linuxbabe.com

How to Easily Set up a Full-Fledged Mail Server on Ubuntu 16.04 with iRedMail

https://www.linuxbabe.com/mail-server/ubuntu-16-04-iredmail-server-installation

Setting up your own mail server on Linux is complex and tedious, until you meet iRedMail. This tutorial is going to show you how you can easily and quickly set up a full-fledged mail server on Ubuntu 16.04 with iRedMail under 20 minutes.

What is iRedMail?

iRedMail is a shell script that automatically install and configure all necessary mail server components on your Linux/BSD server and thus eliminates manual installation and configuration. Supported OS are as follows:

- RHEL/CentOS
- Debian/Ubuntu
- FreeBSD/OpenBSD

Open-source software used in iRedMail:

- Postfix
- Dovecot
- Apache, Nginx
- OpenLDAP, ldapd
- MySQL/MariaDB, PostgreSQL
- Amavised-new
- SpamAssassin
- ClamAV
- Roundcube webmail
- SOGo Groupware
- Fail2ban
- Awstats
- iRedAPD

iRedMail features:

- All components are open-source.

- TLS is enabled by default. SMTP/IMAP over TLS, HTTPS webmail
- Create as many virtual mailboxes as you want in a web-based admin panel.
- Stores mail accounts in OpenLDAP, MySQL/MariaDB, or PostgreSQL.

It is recommended that you follow the instructions below on a **clean install** Ubuntu 16.04 system that has at least **2GB of RAM**. Let’s get started.

Before the Installation

First, SSH into your Ubuntu 16.04 server and update all software.

```
sudo apt update;sudo apt upgrade
```

Then set a fully qualified domain name (FQDN) for your server with the following command.

```
sudo hostnamectl set-hostname mail.your-domain.com
```

We also need to update `/etc/hosts` file.

```
sudo nano /etc/hosts
```

Edit it like below:

```
127.0.0.1       mail.your-domain.com localhost
```

Save and close the file. To see the changes, re-login and use the following command to see your hostname.

```
hostname -f
```

Don’t forget to set A record and MX record for your domain name.

Setting up a Mail Server on Ubuntu 16.04 with iRedMail

Next, download the iRedMail Bash installer with `wget`. At the time of writing, the latest version of iRedMail is 0.9.5-1, released on May 10, 2016. Please go to iRedMail download page (`http://www.iredmail.org/download.html`) to check out the latest version.

```
wget https://bitbucket.org/zhb/iredmail/downloads/iRedMail-0.9.5-1.tar.bz2
```

Extract the tarball.

```
tar xvf iRedMail-0.9.5-1.tar.bz2
```

Then cd into the newly created directory.

```
cd iRedMail-0.9.5-1/
```

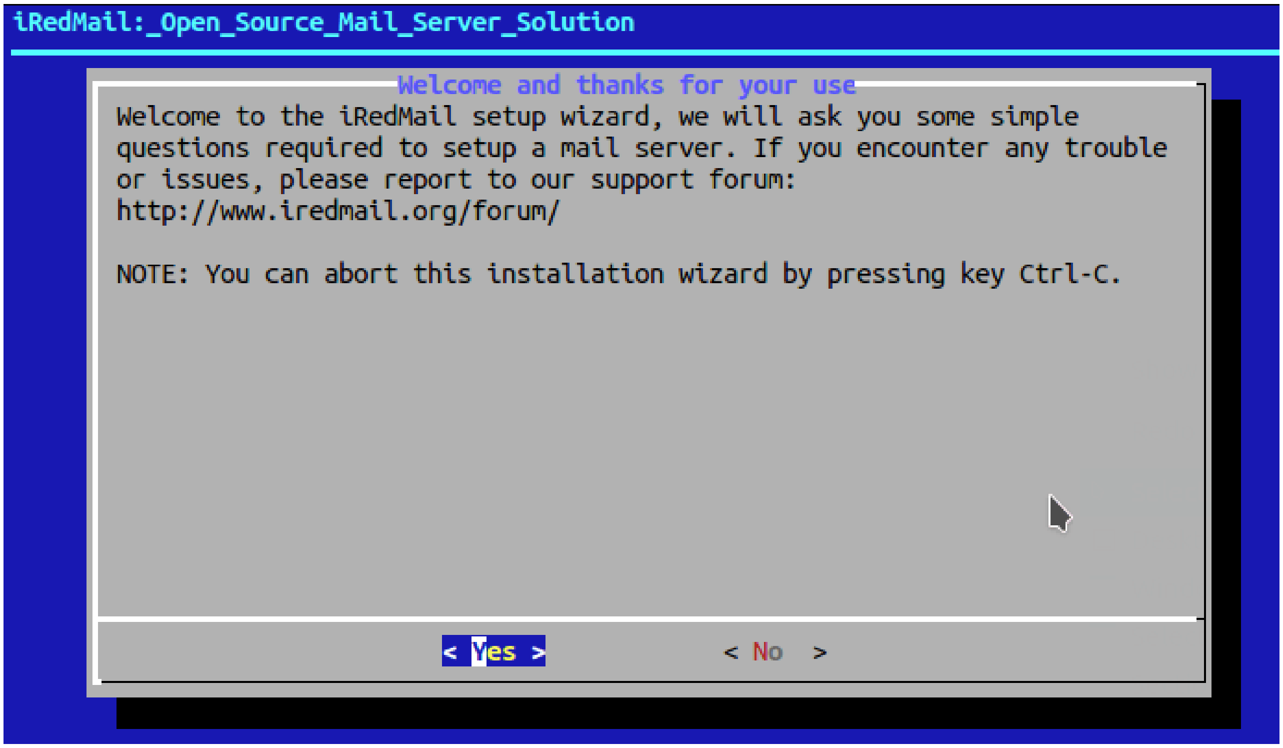
Add executable permission to the `iRedMail.sh` script.

```
chmod +x iRedMail.sh
```

Next, run the Bash script with sudo privilege.

```
sudo bash iRedMail.sh
```

The ncurse-based setup wizard will appear. Select **Yes**.



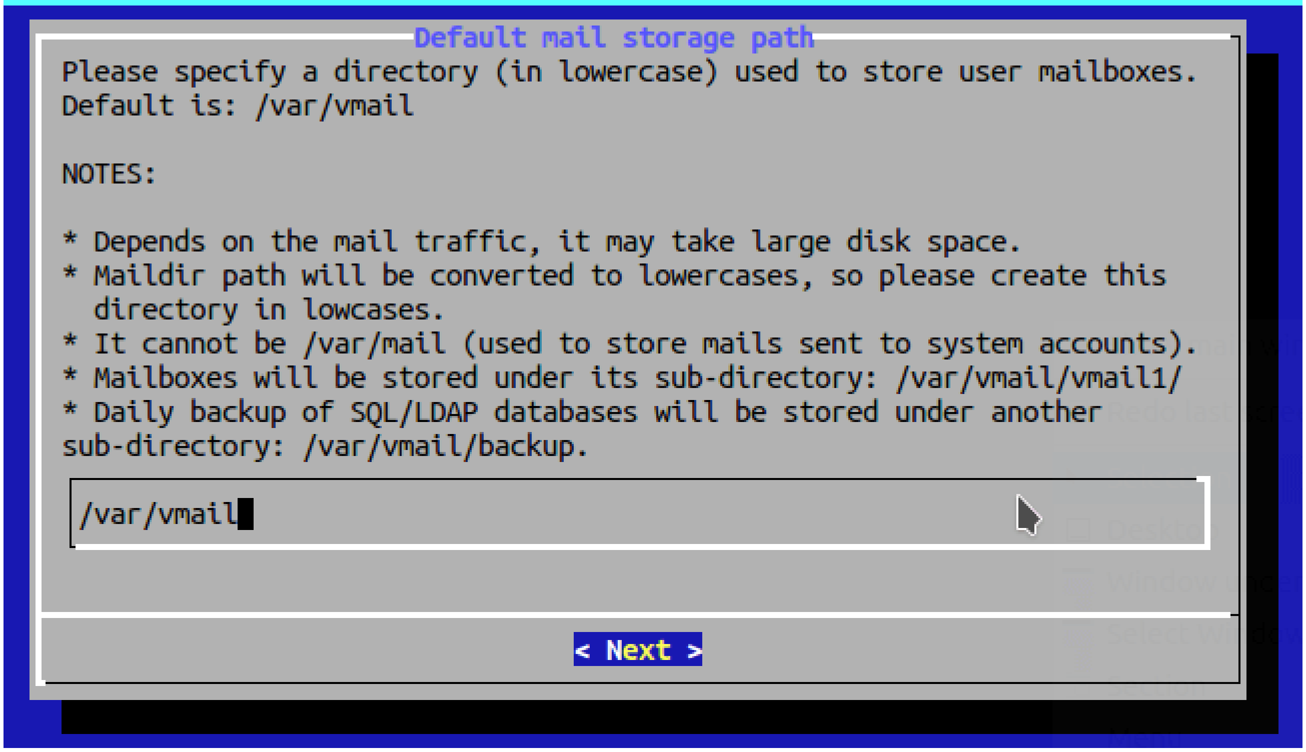
iRedMail:_Open_Source_Mail_Server_Solution

Welcome and thanks for your use

Welcome to the iRedMail setup wizard, we will ask you some simple questions required to setup a mail server. If you encounter any trouble or issues, please report to our support forum:
http://www.iredmail.org/forum/

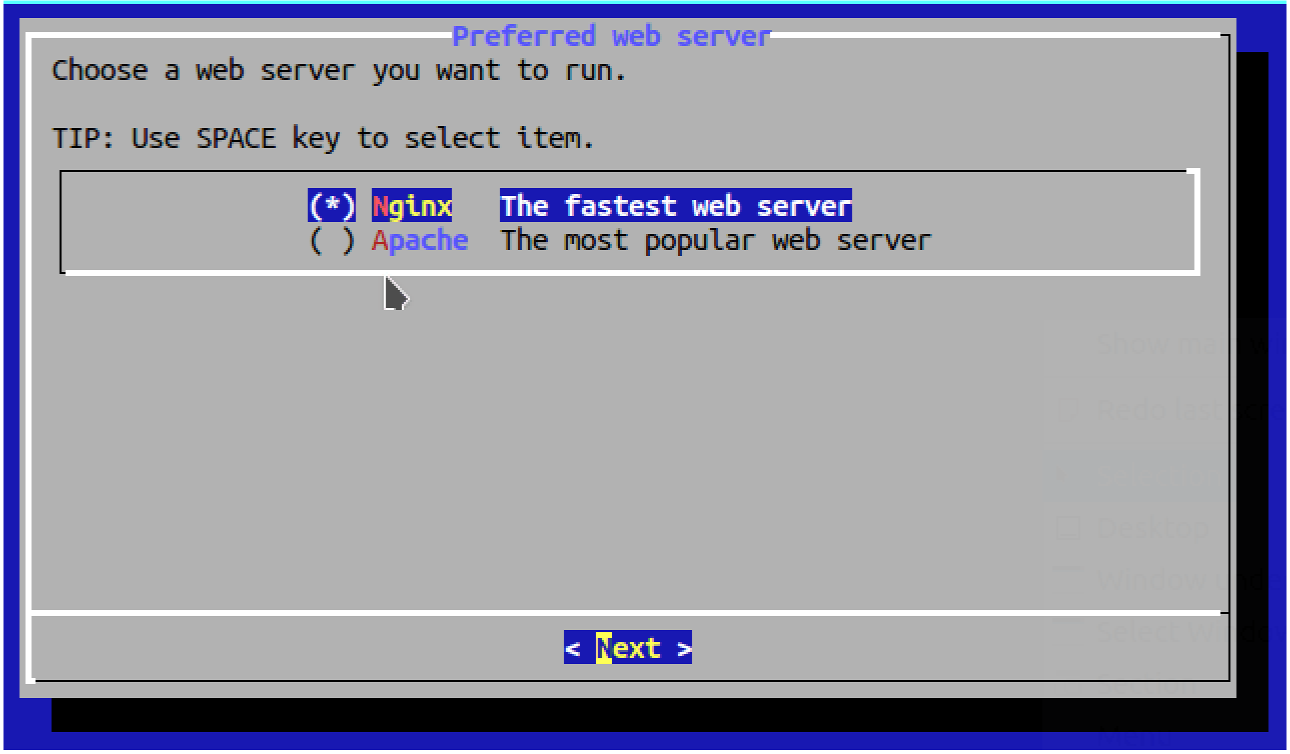
NOTE: You can abort this installation wizard by pressing key Ctrl-C.

The next screen will ask you to select the mail storage path. You can use the default one `/var/vmail`.



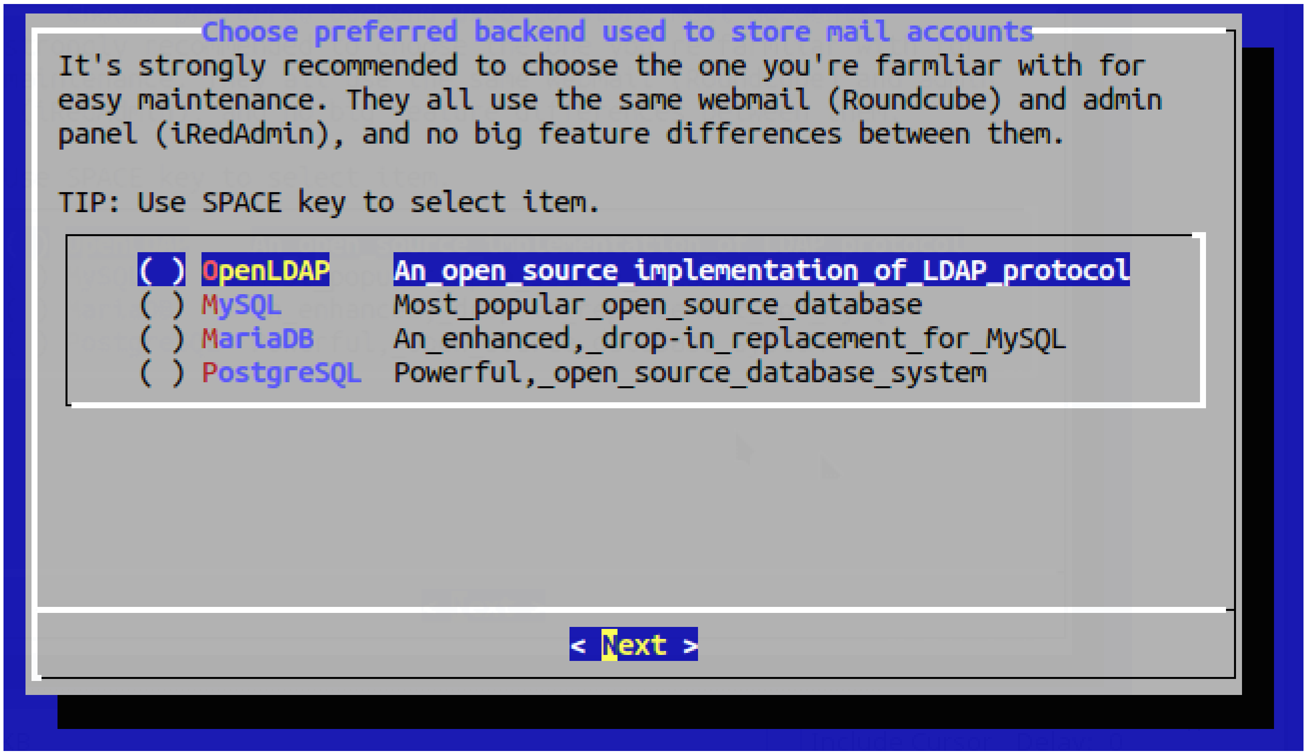
```
Default mail storage path
Please specify a directory (in lowercase) used to store user mailboxes.
Default is: /var/vmail

NOTES:

* Depends on the mail traffic, it may take large disk space.
* Maildir path will be converted to lowercases, so please create this
  directory in lowcases.
* It cannot be /var/mail (used to store mails sent to system accounts).
* Mailboxes will be stored under its sub-directory: /var/vmail/vmail1/
* Daily backup of SQL/LDAP databases will be stored under another
sub-directory: /var/vmail/backup.

/var/vmail
```

Next, choose your preferred web server: Apache or Nginx. You need to use up and down arrow and press the spacebar to select.



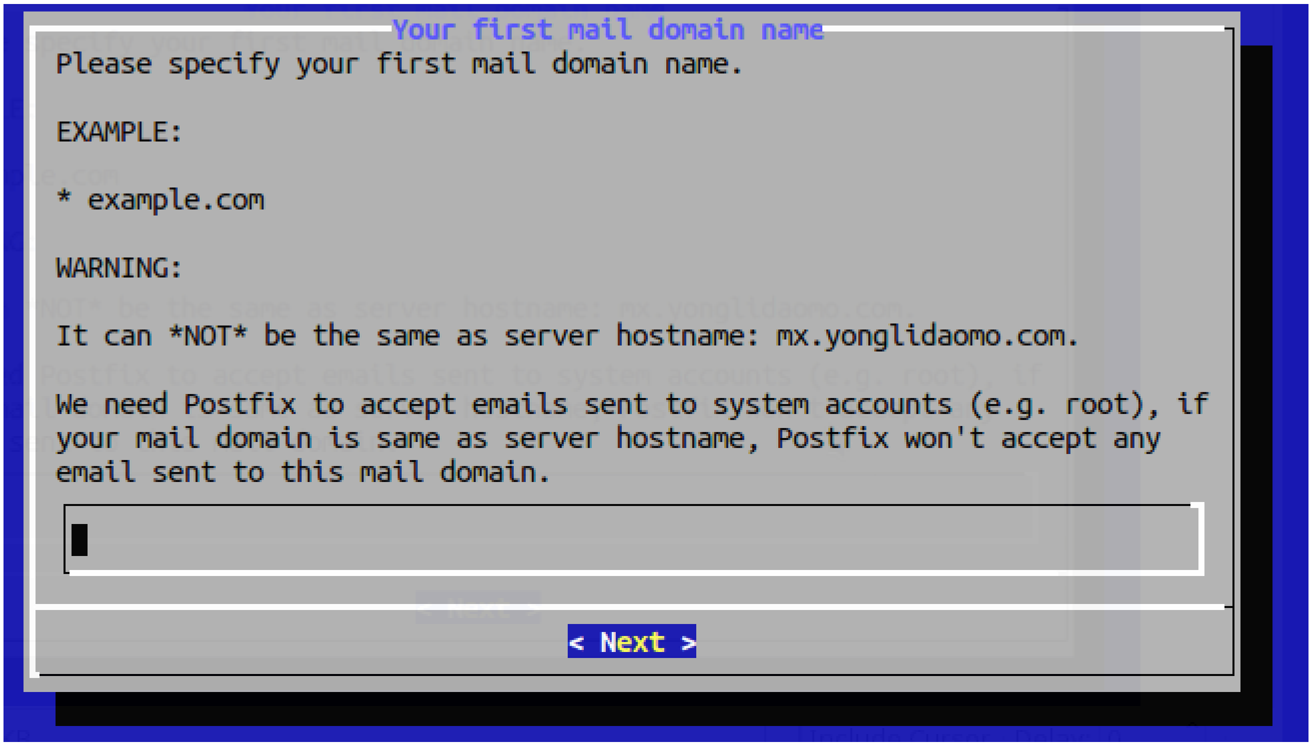
```
Preferred web server
Choose a web server you want to run.

TIP: Use SPACE key to select item.

(*) Nginx    The fastest web server
( ) Apache   The most popular web server
```

Then select the storage backend. Choose one that you are familiar with. This tutorial chose MySQL. Please note that I do not recommend MariaDB here since it by default uses unix_socket plugin which may cause access denied error.



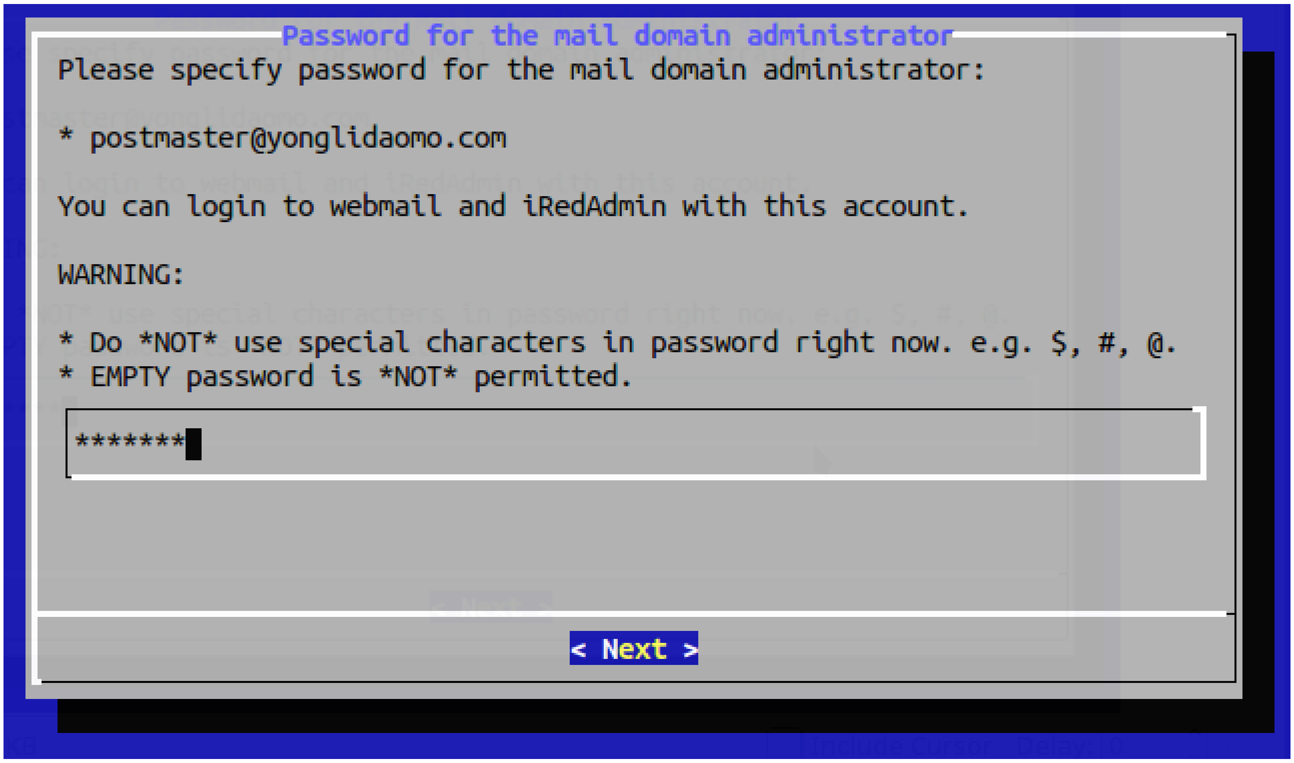
```
Choose preferred backend used to store mail accounts
It's strongly recommended to choose the one you're farmliar with for
easy maintenance. They all use the same webmail (Roundcube) and admin
panel (iRedAdmin), and no big feature differences between them.

TIP: Use SPACE key to select item.

     ( ) OpenLDAP    An_open_source_implementation_of_LDAP_protocol
     ( ) MySQL       Most_popular_open_source_database
     ( ) MariaDB     An_enhanced,_drop-in_replacement_for_MySQL
     ( ) PostgreSQL  Powerful,_open_source_database_system

                            < Next >
```

Enter your first mail domain. (e.g, linuxbabe.com) You can add multiple mail domains later in the web-based admin panel.



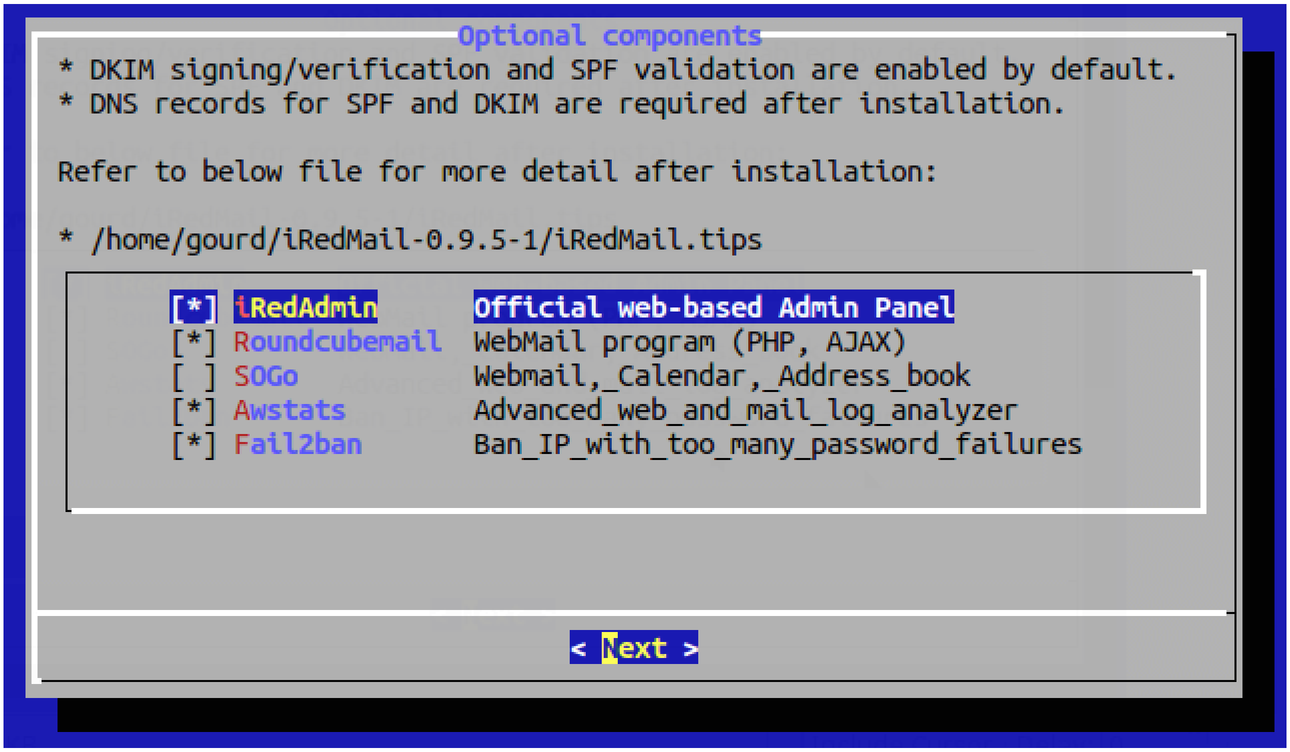
```
Your first mail domain name
Please specify your first mail domain name.

EXAMPLE:

* example.com

WARNING:

It can *NOT* be the same as server hostname: mx.yonglidaomo.com.

We need Postfix to accept emails sent to system accounts (e.g. root), if
your mail domain is same as server hostname, Postfix won't accept any
email sent to this mail domain.

                            < Next >
```

Next, set a password for the mail domain administrator.



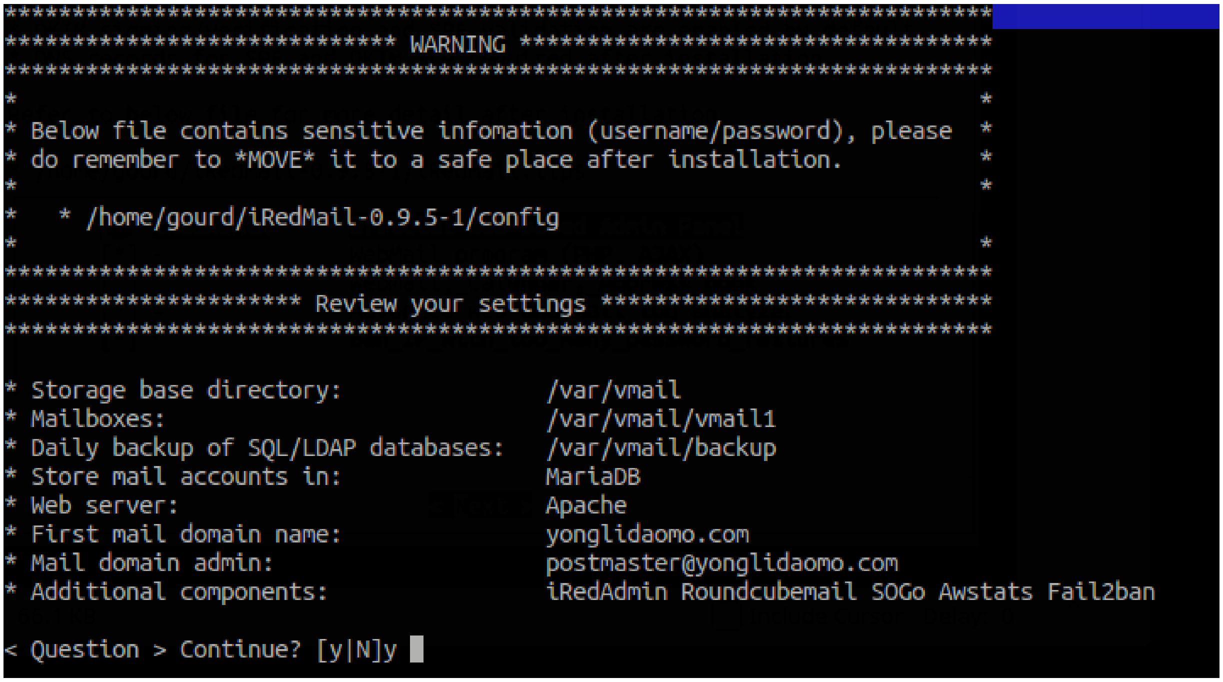
```
Password for the mail domain administrator
Please specify password for the mail domain administrator:

* postmaster@yonglidaomo.com

You can login to webmail and iRedAdmin with this account.

WARNING:

* Do *NOT* use special characters in password right now. e.g. $, #, @.
* EMPTY password is *NOT* permitted.

*******
```

Choose optional components.



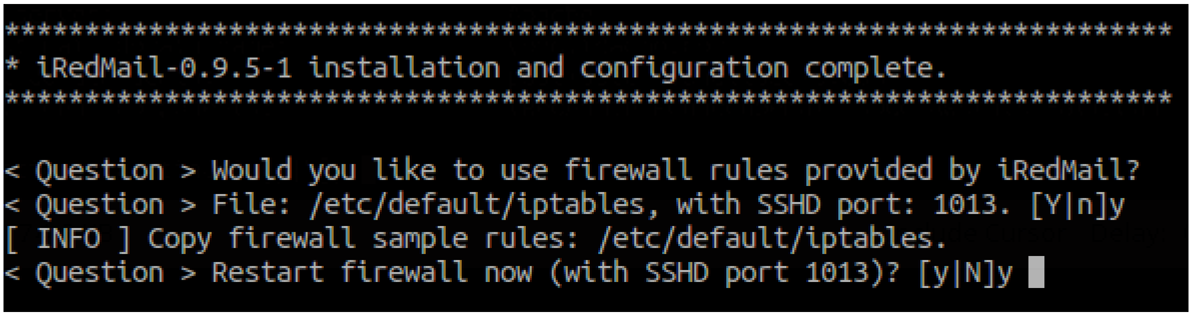
```
Optional components
* DKIM signing/verification and SPF validation are enabled by default.
* DNS records for SPF and DKIM are required after installation.

Refer to below file for more detail after installation:

* /home/gourd/iRedMail-0.9.5-1/iRedMail.tips

      [*] iRedAdmin        Official web-based Admin Panel
      [*] Roundcubemail    WebMail program (PHP, AJAX)
      [ ] SOGo             Webmail,_Calendar,_Address_book
      [*] Awstats          Advanced_web_and_mail_log_analyzer
      [*] Fail2ban         Ban_IP_with_too_many_password_failures
```

Now you can review your configurations. Type Y to begin the installation of all mail server components.



```
*************************************************************************
***************************** WARNING ***********************************
*************************************************************************
*                                                                       *
* Below file contains sensitive infomation (username/password), please  *
* do remember to *MOVE* it to a safe place after installation.          *
*                                                                       *
*   * /home/gourd/iRedMail-0.9.5-1/config
*                                                                       *
*************************************************************************
********************** Review your settings *****************************
*************************************************************************

* Storage base directory:               /var/vmail
* Mailboxes:                            /var/vmail/vmail1
* Daily backup of SQL/LDAP databases:   /var/vmail/backup
* Store mail accounts in:               MariaDB
* Web server:                           Apache
* First mail domain name:               yonglidaomo.com
* Mail domain admin:                    postmaster@yonglidaomo.com
* Additional components:                iRedAdmin Roundcubemail SOGo Awstats Fail2ban

< Question > Continue? [y|N]y
```

At the end of installation, choose y to use firewall rules provided by iRedMail and restart firewall.



```
*************************************************************************
* iRedMail-0.9.5-1 installation and configuration complete.
*************************************************************************


< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/default/iptables, with SSHD port: 1013. [Y|n]y
[ INFO ] Copy firewall sample rules: /etc/default/iptables.
< Question > Restart firewall now (with SSHD port 1013)? [y|N]y
```

Now iRedMail installation is complete. You will be notified the URL of webmail, SOGo groupware and web admin panel and the login credentials. The `iRedMail.tips` file contains important information about your iRedMail server.

```
********************************************************************
* URLs of installed web applications:
*
* - Roundcube webmail: httpS://mail.your-domain.com/mail/
* - SOGo groupware: httpS://mail.your-domain.com/SOGo/
*
* - Web admin panel (iRedAdmin): httpS://mail.your-domain.com/iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@your-domain.com
* - Password: *********
*
*
********************************************************************
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
```

```
*   - /home/gourd/iRedMail-0.9.5-1/iRedMail.tips
*
* And it's sent to your mail account postmaster@your-domain.com.
*
********************* WARNING **************************************
*
* Please reboot your system to enable all mail services.
*
********************************************************************
```

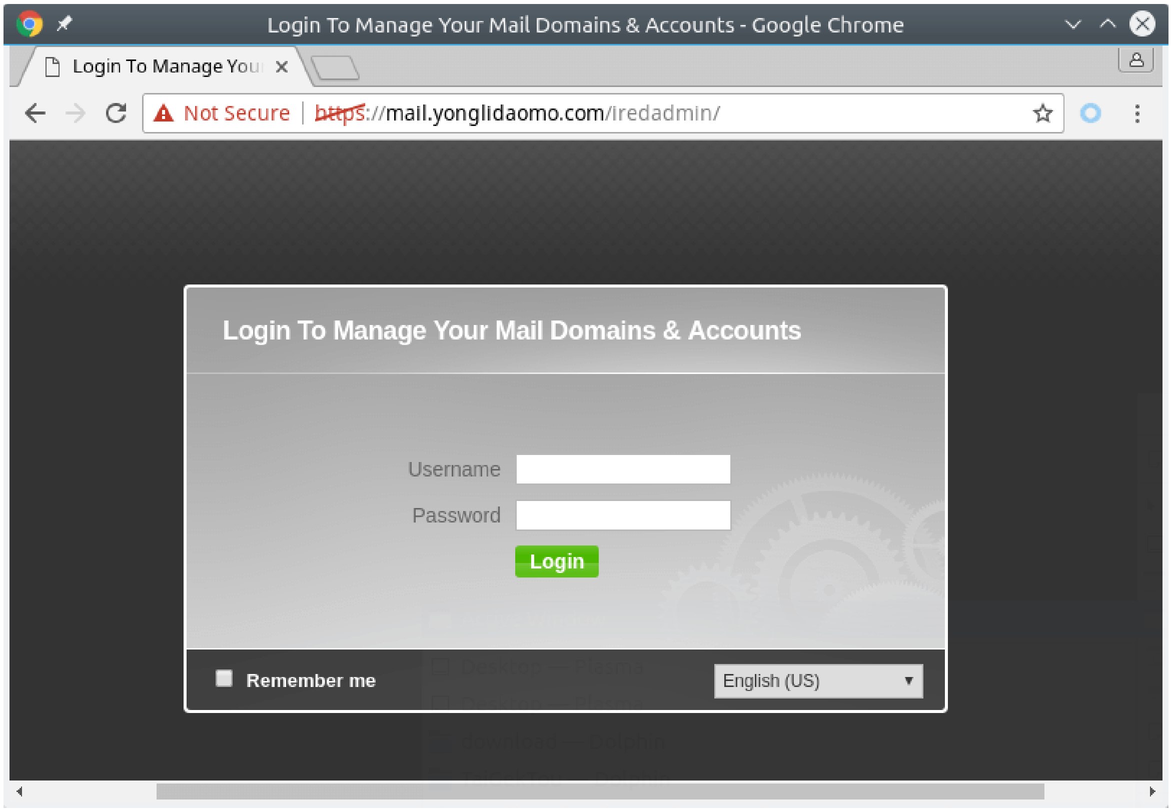
Reboot your Ubuntu 16.04 server.

```
sudo shutdown -r now
```

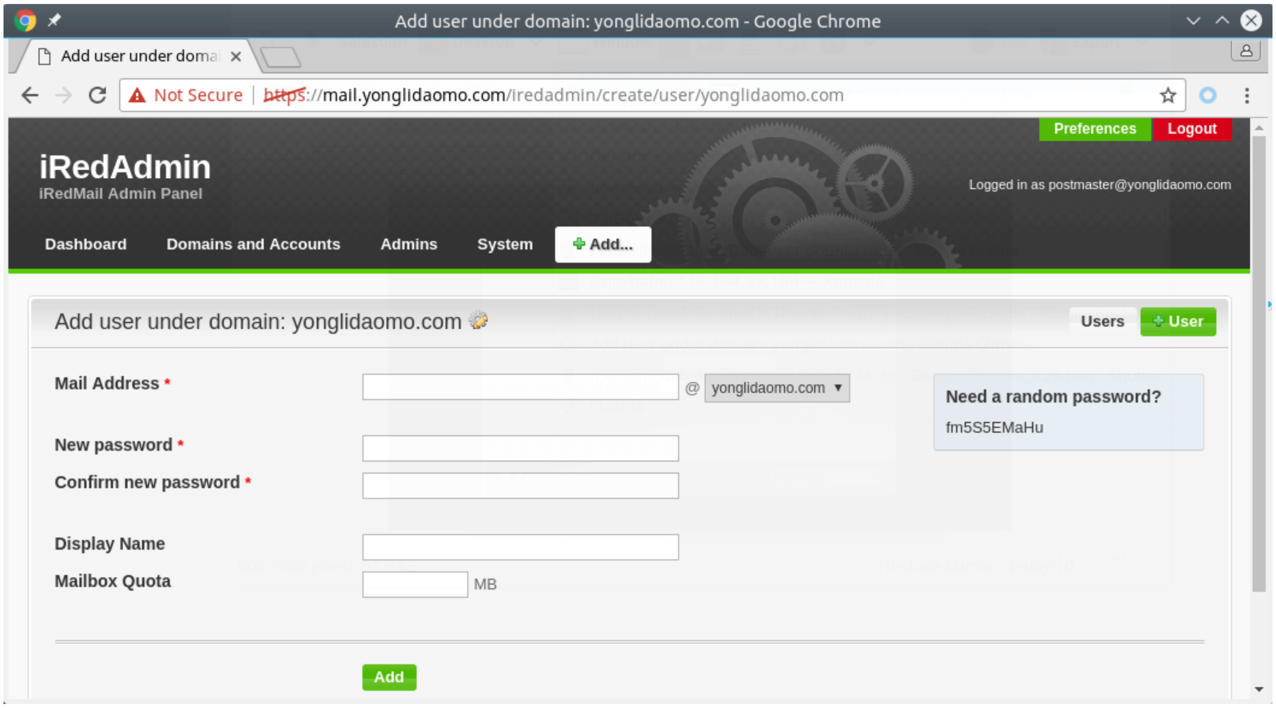
Once your server is back online, you can visit the web admin panel.

```
https://mail.your-domain.com/iredadmin/
```

Because it’s using a self-signed TLS certificate, so you need to add security exception. Login with the postmaster mail account.


Login To Manage Your Mail Domains & Accounts - Google Chrome
Login To Manage You
Not Secure
https://mail.yonglidaomo.com/iredadmin/
Login To Manage Your Mail Domains & Accounts
Username
Password
Login
Remember me
English (US)

In the Add tab, you can add multiple domains or mail users.



Add user under domain: yonglidaomo.com - Google Chrome

Not Secure | ~~https~~://mail.yonglidaomo.com/iredadmin/create/user/yonglidaomo.com

iRedAdmin
iRedMail Admin Panel

Logged in as postmaster@yonglidaomo.com

Add user under domain: yonglidaomo.com

Mail Address * @ yonglidaomo.com

New password *

Confirm new password *

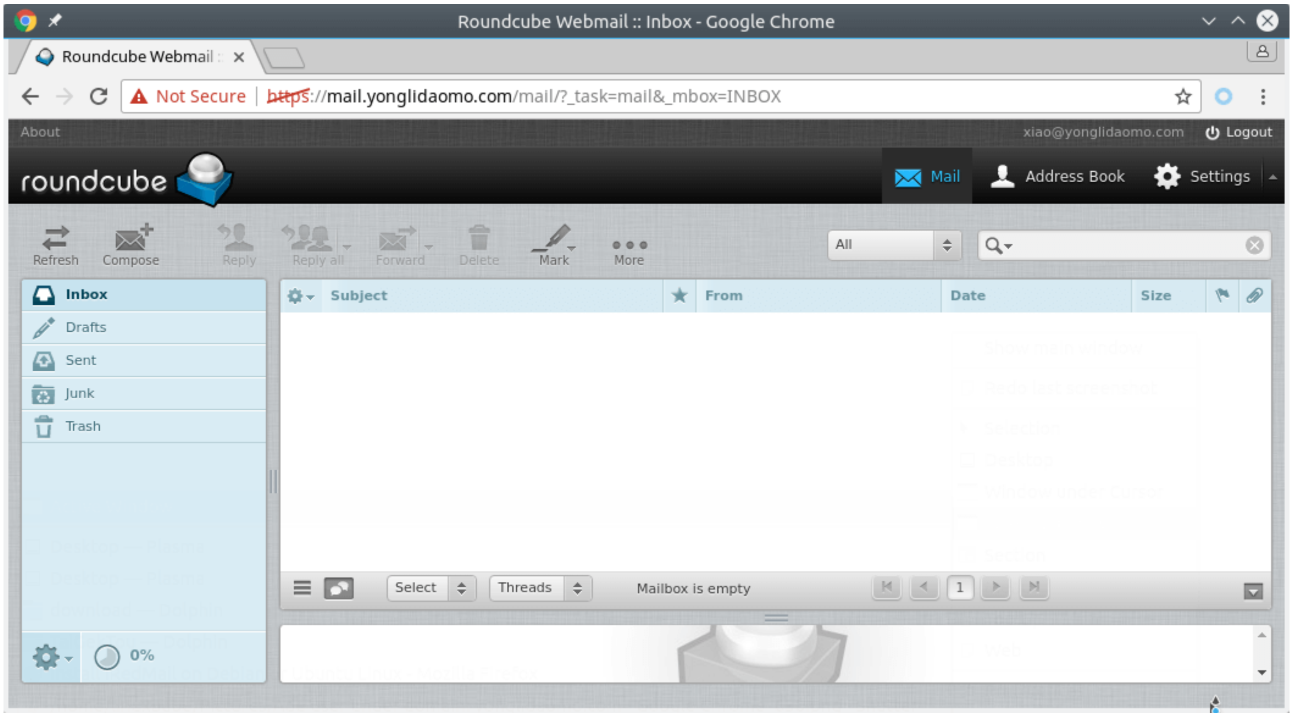
Display Name

Mailbox Quota MB

Need a random password?
fm5S5EMaHu

After you create a user, you can visit the Roundcube webmail address and login with the new mail user account.

```
https://mail.your-domain.com/mail/
```



Roundcube Webmail :: Inbox - Google Chrome

Not Secure | ~~https~~://mail.yonglidaomo.com/mail/?_task=mail&_mbox=INBOX

xiao@yonglidaomo.com

Mailbox is empty

And test email sending and receiving. Please note that you may need to wait for a few minutes to receive emails because greylisting is enabled by default.

Installing Let’s Encrypt TLS Certificate

Since the mail server is using a self-signed TLS certificate, both desktop mail client users and webmail client users will see a warning. To fix this, we can obtain and install a free Let’s Encrypt TLS cert.

Obtaining the Certificate

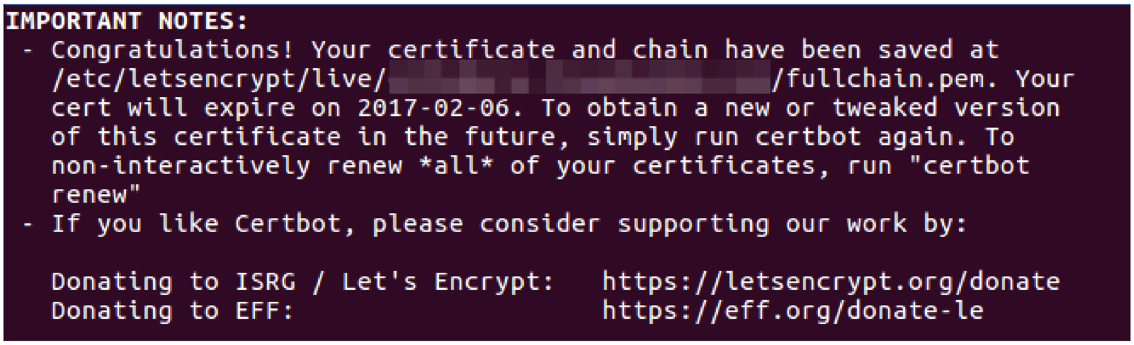
First, install Let’s Encrypt (certbot) client on Ubuntu 16.04.

```
sudo apt install letsencrypt
```

Then use the webroot plugin to obtain the certificate. Replace red text with your actual data.

```
sudo letsencrypt certonly --webroot --agree-tos --email your-email-address -d
mail.your-domain.com -w /var/www/html/
```

You will see the following text indicating that you have successfully obtained a TLS certificate. Your certificate and chain have been saved at `/etc/letsencrypt/live/mail.your-domain.com/` directory.



```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/[redacted]/fullchain.pem. Your
   cert will expire on 2017-02-06. To obtain a new or tweaked version
   of this certificate in the future, simply run certbot again. To
   non-interactively renew *all* of your certificates, run "certbot
   renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

If you use Nginx, you need to add the following lines in the http section of `/etc/nginx/conf.d/00-default.conf` file.

```
location ~ /.well-known/acme-challenge {
     allow all;
 }
```

And comment out the following line.

```
include /etc/nginx/templates/misc.tmpl;
```

Then reload nginx.

```
sudo systemctl reload nginx
```

And issue the following line to obtain the certificate.

```
sudo letsencrypt certonly --webroot --agree-tos --email your-email-address -d
mail.your-domain.com -w /var/www/
```

Installing the Certificate

After obtaining the TLS certificate, let’s configure web server to use it. If you use Apache web server, then edit the default virtual host file.

```
sudo nano /etc/apache2/sites-available/000-default.conf
```

Add the following 3 lines above `</VirtualHost>`.

```
RewriteEngine on
RewriteCond %{SERVER_NAME} =mail.your-domain.com
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,QSA,R=permanent]
```

This will redirect HTTP connection to HTTPS. Then edit the https version of the default virtual host.

```
sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Find the following 2 lines.

```
SSLCertificateFile /etc/ssl/certs/iRedMail.crt
SSLCertificateKeyFile /etc/ssl/private/iRedMail.key
```

We need to replace the self-signed certificate with Let’s Encrypt issued certificate. So the above two lines need to be changed to the following.

```
SSLCertificateFile /etc/letsencrypt/live/mail.your-domain.com/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/mail.your-domain.com/privkey.pem
```

Save and close the file. Then reload Apache web server.

```
sudo systemctl reload apache2
```

Now if you visit iRedMail admin panel or Roundcube webmail again, you shall see a green lock in the browser address bar.

If you use Nginx, then edit the default server block file.

```
sudo nano /etc/nginx/conf.d/00-default.conf
```

In the `https` section, find the following 2 lines.

```
ssl_certificate /etc/ssl/certs/iRedMail.crt;
ssl_certificate_key /etc/ssl/private/iRedMail.key;
```

Replace them with:

```
ssl_certificate /etc/letsencrypt/live/mail.your-domain.com/fullchain.pem
ssl_certificate_key /etc/letsencrypt/live/mail.your-domain.com/privkey.pem
```

Save and close the file. Then test nginx configuration and reload.

```
sudo nginx -t
```

```
sudo systemctl reload nginx
```

Visit iRedMail admin panel or Roundcube webmail again, you shall see a green lock in the browser address bar.

We also need to configure Postfix and Dovecot to use the Let’s Encrypt issued certificate so that desktop mail client won’t display security warning.

Edit the main configuration file of Postfix.

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

Find the following 3 lines. (line 95, 96, 97).

```
smtpd_tls_key_file = /etc/ssl/private/iRedMail.key
smtpd_tls_cert_file = /etc/ssl/certs/iRedMail.crt
smtpd_tls_CAfile = /etc/ssl/certs/iRedMail.crt
```

Replace them with:

```
smtpd_tls_key_file = /etc/letsencrypt/live/mail.your-domain.com/privkey.pem
smtpd_tls_cert_file = /etc/letsencrypt/live/mail.your-domain.com/cert.pem
smtpd_tls_CAfile = /etc/letsencrypt/live/mail.your-domain.com/chain.pem
```

Save and close the file. Then reload Postfix.

```
sudo postfix reload
```

Next, edit the main configuration file of Dovecot.

```
sudo nano /etc/dovecot/dovecot.conf
```

Fine the following 2 lines. (line 40, 41)

```
ssl_cert = </etc/ssl/certs/iRedMail.crt
ssl_key = </etc/ssl/private/iRedMail.key
```

Replace them with:

```
ssl_cert = </etc/letsencrypt/live/mail.your-domain.com/fullchain.pem
ssl_key = </etc/letsencrypt/live/mail.your-domain.com/privkey.pem
```

Save and close the file. Then reload dovecot.

```
sudo dovecot reload
```

From now on, desktop mail users won’t see security warnings.

Auto Renew TLS Certificate

To auto renew certificate, simply open root user’s crontab file.

```
sudo crontab -e
```

Then add the following line at the bottom of the file.

```
@daily letsencrypt renew --quiet && postfix reload && dovecot reload && systemctl
reload apache2
```

If you use Nginx, then replace `systemctl reload apache2` with `systemctl reload nginx`. Reloading is necessary to make these programs pick up the new certificate and private key.

Creating PTR, SPF, DKIM Records

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

PTR record

A pointer record, or PTR record, maps an IP address to a FQDN. It's the counterpart to the A record and is used for reverse DNS lookup.

Reverse resolution of A record with PTR record can help with blocking spammers. Many MTAs accept email only if the server is really responsible for a certain domain.

To check the PTR record for an IP address:

```
dig -x <IP> +short
```

or

```
host <IP>
```

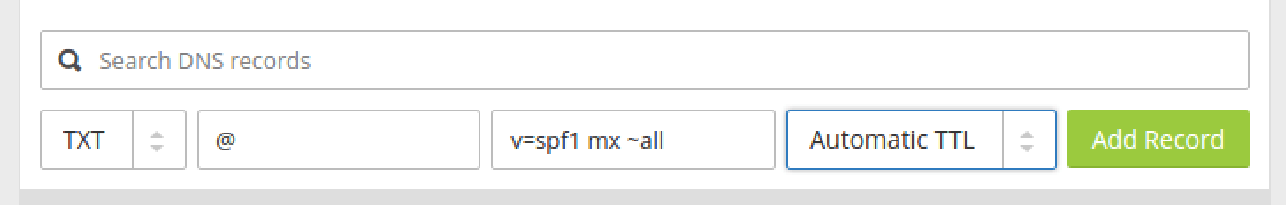
Because you get IP address from your hosting provider, not from your domain registrar, so you must set PTR record for your IP in the control panel of your hosting provider.

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.

```
TXT  @   v=spf1 mx ~all
```



TXT | @ | v=spf1 mx ~all | Automatic TTL

Explanation:

- **TXT** indicates this is a TXT record.
- Enter **@** in the name field.

- **v=spf1** indicates this is a SPF record and the SPF record 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.

Note that some DNS managers require you to wrap the SPF record with quotes like below.

```
TXT  @   "v=spf1 mx ~all"
```

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.

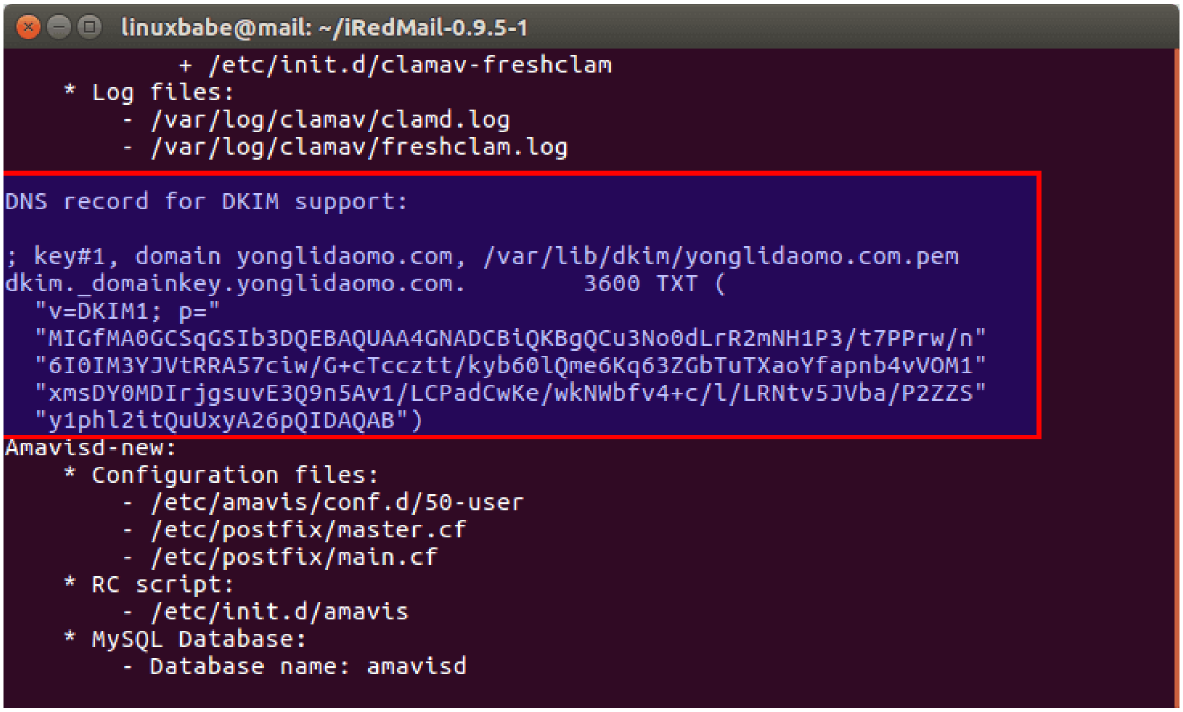
DKIM Record

DKIM (DomainKeys Identified Mail) use a private key to **add a signature to emails sent from your domain**. Receiving SMTP server verify the signature using the pubic key which is published in your DNS manager.

The iRedMail script automatically configured DKIM for your server. The only thing left to do is creating DKIM record in DNS manager. Open the `iRedMail.tips` file under `iRedMail-0.9.5-1` directory.

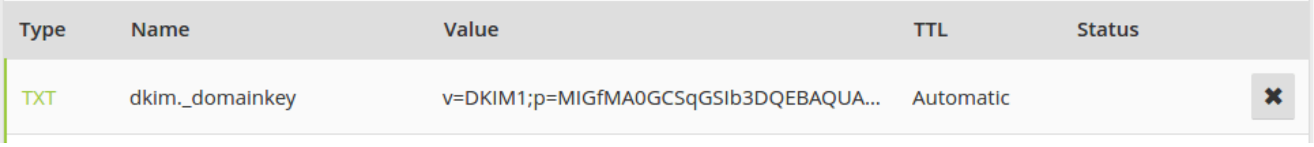
```
sudo nano iRedMail.tips
```

Scroll down to `DNS record for DKIM support` section.



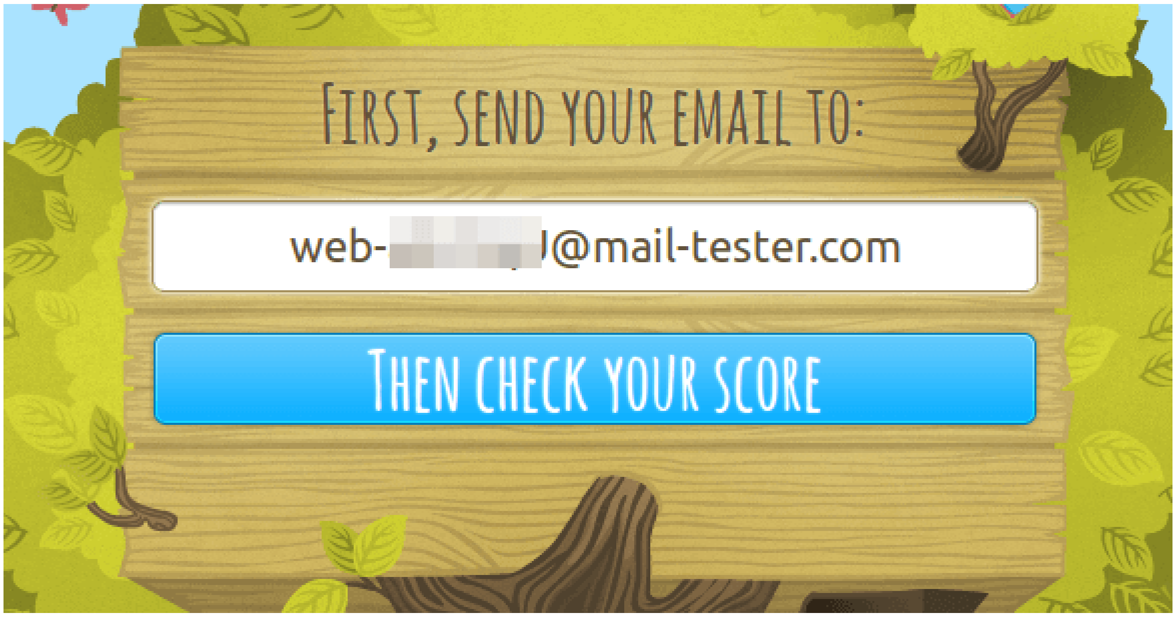
```
linuxbabe@mail: ~/iRedMail-0.9.5-1
            + /etc/init.d/clamav-freshclam
    * Log files:
        - /var/log/clamav/clamd.log
        - /var/log/clamav/freshclam.log

DNS record for DKIM support:

; key#1, domain yonglidaomo.com, /var/lib/dkim/yonglidaomo.com.pem
dkim._domainkey.yonglidaomo.com.        3600 TXT (
  "v=DKIM1; p="
  "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCu3No0dLrR2mNH1P3/t7PPrw/n"
  "6I0IM3YJVtRRA57ciw/G+cTcztt/kyb60lQme6Kq63ZGbTuTXaoYfapnb4vVOM1"
  "xmsDY0MDIrjgsuvE3Q9n5Av1/LCPadCwKe/wkNWbfv4+c/l/LRNtv5JVba/P2ZZS"
  "y1phl2itQuUxyA26pQIDAQAB")
Amavisd-new:
    * Configuration files:
        - /etc/amavis/conf.d/50-user
        - /etc/postfix/master.cf
        - /etc/postfix/main.cf
    * RC script:
        - /etc/init.d/amavis
    * MySQL Database:
        - Database name: amavisd
```

Then in you DNS manager, create a TXT record, enter dkim._domainkey in the name field. Copy everything in the parentheses and paste into the value field. Delete all double quotes and white spaces.



Type	Name	Value	TTL	Status	
TXT	dkim._domainkey	v=DKIM1;p=MIGfMA0GCSqGSIb3DQEBAQUA...	Automatic		✖

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.



Adding Multiple Mail Domains

If you want to add another mail domain, then you need to

- add a new mail domain and user in iRedMail admin panel.
- create MX, SPF record for the new mail domain.
- tell amavisd to sign email messages for the new domain.

The MX record should point to your mail server's FQDN,

```
Record Type    Name      Value

MX             @         mail.your-domain.com
```

Then create SPF record to allow the MX host to send email for the new mail domain.

```
Record Type    Name      Value

TXT            @         v=spf1 mx ~all
```

Next you need to tell amavisd to sign every email message for the new mail domain. You can use the existing private key to sign for the new domain. Edit `/etc/amavis/conf.d/50-user` file.

```
sudo nano /etc/amavis/conf.d/50-user
```

Find the following lines in the file.

```
@dkim_signature_options_bysender_maps = ( {
    ...
    "your-domain.com"  => { d => "your-domain.com", a => 'rsa-sha256', ttl =>
10*24*3600 },
    ...
});
```

Add the following line to tell amavisd to sign with the same private key.

```
"new_domain.com" => { d => "your-domain.com", a => 'rsa-sha256', ttl =>
10*24*3600 },
```

So the configurations will be changed to the following.

```
@dkim_signature_options_bysender_maps = ( {
    ...
    "your-domain.com"  => { d => "your-domain.com", a => 'rsa-sha256', ttl =>
10*24*3600 },
    "new_domain.com" => { d => "your-domain.com", a => 'rsa-sha256', ttl =>
10*24*3600 },
    ...
});
```

Save and close the file. Then restart amavisd.

```
sudo systemctl restart amavis
```

Now you can use the new domain to send and receive emails. Don’t forget to test your score at **https://www.mail-tester.com**.

PTR record is used for mapping IP address to hostname, so you don’t need to worry about it when adding another mail domain.

That’s it!

I hope this tutorial helped you set up a mail server with iRedMail on Ubuntu 16.04. **Subscribe to our free newsletter** to get latest Linux tutorials. You can also follow us on Google+, Twitter or like our Facebook page.

Rate this tutorial

[Total: 12 Average: 4.3]