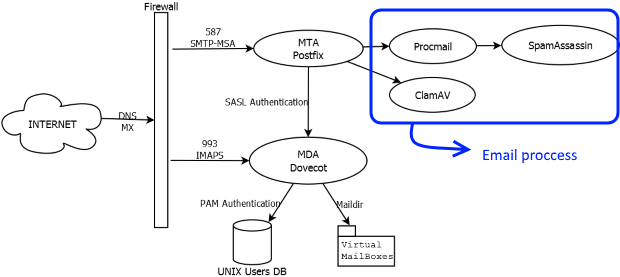
Setting up an email server for our website is the most complicated.   
Make sure you really need a hosted email server by you before doing this step.   
We will set up a configuration shown below :   
   
  
The "email process" section will be covered in a later chapter of this ebook.   
The core of the server is done by a so called Mail Transfer Agent (MTA).   
We are going to use **Postfix** as MTA in our setup.   
An older less secure MTA was sendmail but most modern systems use Postfix.   
Postfix will listen to the Port 587.   
This port is used for the so called: Simple Mail Transfer Protocol - Mail Submission Agent.   
SMTP is a protocol for **sending** emails over the Internet.   
MSA requires that clients are authorized and authenticated in order to sent mails.  
  
In order to **deliver** emails you need a MDA (Mail Delivery Agent).   
We are going to use **Dovecot** with IMAPS protocol.   
Internet Message Access Protocol (over SSL) is a secure email protocol used for accessing emails on a remote mail server from a local client.   
For retrieving messages, email client applications, also called Mail User Agents (MUA), usually use either POP3 or IMAP.   
We will cover only the IMAP protocol since it is more **powerful** than the POP3.   
IMAP stores all emails at the server instead POP3 downloads all emails to the client and after that deletes them from the server.   
If you have more physical devices connected on the same email account, like nowadays, IMAP protocol is a better option since it allows you to synchronize all of your devices at once.   
Using POP3 instead you have to synchronize your devices manually.   
Notice that Dovecot also supports the POP3 communication protocol. 

We will use **Thunderbird** as email client (MUA) .   
Using the Port 993 (IMAPS) we can deliver our emails from Dovecot to our email client.   
Before starting, if you followed this ebook, you should have already created a **MX** record like **mail.website1.com** for your zone **website1.com**. If not take a look again at the [DNS](http://www.trustfm.net/ebooks/DedicatedServer.php?page=DNS) section. 

Installations

Log in to your dedicated server using **PuTTY**. Make sure you remove sendmail. 

**yum remove sendmail sendmail-cf sendmail-doc**

Install Postfix:

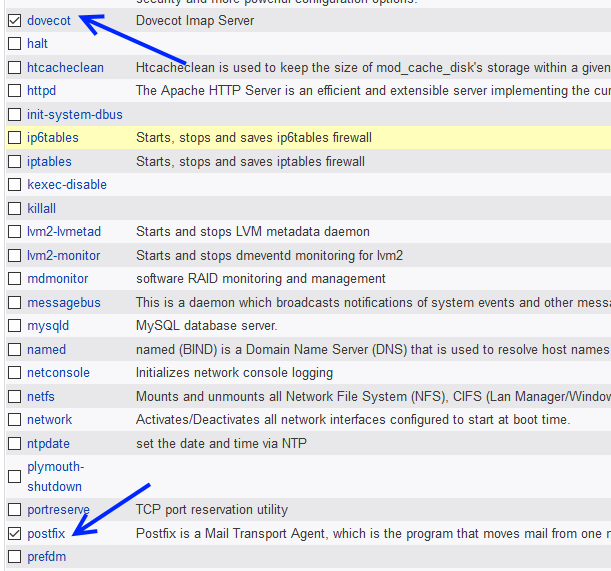
**yum install postfix**

Install Dovecot: 

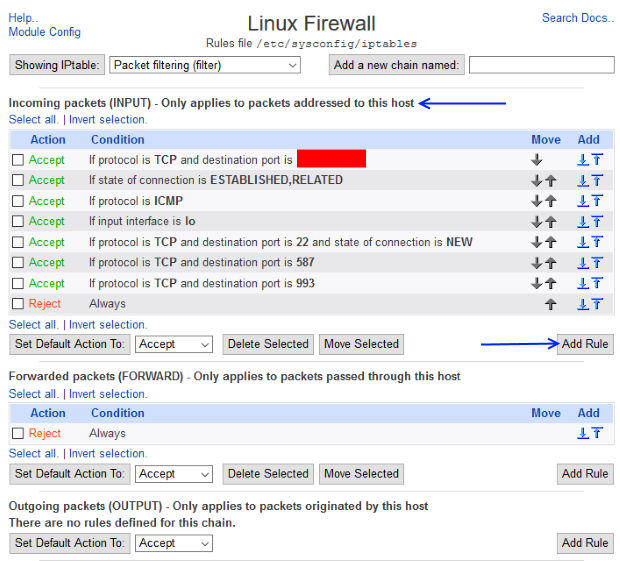
**yum install dovecot**

If for some reason you want to un-install Postfix and / or Dovecot : 

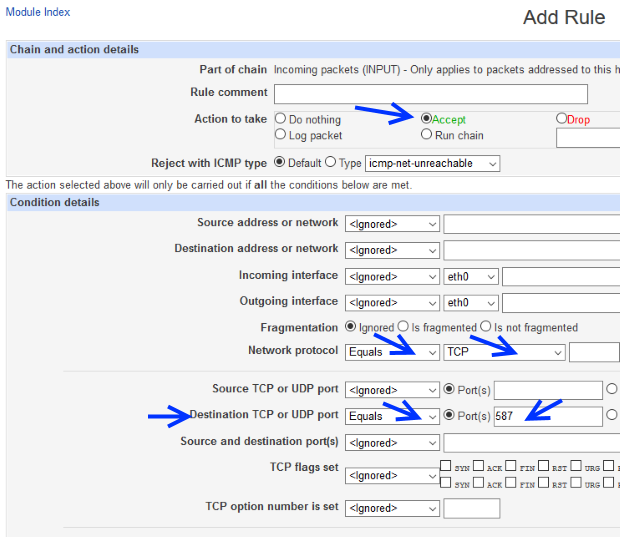
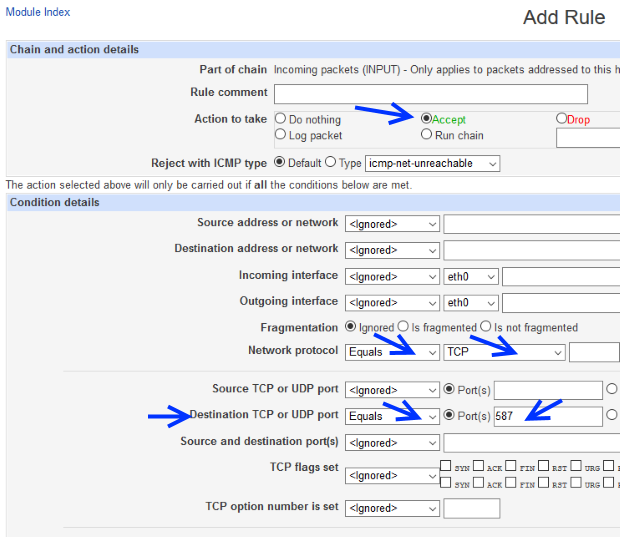
**yum -C remove postfix**  
**yum -C remove dovecot**

Notice that both of the modules can be also installed from Webmin Web interface under the **Un-used Modules** section.   
  
From Webmin go to System > Bootup and Shutdown.   
Check **dovecot**, **postfix** and press the **Start on Boot** button.   
 

Firewall Configuration

From Webmin go to Networking > Linux Firewall.   
Under **Incoming packets (INPUT) - Only applies to packets addressed to this host**, find and click on the "Add Rule" button.   
   
  
In the "Add Rule" page fill like this : 

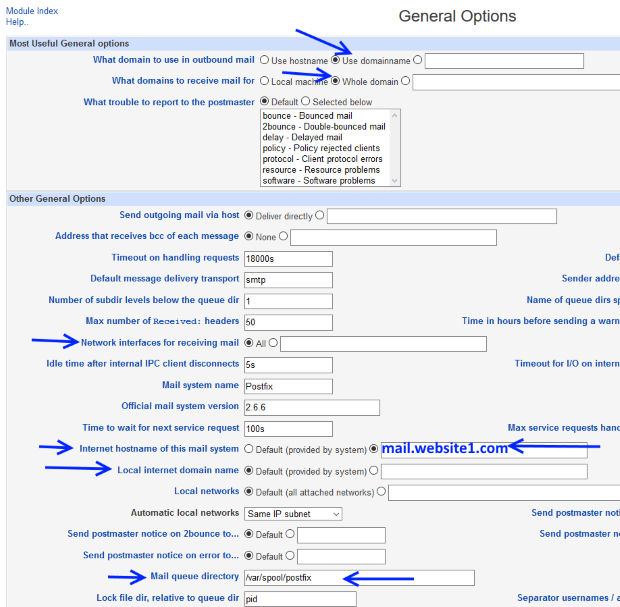
Set "Action to take" to **Accept**  
As "Network protocol", select **Equals** and **TCP**  
As "Destination TCP or UDP port", select **Equals** and set Port(s) to **587**

Click the "Create" button on the bottom of the page.   
   
  
Do the same for the port **993**  
Notice that the port 25 is not needed to be open since we are going to use only secure connections on our server.  
  
So as final result you should have under "Incoming packets (INPUT) - Only applies to packets addressed to this host" something like the photo below   
   
  
Click on the "Apply Configuration" button in order to apply your firewall rules.   
After doing this go to [Kimsufi manager](https://www.kimsufi.com/fr/manager/" \t "parent) and press the "Restart" button in order to do a hardware restart of your machine.

Postfix Configuration

Go to Servers > Postfix Mail Server and click over the "General Options" icon.   
 Fill the "General Options" page like this :

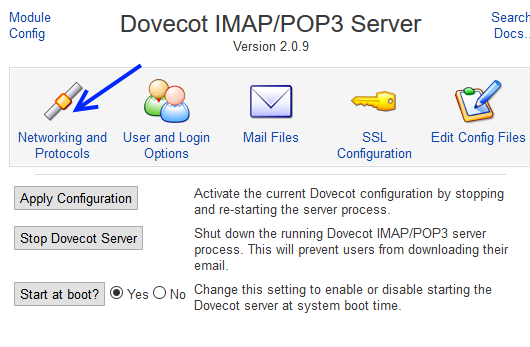
Set "What domain to use in outbound mail" to: **Use domainname**.  
Set "What domains to receive mail for" to: **Whole domain**.  
Set "Network interfaces for receiving mail" to **All**.   
Set "Internet hostname of this mail system" to **mail.website1.com**   
Notice that this hostname will be our base host name for all other email domains hosted in our server.   
Set "Local internet domain name" to **Default**.   
This sets the mail domain to the hostname without the first component. In our case, this would be website1.com   
Make sure that "Mail queue directory" is set to : **/var/spool/postfix**.

   
  
Click the "Save and Apply button".   
Click the "Stop Postfix" and then the "Start Postfix" button to restart the mail system.   
  
Test your Postfix mail server by logging at your server using PuTTY and writing the command : 

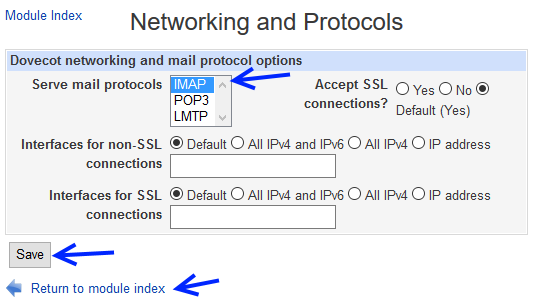
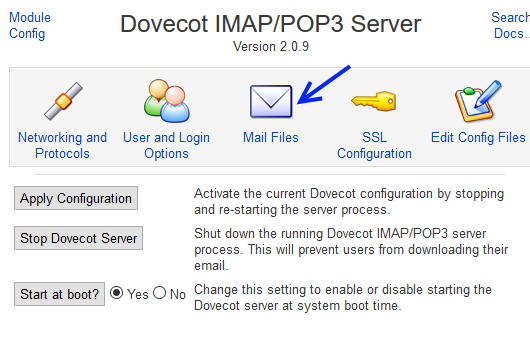
**echo "TestEmail" | mail -s yoursubject freemail@yahoo.com**

Control your freemail@yahoo.com. Control also your spam folder if you can not find the mail. Postfix should have sent the email. 

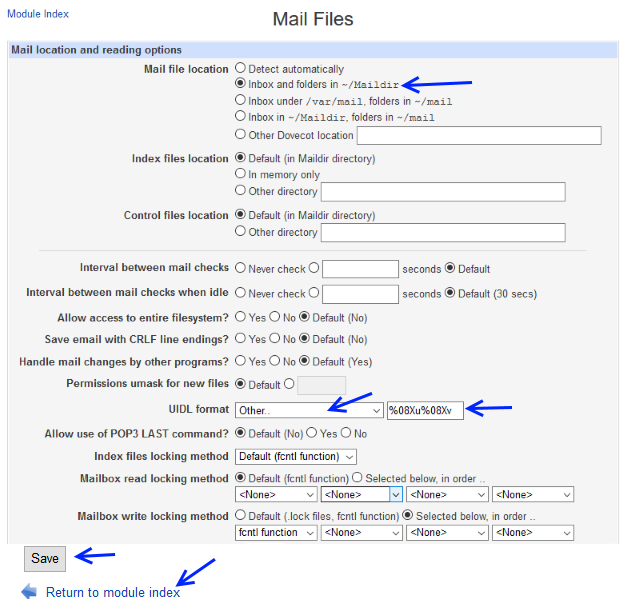
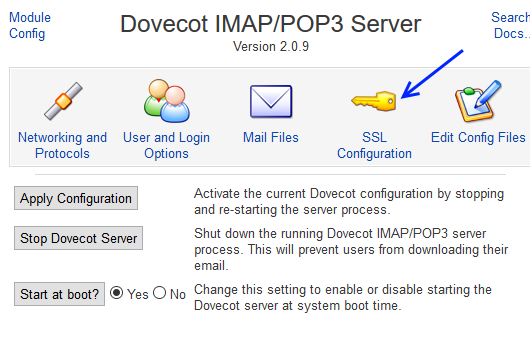
Configure Dovecot

Till now our web server is capable of sending messages using Postfix.   
Let's see now how we can receive emails with the help of dovecot.   
Navigate to Servers > Dovecot IMAP/POP3 Server Now click over the Networking and Protocols icon.  
   
  
Under "Dovecot networking and mail protocol options" at the "Networking and Protocols" page do like so: 

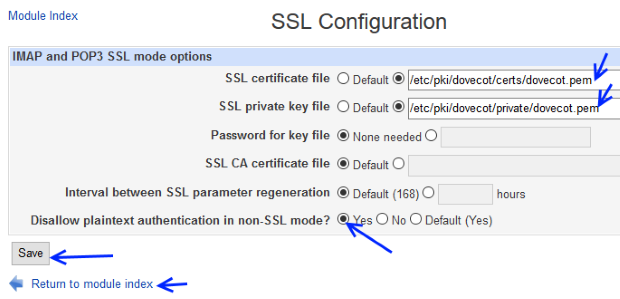
In the Serve mail protocols, select **IMAP**.  
Leave the rest at the defaults settings.

   
  
Click the "Save" button.   
Now hit over the "Return to module index" link   
Click over the "Mail Files" icon.  
   
  
At "Mail Files" page do like this : 

Mail file location : Inbox and folders in **~/Maildir**  
Set UIDL format to **Other**, and enter : **%08Xu%08Xv** in the text field.   
Left all other settings as is.

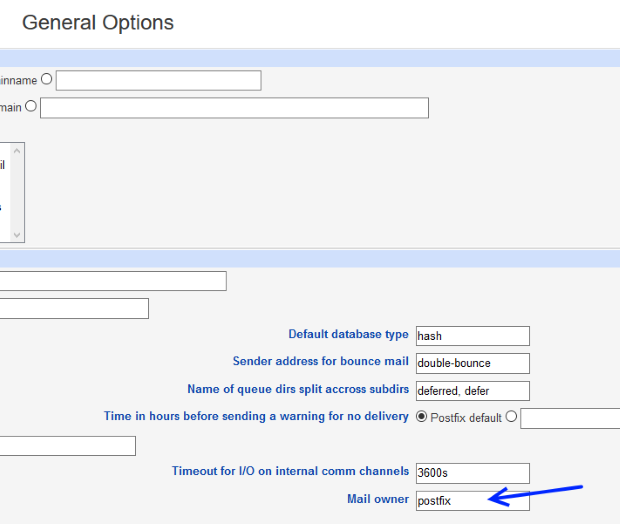
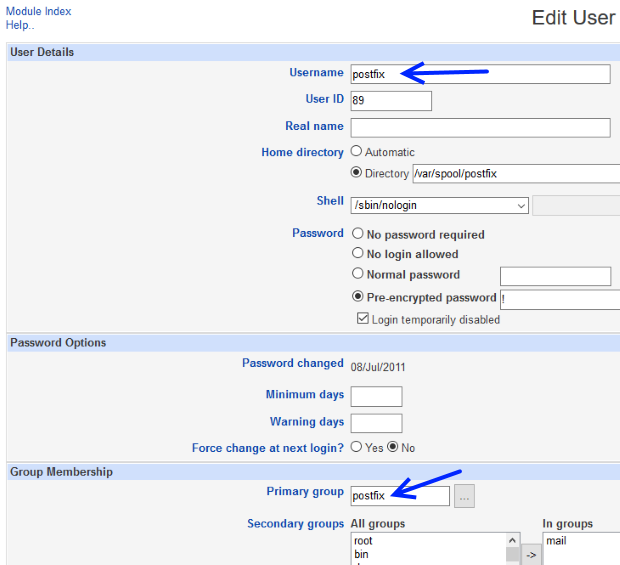
Click the "Save" files.  
Now hit over the "Return to module index" link   
  
   
  
Click over the "SSL Configuration" icon.   
   
  
At "SSL Configuration" page, under "IMAP and POP3 SSL mode options" do like this : 

Copy at notepad the SSL certificate file, ex : **/etc/pki/dovecot/certs/dovecot.pem**  
Copy at notepad the SSL private key file, ex: **/etc/pki/dovecot/private/dovecot.pem**  
Set Disallow plaintext authentication in non-SSL mode? to **Yes**.

Click the "Save" button.   
Now hit over the "Return to module index" link   
  
   
Click the "Apply Configuration" button.

Simple Authentication and Security Layer (SASL) is a technology for authentication and data security in Internet protocols. We will use SASL in order to authenticate Postfix. 

Setup a SASL authentication

We will use a combination of Postfix and Dovecot to set up SASL authentication for your SMTP server.   
We will set up a TLS encryption for SMTP connections.  
Using Webmin navigate to Servers > Postfix Mail Server and click on the "General Options" icon.   
Make a note of the "Mail owner" value, this is the Postfix user name (should be : **postfix**).   
   
  
Now go to System > Users and Groups, and check the primary group of this user (should be : **postfix**).   


Time to setup a secure SMTP relay for any email user.   
Go to Servers > Postfix Mail Server and click over the "SMTP Authentication And Encryption" icon   
Fill the "SMTP Authentication And Encryption" page like this : 

Set Require SASL SMTP authentication? to **Yes**.   
Set Disallow SASL authentication over insecure connections? to **Yes**.   
Set Handle non-compliant SMTP clients? to **Yes**.   
Under SMTP security options, **check** the box labeled **Reject anonymous logins**.   
Under "SMTP relaying restrictions", **check** the boxes :  
 **Allow connections from same network**   
 **Allow authenticated clients**   
 **Reject email to other domains**   
Set Enable TLS encryption? to **If requested by client**.  
You should use the same SSL certificate that the Dovecot server uses.   
So in our case we have to use :   
"TLS certificate file": **/etc/pki/dovecot/certs/dovecot.pem**  
"TLS private key file": **/etc/pki/dovecot/private/dovecot.pem**  
"TLS certificate authority file" : **None**  
Use SASL SMTP authentication? **No**

   
  
Click "Save and Apply" button.

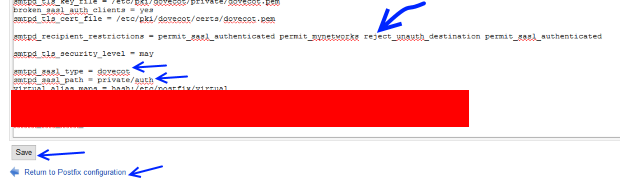
Postfix edit config files

Go to Servers > Postfix Mail Server and click over the "Edit Config Files" icon.  
Select **main.cf** from the "Edit config file" dropdown box.   
Click the "Edit" button.   
Scroll down to the end of the configuration file, and add the following settings: 

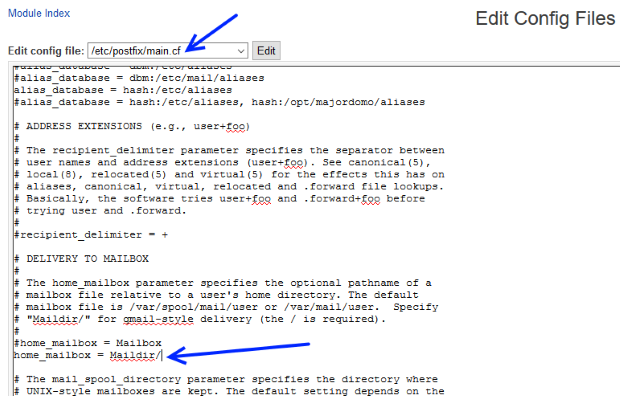
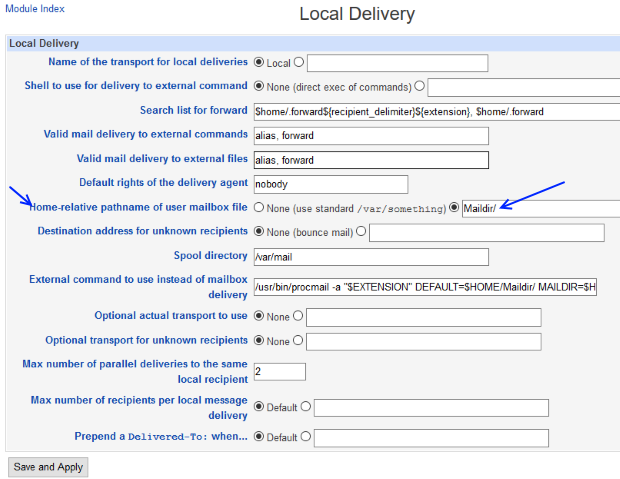
**smtpd\_sasl\_type = dovecot**  
**smtpd\_sasl\_path = private/auth**

Also make sure you have exactly this line into your **main.cf** file : 

**smtpd\_recipient\_restrictions = permit\_sasl\_authenticated, permit\_mynetworks, reject\_unauth\_destination permit\_sasl\_authenticated**

   
  
Finally also at the same file (at the middle of the file this time) uncomment the line : 

**home\_mailbox = Maildir/**

Click the "Save" button.   
   
  
Notice that for the last setting we could have done it by navigating at Server > Postfix Mail Server, and by clicking at "Local delivery" icon and by setting **Maildir/** at the voice "Home-relative pathname of user mailbox file".   
 

Dovecot edit config files

Navigate to Servers > Dovecot IMAP/POP3 Server and click over the "Edit Config Files" icon.   
Select **/etc/dovecot/conf.d/10-master.conf** from the "Edit config file" dropdown.   
Click the "Edit" button.  
Find the configuration section for the auth service, and uncomment lines related to the socket. Specify the username and group name of your Postfix user.   
In our case is user=postfix, group = postfix.  
The section should look something like the following code when finished: 

service auth

{

...

# Postfix smtp-auth

unix\_listener /var/spool/postfix/private/auth

{

mode = 0660

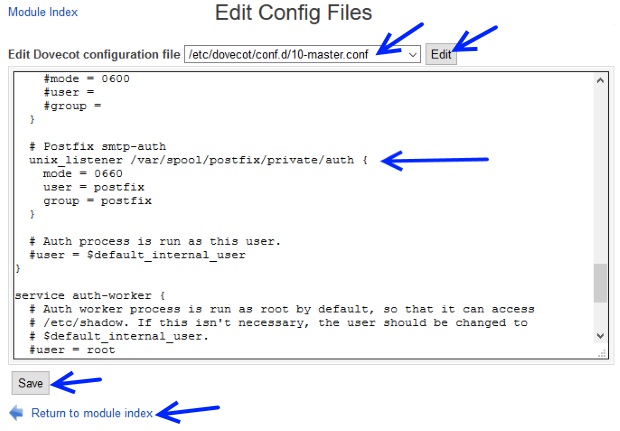
user = postfix

group = postfix

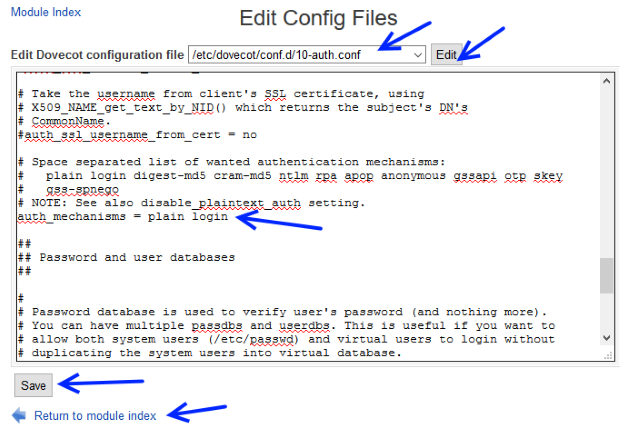
}

...

}

Click "Save"   
   
  
Now go to file : **/etc/dovecot/conf.d/10-auth.conf** and hit the "Edit" button.   
Find and change auth\_mechanisms to : 

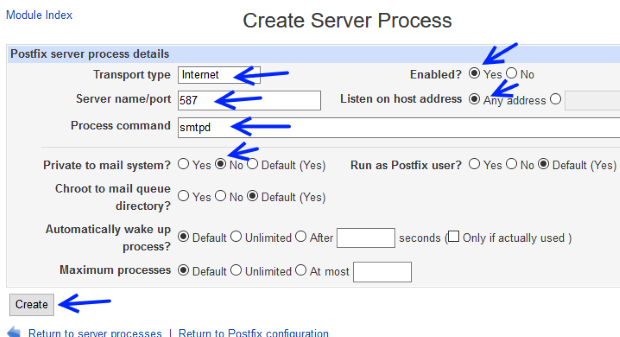
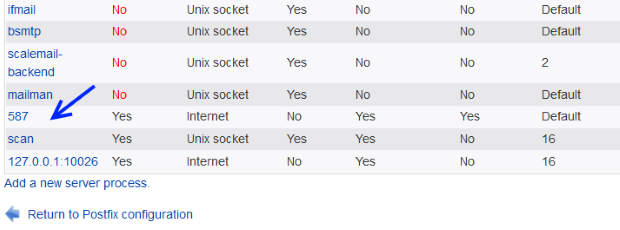
**auth\_mechanisms = plain login**

Click "Save".  
   
  
Click the "Stop Dovecot Server" button and then the "Start Dovecot Server" button to restart the dovecot daemon.

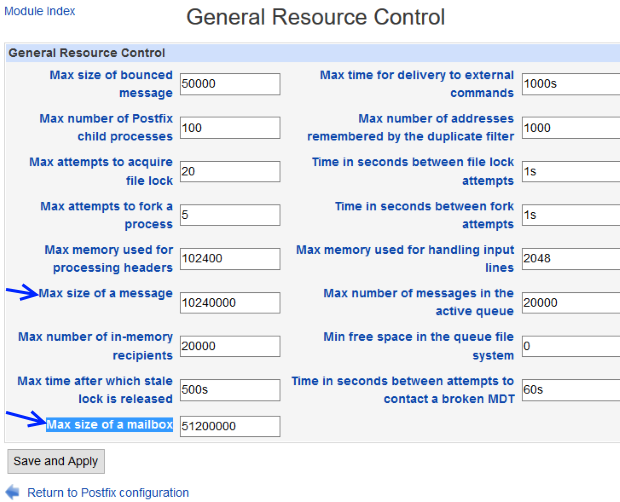
Set Postfix to listen at Port 587

We need to instruct Postfix to listen for SMTP connections on port 587.   
Navigate to Servers > Postfix Mail Server and click at the "Server Processes" icon.   
Click the "Add a new server process" link.   
In the "Create Server Process" form fill like this : 

Set "Transport type" to **Internet**.   
Set Server name/port" to **587**.  
Set "Process command" to **smtpd**.  
Set "Enabled?" to **Yes**.  
Set "Listen on host address" to **Any address**.  
Set "Private to mail system?" to **No**.

   
  
Click the "Create" button.  
  
At the "Server Processes" list you should have a new process with name 587 like the picture below.   
   
  
Navigate to Servers > Postfix Mail Server.  
Click "Stop Postfix" and then "Start Postfix" to restart the service. 

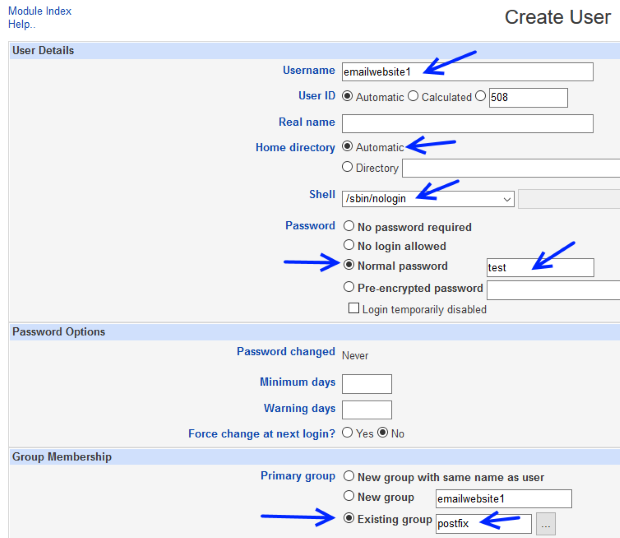
Configure Email boxes

Navigate at Servers > Postfix Mail Server.   
By clicking over "General Resource Control" icon you can modify how big your email inboxes are and some other important parameters for your email accounts.   
 Two important parameters to take note are:  
**Max size of a message**: This option limits the size in bytes of a message that will be delivered, including the message envelope information.   
**Max size of a mailbox**: The maximum size of an mailbox in bytes.   
The default values are OK for start but you can modify them at your needs.   


Setting up email users

Let's say we want to create two email accounts called: **email@website1.com**,   
**email@website2.com**   
Go to System > Users and Groups and click the "Create a new user" link. 

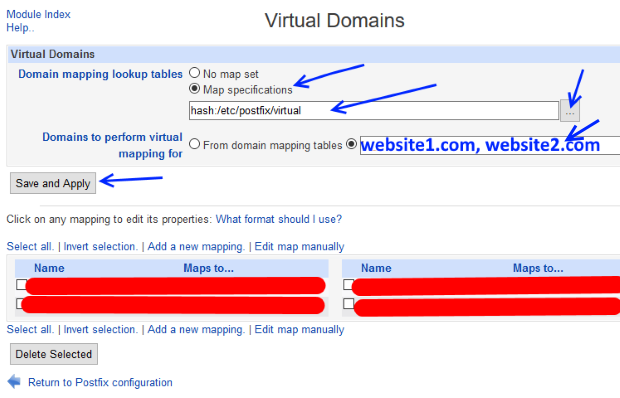
Give a Username ex : **emailwebsite1**  
Home directory: **Automatic**  
Shell: **sbin/nologin**  
Password: **Normal password**. Give a password for this user.  
Primary group: Existing group : **postfix**

   
  
Click the "Create" button.   
Do the same for the user **emailwebsite2**   
  
**Notice** : Generally you do not need any **aliases** for the **email@website1.com** since website1.com is the main mail server.   
So if you create the user "email" this will work out of the box for the email@website1.com.   
If in "Postfix Mail Server" > "Mail Aliases" there is an "email" alias you can delete it.   
  
**Virtual domains** can be used for local or non-local addresses, while aliases can only be used for local address.   
Since the base email domain is **website1.com**, we have to use virtual domains and not aliases for the **website2** domain and so on.   
  
In our example we could have done :   
Email: email@website1.com User: email -> No virtual domain is needed   
Email: email@website2.com User: email2 -> Virtual domain is needed   
  
But since the account "email" is not self explanatory i suggest doing something like this :   
Email: email@website1.com User: emailwebsite1 -> Virtual domain is needed (we could also have used an alias).   
Email: email@website2.com User: emailwebsite2 -> Virtual domain is needed. 

Setting up Virtual Domains on Postfix

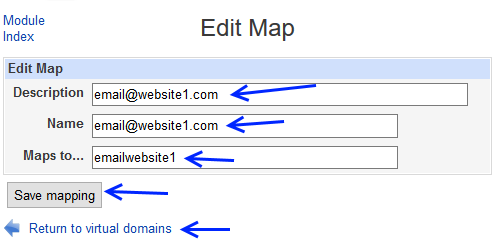
As we have seen in our example we need to make two virtual domains for our two email accounts. Go to Servers > Postfix Mail Server and click over "Virtual Domains" icon.   
Fill the "Virtual Domains" form like this : 

Domain mapping lookup tables : **Map specifications**   
Hit the [...] button and at the pop up window.  
Select Mapping file **/etc/postfix/virtual**   
Hit the "Save" button.   
You should have : **hash:/etc/postfix/virtual**   
Domains to perform virtual mapping for: **website1.com, website2.com**

   
  
Press "Save and apply" button.

Now again go at Servers > Postfix Mail Server and click over "Virtual Domains" icon.   
Click the "Add a new mapping" link.   
Fill the "Edit Map" form like this : 

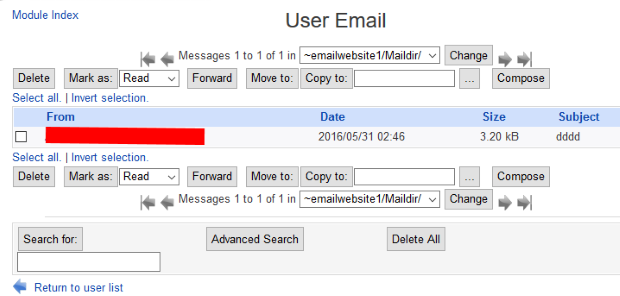
Description : **email@website1.com**  
Name : **email@website1.com**  
Maps to... : **emailwebsite1** (user)

   
  
Click the "Save mapping" button.   
Repeat for the second account **email@website2.com**   
  
Click the "Add a new mapping" link. 

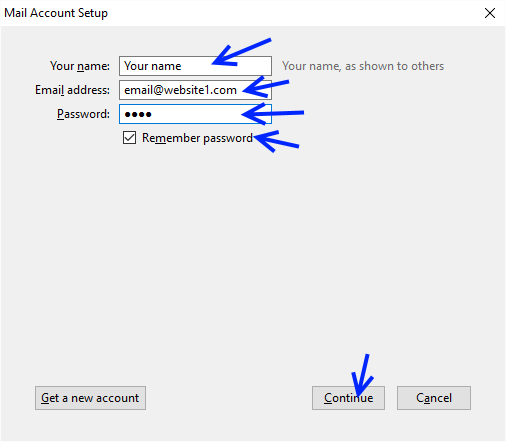
Description : **email@website2.com**   
Name : **email@website2.com**   
Maps to... : **emailwebsite2** (user)

Click the "Save mapping" button.   
  
Finally **stop and then start postfix**  
and **stop and then start dovecot**.   
  
Our email system is set and is ready to use. 

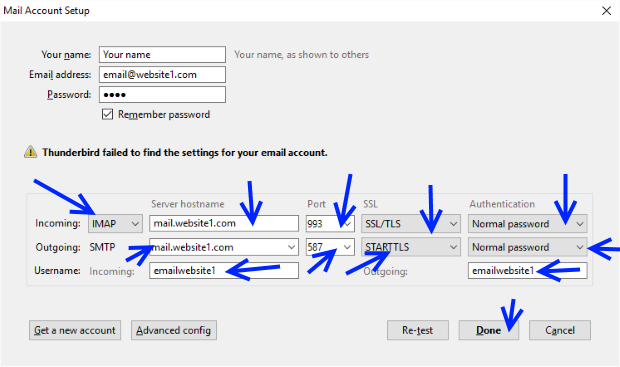
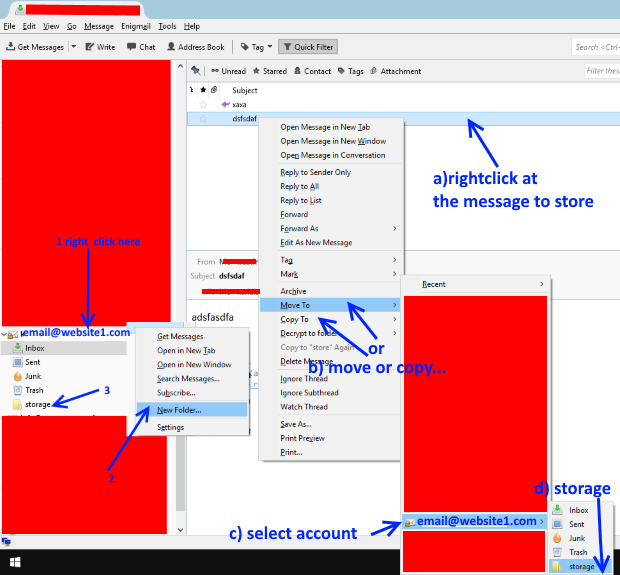
Sending and Receiving emails

Log into an external email account ex: freemail@yahoo.com Send an email at your newly created account **email@website1.com**   
You can now check your mail box using Webmin.   
Navigate to Servers > Read User Mail.  
Click over the **emailwebsite1** user.  
   
  
You should have received a new email like the image below :   
   
  
From the same interface you can also sent emails.   
  
Since we have set up the IMAPS protocol now we are ready to configure an email client in order to receive and send our emails from **email@website1.com**. I will cover only Thunderbird as client the procedure is similar into any email client.   
Run Thunderbird and click over File > New > Existing Mail Account. 

Your name: **Your name**   
Email address: **email@website1.com**   
Password: **password of the user emailwebsite1**   
Remember password : **checked**

   
  
Click the "Continue" button.   
Fill the Mail Account Setup form like this : 

Incoming: **IMAP** Server hostname: **mail.website1.com** (use mail.website2.com for the email@website2.com)   
Port: **993**   
SSL: **SSL/TLS**   
Authentication method: **Normal password**  
Username Incoming: **emailwebsite1**   
  
Outgoing: **SMTP**  
Server hostname: **mail.website1.com**   
Port: **587**   
SSL: **STARTTLS**   
Authentication method: **Normal password**  
Username Outgoing: **emailwebsite1**

   
  
Now you can receive and send emails using Thunderbird.   
As we have alredy said, at the IMAP protocol, all the emails are stored in the server so we can access with different devices at our email account. The only downside is that if our server does not host any emails we will loose them from all of our devices.   
In order to prevent this i suggest creating a folder "storage" into Thunderbird. (steps 1-3 at the image below.)  
Now all the important Inboxed emails can be moved at the "storage" folder. (Steps a-d at the image below.)  
Thunderbird will synchronize (and delete in case of server corruption) only the emails located at the Inbox folder.   


In the next chapter we will discuss how we can [process](http://www.trustfm.net/ebooks/DedicatedServer.php?page=EmailProcess) our received emails.   
We are going to use SpamAssasun as spam filtering.