correct. (Modoboa checks DNS records for your mail server every 30 minutes, so you might need to wait some time for autoconfig to turn green.)



Once the CNAME records are propagated to Internet, you don't have to enter the SMTP or IMAP server details when setting up mail account in Microsoft Outlook and Mozilla Thunderbird.