

Setting up a VPS Server

--For beginners!!

(This document is optimized for VPSLink Service, but can apply to some other services as well)

By Ricky Bryce – Irving, Illinois

Note: There are many ways to register a domain name, and configure a server, and there are many services that allow you to do this. This document will express my personally preferred methods, and can act as guidelines for those of you wishing to configure your own server.

Disclaimer: By continuing to read this document, you agree to hold no one liable who writes, publishes, or modifies this document in any way (even negligence) Although I've taken steps for this document to be accurate, it is YOUR responsibility to verify any information before using this document. This document could be out of date due to improvements and changes made to websites, and to the Linux Operating System. Security is also YOUR responsibility. Do not read this document if you do not agree to these terms. This document is for general guidelines only.

Introduction: This document is written to help you set up a Linux server using VPS Link. This document will show you how to register your domain name if you don't already have one, how to point it to your VPS IP Address, how to install your Operating System on the VPS, and how to configure your server. This document will be written in modules, so you will need to access the main document at LearnAutomation.com for an index of all modules.

What is a virtual private server (VPS)? Many virtual servers can run on a single hardware server, each of them acting as an individual 'server' within the hardware server. This means you are your own administrator, and have access and control of all files on your virtual machine almost completely as if you would have with a standard dedicated machine. The advantages are that a virtual server costs much less than a dedicated server, and are generally more secure than shared hosting on a single server with a single operating system. The disadvantages are that you are sharing some resources, such as the processor time with other users on the system. Typically, an individual starting out would use a very small amount of resources anyway, so a VPS might be a great choice.

What would this cost me? This depends on which server you chose. The services at VPS Link are typically around \$15/month for a Link 2 server if paid yearly. You will also have the cost of your domain name, which is usually around \$10 a year with services such as godaddy.com. This document is actually written by using a Link 1 server, but Link 2 is recommended.

Managed vs. Unmanaged: On a managed server, software is used to assist you in administration. This software usually requires a licensing fee. This document will show you how to set up an unmanaged server, and you will be doing the administration yourself without purchasing a proprietary software license, or installing software that takes up your drive space.

Table of Contents

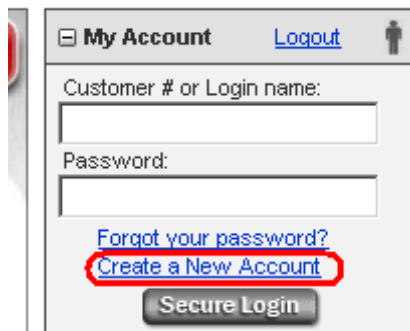
Registering your Domain.....	4
Register your VPS Account.....	5
Install the Operating System.....	6
Configure DNS.....	7
Log into Your Server.....	12
Setting Your Host Name.....	14
Adding Users.....	16
Install Packages/Updates.....	17
Apache (WebServer).....	18
Webmin (Web Administration).....	25
MySQL (Database Server).....	32
VSFTP (FTP Server).....	45
Postfix (Mail Server).....	48
SquirrelMail (Webmail).....	62
IPTables (Firewall Configuration).....	65
Configure Services (for startup).....	69
EchoLink Proxy (for ham radio).....	72

Registering your Domain

Before we get the VPS set up, let's decide what domain name you are going to use. Examples of domain names are “myfirstandlastname.com” or “mylastname.com”. Try to pick a domain name that is easy for people to remember. It's possible you might be using this domain name for your own email as well “me@mylastname.com”

Now, that you have decided what name you wish to register, let's see if that domain name is available. The service I prefer is godaddy.com, but there are many others. Depending on the type of domain name you wish to register, the cost will probably be around \$10/year.

- 1) Let's get started. First, go to godaddy.com, and set up an account (As I said, you can use any registrar you wish, but this document is based on my personal preferences, to keep things simple). Register your preferred domain name. If your preferred name is already taken, you can keep trying until you find a name that is available. When you register the domain, you can skip all the extra features they try to sell you (unless you see any that catch your eye) At some point during the registration process you may be asked for DNS servers, and should have the option to use the parked name servers for now. We will need to come back later and adjust the DNS information.



2)

Write down the password you used to log into godaddy.com with!! We will be using several passwords throughout this document, so you will want to keep track of them!

Username _____

Password _____

Register your VPS Account

There are many VPS providers. I believe Godaddy even has their own VPS servers, but my personal preference is VPS Link. I've been very happy with their service, and have tried many of them. You may be able to get by with a Link 1 VPS (using **Xen**) for around \$6 or \$7/month if paid by the year, but it could be slow, and the services you run may be limited, so if you can afford the Link 2 for around \$15/month (paid by the year) or a little more, that would be better for you. I strongly recommend you use **Xen** Technology instead of OpenVZ based on my experience. You will be given the option when you are signing up, and it might default to OpenVZ, so be careful.

If you follow the Link below (click the VPSLink icon), and enter the referral code, **MJDCDJ**, you will receive a 10% discount. I will also get some service credit for referring you, so I would appreciate you entering the code if asked. While setting up your account, you will be asked to enter the domain name you wish to associate this account with. This will be the domain you registered with godaddy on the previous step.

Note: VPSLink has instant provisioning, so you should get an email with your account information within a few minutes.

Click this icon to receive the 10% discount!



When you get to VPSLink, Just click "Order Now"



Write down the password you used to log into vpslink.com with!! We will be using several passwords throughout this document, so you will want to keep track of them!

Email (username)_____

Password_____

Install the Operating System

Next, you must choose an operating system to install. This example will use CentOS 5. That's "Community Enterprise Operating System (version 5)" This is a very stable operating system. Again, you can choose another distribution, but in this document, I'm just giving examples of my own preferences to get you started. If you are unfamiliar with Linux, and choose a different distribution, you could get lost very quickly while trying to follow this document!

Go to cp.vpslink.com, and enter the username and password you gave when you signed up for the VPSLink service.

Now, you must install the OS



[Install OS](#)

Choose your Operating system, and submit your choice. Here we are choosing Centos-5-i386-LAMP. This package will consume around 700MB of your virtual hard drive. **LAMP** = Linux, Apache, MySQL, and PHP, which is a common configuration for a web server.

Operating System to Install:

Be sure the installation was successful, and, go to your VPS Home.



[Home](#)

Write down the IP address for your Virtual Machine. We will need this to configure your DNS later on.

IP address: 66.249.9.205



[Manage Server](#)



[Manage Billing](#)



[Manage DNS](#)



[Get Support](#)



[Order New Server](#)



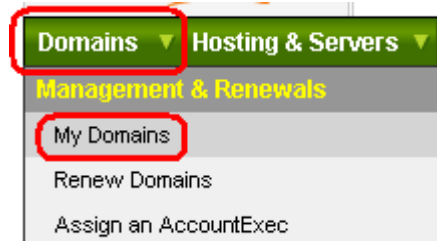
[Referral Program](#)

Configure DNS

Now that we know your server's IP address, we need to go back to godaddy.com to set up the DNS servers. Here, we will use the Total DNS Control method. If you don't have that option with your registrar, then you will need to use the DNS servers provided to you by your VPS provider (in this case VPSLink), then your VPS provider should have a way for you to configure the DNS.

Realize this procedure can change, but here is the basic concept of what I usually do.

- 1) Log into godaddy.com
- 2) Click Domains | My Domains



- 3) Click the Domain you wish to modify. (Click the text of the domain name)



- 4) Follow the “Nameservers” icon:



- 5) Choose “Hosting Nameservers”, and hit OK (*Note: You might have to hit OK a second time to confirm*)



- 6) You may need to wait a few minutes for the changes to take place.

7) Now, go to Total DNS Control

[Active \(Refresh Page\)](#)
[\(Add\)](#)
[\(Add\)](#)
[\(Add\)](#)
[Checked \(Change\)](#)
[/2000](#)
[/2010 \(Renew Now\)](#)
[\(Change\)](#)
[Enabled \(Change Status\)](#)
[Send by Email](#)

Name Servers: (Last Update 8/19/2008)
[NS51.DOMAINCONTROL.COM](#)
[NS52.DOMAINCONTROL.COM](#)

Forwarding:
[Domain is not forwarded.](#)

Total DNS: (Available)
 ARecord @ 208.83.233.76
 CNAME mail brycefamily.com
 CNAME www @
 CNAME ftp @
 MX @ brycefamily.com

[Total DNS Control and MX Records](#)

8) You can configure your DNS records similar to those shown here, but use your own domain, and your own IP address.

brycefamily.com

[Import/Export](#) [Check Zone Records](#) [Advanced Mode](#) [Return to List](#)

A (Host) [Add New A Record](#)

<input checked="" type="checkbox"/>	Host	Points To	TTL	Actions
<input type="checkbox"/>	@	66.249.9.205	1 Hour	Edit Delete

CNAMEs (Aliases) [Reset to Default Settings](#) [Add New CNAME Record](#)

<input checked="" type="checkbox"/>	Host	Points To	TTL	Actions
<input type="checkbox"/>	mail	brycefamily.com	1 Hour	Edit Delete
<input type="checkbox"/>	www	@	1 Hour	Edit Delete
<input type="checkbox"/>	ftp	@	1 Hour	Edit Delete

MX (Mail Exchange) [Reset to Default Settings](#) [Add New MX Record](#)

<input checked="" type="checkbox"/>	Priority	Host	Goes To	TTL	Actions
<input type="checkbox"/>	0	@	brycefamily.com	1 Hour	Edit Delete

TXT (Text) [Add New SPF Record](#) [Add New TXT Record](#)

SRV (Service) [Add New SRV Record](#)

AAAA (IPv6 Hosts) [Add New AAAA Record](#)

- 9) Note: The DNS change could take a couple days to complete now. Especially if you attempted to access your domain before this step was complete.
- 10) Now let's verify your domain is working (This is an optional step). Wait about 5 minutes, then go to the command prompt, and type "ping" then hit the space bar, and type your domain name, then press enter. You should be getting replies from your IP address. In this example I'm attempting to ping BryceFamily.com. You can see the IP address resolves properly, and I'm getting a response from the server.

```
C:\ F:\WINDOWS\system32\cmd.exe
F:\Documents and Settings\Ricky Bryce>ping brycefamily.com
Pinging brycefamily.com [66.249.9.205] with 32 bytes of data:
Reply from 66.249.9.205: bytes=32 time=98ms TTL=50
Reply from 66.249.9.205: bytes=32 time=107ms TTL=50
Reply from 66.249.9.205: bytes=32 time=103ms TTL=50
Reply from 66.249.9.205: bytes=32 time=97ms TTL=50
Ping statistics for 66.249.9.205:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 97ms, Maximum = 107ms, Average = 101ms
```

- 11) Now, we need to generate a reverse DNS request so your IP address can be resolved to your domain name. This is mainly for the purpose of the mail server, so the remote servers can verify you are who you say you are. If using VPSLink, go to cp.vpslink.com, and log in using the email and password you used when you registered with VPSLink.

VPSLink Control Panel Login

Email Address:

Password:

[Forgot your password?](#)

- 12) Click "Get Support"



13) Enter your VPS Username and password again.

Support Login

Please enter your email address and VPSLink

E-mail:
Password:

Login

[Forgot your password?](#)

14) Click “Reverse DNS Request”

VPSLink Support Center

Welcome to the support section of VPSLink.com. Here can requests.

- [Create a Support Ticket](#) - Submit a ticket if you encounter around the clock, every day of the year, to ensure your VPS
- [Reverse DNS Request](#) - Submit a Reverse DNS Request.
- [Ticket History](#) - View and respond to tickets.
- [Cancel Package\(s\)](#) - Cancel VPSLink service.

15) Enter the domain name, and submit query.

VPSLink 1 - 66.249.9.205 - ethernetsupport.com

66.249.9.205 - currently: None

new value:

Submit Query

- 16) You are done! You will get a message when they have made the DNS entry. If you made the request on a weekend, it will probably be Monday morning by the time your request is complete. If you made the request during their working hours, the request could be complete within a few hours.

Thank you for submitting your support request.

Your ticket number for this request is 610491. You

We will begin working on this request as soon as contact with you shortly.

- 17) Once you get a message that your reverse DNS entry is complete, you can go to a site that will check the reverse mapping, such as <http://remote.12dt.com/>. Enter your IP address, and see if the IP address now maps back to your domain.

Lookup an IP Address

Enter IP Address:

Log into Your Server

Now you are ready to log into your server to start configuring it for your own preferences. You can do this from the VPSLink Control Panel, but some find it much quicker to use a program called “PUTTY” in Windows. If your home computer is Linux or Macintosh based, you can simply use the terminal.

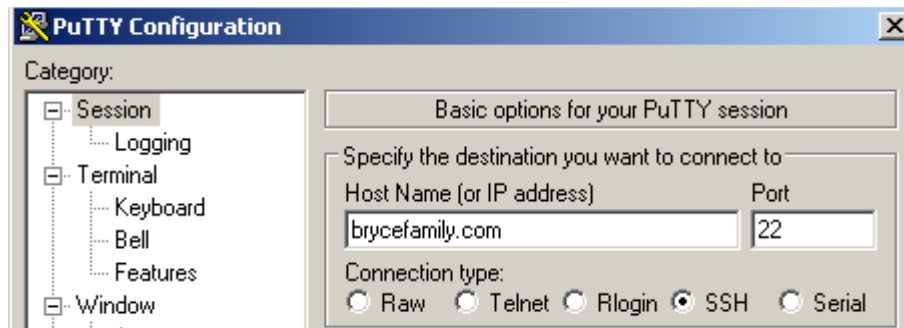
- 1) To download PUTTY, follow this link:

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

If the link is not clickable, you can simply paste it into the address bar of your web browser, or do a simple google search for putty. When downloading PUTTY, you can just place it on your desktop for easy access.



- 2) Now you can double click PUTTY, and enter your domain name as shown. If the DNS servers have not yet updated, you can still log into your server by entering the IP address instead. Hit “Open”

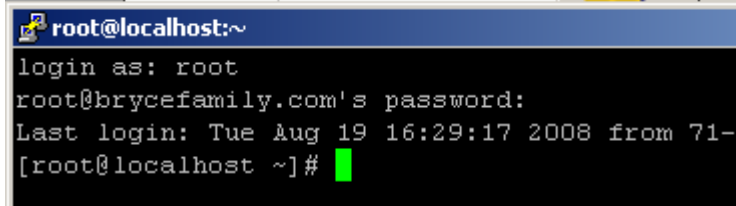


3) Now, you will get a warning. Just hit “Yes”



4) Now you can log in as “root” with your password. If you are using VPSLink, you can use the password you provided to them to log into your account. Other services might send you a password to use for the root account.

5) If your login was successful, you will see a # followed by your cursor as shown.



6) You are now ready to administer your VPS machine!

7) Write down the username and password you used to log on as root! This is your administrator account.

Username: root

Password _____

Setting Your Host Name

You registered your domain name, so now we will set this up on the server.
For this example, I'm going to assume you are already logged in as root using PUTTY.

- 1) From the root prompt, type: **cd /etc/sysconfig**

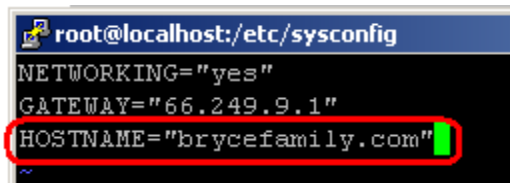
(CD = Change Directory) Then you need a space followed by the directory we are changing to (/etc/sysconfig)

- 2) Now type **vi network**

(VI is a text editor) Then we need a space followed by the file we want to edit (network)

- 3) Now, edit your host name. You can use your cursor keys to navigate to the location where you will be changing the host name, **then press the letter i to insert text.**

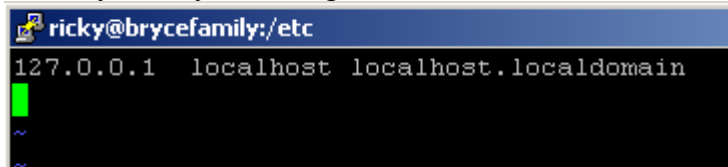
- 4) Now set your host name as shown (be sure to use your own host name though)



```
root@localhost:/etc/sysconfig
NETWORKING="yes"
GATEWAY="66.249.9.1"
HOSTNAME="brycefamily.com"
```

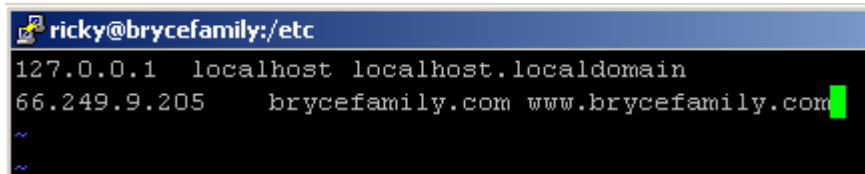
- 5) Now you must save your changes.
 1. **Press the escape key on your keyboard (upper left)** (This will escape the insert mode, and put you back into command mode.)
 2. **Now press :wq** colon, then w for write (save), and q for quit (exit).

- 6) Next, we need to edit the host file. Type **cd /etc/**
- 7) type **vi hosts**
- 8) tap “**i**” on your keyboard for insert mode.
- 9) Using your arrow keys, move to the very end (right side) of the last line in your hosts file.
- 10) Now press ENTER on your keyboard to go to the next line.



```
ricky@brycefamily:/etc
127.0.0.1 localhost localhost.localdomain
~
~
```

- 11) Now enter your IP address followed by a tab. Then your server alias, then tab, and server name. Use the example below to help you. Your file will be similar to this one. (Be sure to use your OWN IP Address address and domain names.)



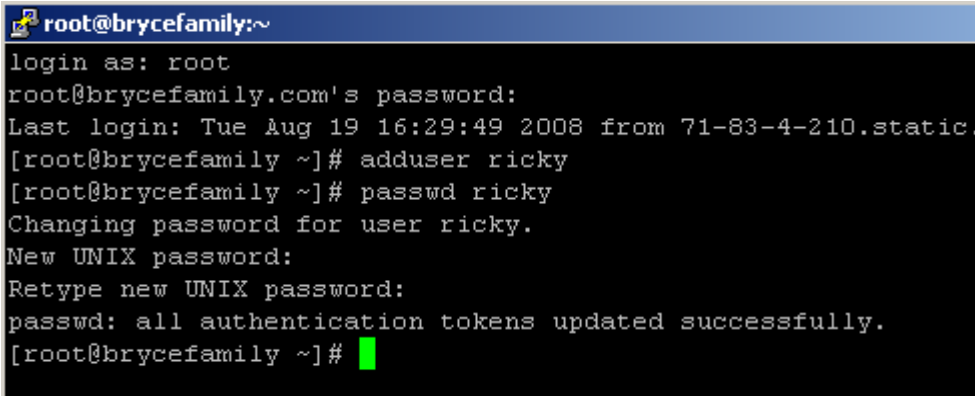
```
ricky@brycefamily:/etc
127.0.0.1 localhost localhost.localdomain
66.249.9.205 brycefamily.com www.brycefamily.com
~
~
```

- 12) Now we need to save the file:
 1. Press **ESC** on your keyboard to enter command mode.
 2. Now Press **:wq** (colon, then w for write, and q to quit.)
- 13) Now you are ready to reboot. Just type **reboot** at the command prompt, and close PUTTY.

Adding Users

Now we must add users who are going to utilize this server because we don't want to always be using the root account. You will want the users to have a strong password consisting of numbers and letters, upper case and lower case. For example, if you have a username of john, and the password is simply set to 'password', someone can easily gain access to that account (and probably eventually will!)

- 1) I'm going to assume you are logged in through PUTTY using the root account.
- 2) Adding users to your machine can be accomplished with the `adduser` command. Type the following (substitute 'username' for the name of the user you are adding).
Type **`adduser username`**
Later, if you want to delete a user, you can do this through the **`userdel`** command
- 3) Now, we need to set the password for the user you just added.
Type: **`passwd username`** (again where username is the name of the user you are changing the password for).
- 4) Now, you can type `exit`, and log back into your VPS using a username and password that you created for yourself. This is going to be more secure because you are not always running as the root user. Once you log into your standard user account, you can use the `su` command to become the super user (root) at any time



```
root@brycefamily:~  
login as: root  
root@brycefamily.com's password:  
Last login: Tue Aug 19 16:29:49 2008 from 71-83-4-210.static.  
[root@brycefamily ~]# adduser ricky  
[root@brycefamily ~]# passwd ricky  
Changing password for user ricky.  
New UNIX password:  
Retype new UNIX password:  
passwd: all authentication tokens updated successfully.  
[root@brycefamily ~]# █
```

- 5) Type `exit` to leave the terminal window.
- 6) Write down the username and password of the standard user you just created!!!

Username _____
Password _____

Install Packages/Updates

For this example, I will assume you are logged in as a **standard user** (a user you created with the adduser command earlier. We are going to be installing some packages, and getting some updates to your system using the “**yum**” command.

- 1) To update packages, we'll first become the root user, which is also considered the super user. Type **su** from your prompt to become the super user. You will be prompted for the root password.

```
ricky@brycefamily:/home/ricky
login as: ricky
ricky@brycefamily.com's password:
[ricky@brycefamily ~]$ su
Password:
[root@brycefamily ricky]#
```

- 2) Now, we'll update the machine. Type: **yum update**
- 3) Type '**exit**' once the update is complete to drop back to a standard user, then exit again will leave the terminal..

Apache (WebServer)

By default, Apache should work as-is. In fact, if you open your web browser right now, and type your domain name into the address bar, you should get a test page. Let's try this to make sure the Apache server is up and running. Since the CentOS package was already set up in a LAMP configuration, you should not have any trouble bringing up the test page. If you were to create an index page in the `/var/www/html` directory, your page would display instead of the test page.

We are wanting the ability, however for our server to host multiple web pages with multiple users, so we are going to have to configure virtual hosting in the Apache configuration file. Other features such as directory protection can be configured as well, but this lesson is just going to show how to get the server running for multiple websites.

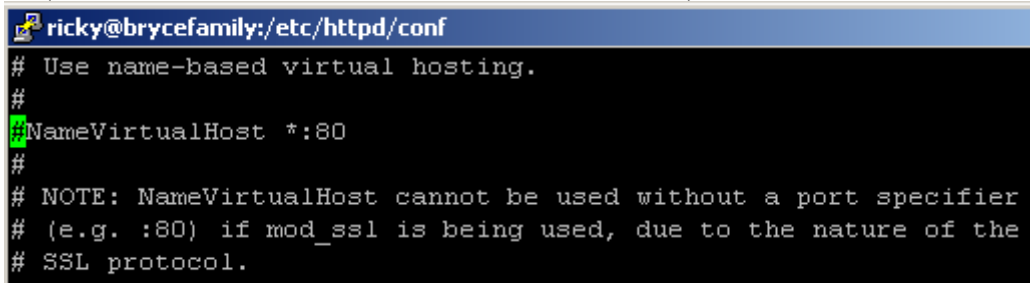
How many different web pages can Apache host? This depends on how large the page is, and the amount of dynamic content. A VPS with 10 Gigs of drive space and 128Megs of RAM (with 256M Swap) using the XEN hypervisor would probably be sufficient to host 25 personal web pages or more depending on how much traffic those pages get, how much drive space they use, and how much dynamic content they have.

Let's configure the server!

- 1) First let's log in to your server using a standard username.
- 2) Now, let's type **su** to become the root user. (press enter after each command)
- 3) Next, we need to enter the Apache configuration file. To do this, type **cd /etc/httpd/conf** then type **vi httpd.conf** (CD changes to the proper directory, and vi is your text editor, so you are editing the httpd.conf file.)

```
ricky@brycefamily:~/etc/httpd/conf
login as: ricky
ricky@brycefamily.com's password:
Last login: Wed Aug 20 10:17:51 2008 from 71-8
[ricky@brycefamily ~]$ su
Password:
[root@brycefamily ricky]# cd /etc/httpd/conf
[root@brycefamily conf]# vi httpd.conf
```

- 4) Hold **CTRL + F** until you reach the bottom (end) of the file. (Control and F at the same time)
- 5) Using your arrow keys, move your cursor up until you reach a line stating “#NameVirtualHost *:80” (This is about 20 lines above the bottom of the file)



```
ricky@brycefamily:/etc/httpd/conf
# Use name-based virtual hosting.
#
#NameVirtualHost *:80
#
# NOTE: NameVirtualHost cannot be used without a port specifier
# (e.g. :80) if mod_ssl is being used, due to the nature of the
# SSL protocol.
```

- 6) Tap “**i**” for insert mode, then press the **del** key on your keyboard to delete the # sign. The # sign makes a line of code inactive, so by deleting the # sign, we are activating the VirtualHost feature of Apache.
- 7) Now press the **esc** key on your keyboard to go back into command mode, and cursor down about 13 lines to #<VirtualHost *:80>
- 8) Count the number of lines from #<VirtualHost *:80> to #</VirtualHost> There should be around 7. This is the number of lines we are going to yank and paste in the next few steps.
- 9) Be sure you pressed **esc** in the above step, so you are in command mode, then type **7yy** This will yank 7 lines of code. If you counted a different number of lines from #<VirtualHost *:80> to #</VirtualHost>, then use that number instead of 7.
- 10) Now we are going to past our code we yanked at the bottom of the file. Cursor down (with your arrow keys) to the bottom of the file.
- 11) Tap “**i**” for insert mode.
- 12) Cursor to the right as far as you can go, then press enter a couple times.
- 13) Press **esc** to get back to command mode
- 14) Now hit “**p**” to paste the lines that you yanked earlier. Yanking the 7 lines and pasting them, we just duplicated the original 7 lines. This way, we will always still have the original 7 lines of code (which are currently inactive) while we modify a copy of those 7 lines.

- 15) Now you are starting to get familiar with the vi editor. Just hit “i” to insert text, and esc will return you to command mode where you can save your work, yank and paste, and many other commands that are available in vi. We are going to modify our copy of the code we just pasted. Using the example below, try to modify these 7 lines as shown, adjusting them for your own needs. Notice I am adding an extra line called ServerAlias. You may want to do the same as well.

```
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without
# a specific server name.
#
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot /www/docs/dummy-host.example.com
#   ServerName dummy-host.example.com
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

<VirtualHost *:80>
    ServerAdmin ricky@learnautomation.com
    DocumentRoot /home/ricky/public_html/
    ServerName www.brycefamily.com
    ServerAlias brycefamily.com
    ErrorLog logs/brycefamily.com-error_log
    CustomLog logs/brycefamily.com-access_log combined
</VirtualHost>
-- INSERT --
```

- 16) Now, we need to save our work. To do this press **esc** on your keyboard, then **:wq** (colon followed by w, for write and q, for quit).
- 17) *Note: If you are going to point other domain names to this server to host web pages, you would want to add the new user to your Linux system using the `adduser` and `passwd` commands as shown earlier in this document. Then you would simply yank these 8 lines, and adjust them to reflect the domain name, and directory location for the new user. The first virtual host is the default, so if a person enters the IP address of your server into the address bar of the web browser, the first virtual host should be the one displayed. Apache uses host headers to determine what directory to serve. This means it goes by the host name entered into the address bar of the web browser.*
- 18) *Now we need to create a directory for the user to store their page in. As you can see from the configuration file in this example, the location of the web page for `brycefamily.com` needs to be in `/home/ricky/public_html`. The reason each user needs their own `public_html` directory is because we are later going to configure the FTP server for that user, and each user will only have access to their own directory. We will create the folder, and web page in the next few steps.*

19) We already added some users in a previous lesson, so let's make sure each user we added has their own folder in the /home/directory. Type **cd /home** to change to the home directory.

20) Now type **ls** (list)

```
ricky@brycefamily:/home
login as: ricky
ricky@brycefamily.com's password:
Last login: Wed Aug 20 10:17:51 2008 from 71-8
[ricky@brycefamily ~]$ su
Password:
[root@brycefamily ricky]# cd /etc/httpd/conf
[root@brycefamily conf]# vi httpd.conf
[root@brycefamily conf]# cd /home/
[root@brycefamily home]# ls
davis2  ricky
[root@brycefamily home]#
```

21) Looks like we are good to go here. When the user “ricky” was added, a folder was automatically created in the home directory. We do need to make the folder “ricky” available for apache to access. To do this, type **chmod 711 ricky** (substitute the username you are using instead of “ricky”) To fully understand the chmod command, you can do a simple google search, but we are simply entering a binary code for 3 different types of users, and giving them read, write or execute permissions. For example, the first number is 7 which is 111 in binary, so you are giving the user himself read, write, and execute permissions. The second number is the group permissions 1, which is 001 in binary, so everyone in the group the user is in only has execute permissions. The last number again is 001, so others will only have execute permissions.

22) Now we need to go into his home directory, and add the public_html folder that apache is looking for. Type **cd ricky** to enter the user's directory. (again use your own username instead of “ricky”).

23) Now type **mkdir public_html** to make the directory the user will store his web page in.

- 24) Type **ls -al** (optional step) Notice the folder `public_html` is owned by `root`, and is set up for the `root` group. That's because we created the folder as `root`. We need to set this folder up so `ricky` owns this folder, and it's in `ricky`'s group.

```
[root@brycefamily home]# chmod 711 ricky
[root@brycefamily home]# cd ricky
[root@brycefamily ricky]# mkdir public_html
[root@brycefamily ricky]# ls -al
total 28
drwx--x--x 3 ricky ricky 4096 Aug 20 11:26 .
drwxr-xr-x 4 root  root  4096 Aug 19 17:38 ..
-rw----- 1 ricky ricky   6 Aug 20 10:19 .bash_history
-rw-r--r-- 1 ricky ricky  33 Aug 19 17:38 .bash_logout
-rw-r--r-- 1 ricky ricky 176 Aug 19 17:38 .bash_profile
-rw-r--r-- 1 ricky ricky 124 Aug 19 17:38 .bashrc
drwxr-xr-x 2 root  root  4096 Aug 20 11:26 public_html
[root@brycefamily ricky]#
```

- 25) Type **chown ricky public_html**

- 26) Type **chgrp ricky public_html**

- 27) Now, type **ls -al** You will see that “`ricky`” or your own user and group now owns the folder.

```
[root@brycefamily ricky]# ls -al
total 28
drwx--x--x 3 ricky ricky 4096 Aug 20 11:26 .
drwxr-xr-x 4 root  root  4096 Aug 19 17:38 ..
-rw----- 1 ricky ricky   6 Aug 20 10:19 .bash_history
-rw-r--r-- 1 ricky ricky  33 Aug 19 17:38 .bash_logout
-rw-r--r-- 1 ricky ricky 176 Aug 19 17:38 .bash_profile
-rw-r--r-- 1 ricky ricky 124 Aug 19 17:38 .bashrc
drwxr-xr-x 2 ricky ricky 4096 Aug 20 11:26 public_html
[root@brycefamily ricky]#
```

- 28) It looks like the permissions might be OK, but you can type **chmod 755 public_html** to be sure.

- 29) Now let's become the user “`ricky`” so we don't have that problem. This way any file we create will be owned by “`ricky`”.

30) Type **su ricky** You will notice the # sign on your cursor became a \$ indicating that you are no longer the privileged user.

```
root@brycefamily ricky]# su ricky
[ricky@brycefamily ~]$
```

31) Let's enter the public_html directory. Type **cd public_html**

32) Now we are ready to create the first web page, and save it... By default, apache looks for a file named index.html, or index.php to serve. We'll just create a simple index.html file. The vi editor can do this for us. Just type **vi index.html**

33) Tap “i” for insert mode, and create your page as shown:

```
ricky@brycefamily:~/public_html
<html>
  <head>
    <title>This is my Page!!</title>
  </head>
  <body>
    <b>Hello World!!</b>
  </body>
</html>
```

34) Hit **esc** on your keyboard, then type **:wq** to write the file and quit.

35) Now type **exit** to get back to the root user.

36) *Because we changed the httpd.conf file, we need to restart apache.*

37) Type **/etc/init.d/httpd restart**

Note: In this example, the host file was not set up properly, so apache displayed a warning that the domain name could not be determined reliably. If your host file is set up properly, apache should start and stop with out this warning. We configured the host file in the section “Setting the Host Name”.

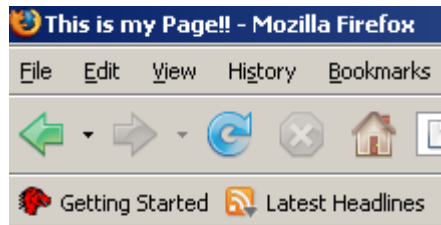
```
[root@brycefamily ricky]# su ricky
[ricky@brycefamily ~]$ cd public_html
[ricky@brycefamily public_html]$ vi index.html
[ricky@brycefamily public_html]$ exit
exit
[root@brycefamily ricky]# /etc/init.d/httpd restart
Stopping httpd:                                     [ OK ]
Starting httpd: httpd: Could not reliably determine the server's fully qualified
domain name, using brycefamily.com for ServerName
[ OK ]
[root@brycefamily ricky]#
```

38) I made a change to the host file, and now it is properly configured. This time, when I restart apache, I do not receive the warning.

```
[root@brycefamily ricky]# su ricky
[ricky@brycefamily ~]$ cd public_html
[ricky@brycefamily public_html]$ vi index.html
[ricky@brycefamily public_html]$ exit
exit
[root@brycefamily ricky]# /etc/init.d/httpd restart
Stopping httpd: [ OK ]
Starting httpd: httpd: Could not reliably determine the server's fully qual
domain name, using brycefamily.com for ServerName [ OK ]

[root@brycefamily ricky]# cd /etc
[root@brycefamily etc]# vi hosts
[root@brycefamily etc]# /etc/init.d/httpd restart
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
[root@brycefamily etc]#
```

39) Open your web browser, and try to load your page by typing your domain name in the address bar.

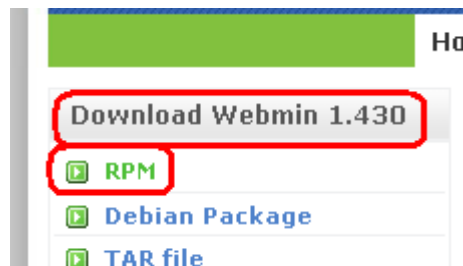


40) Congratulations! Your web server is running!

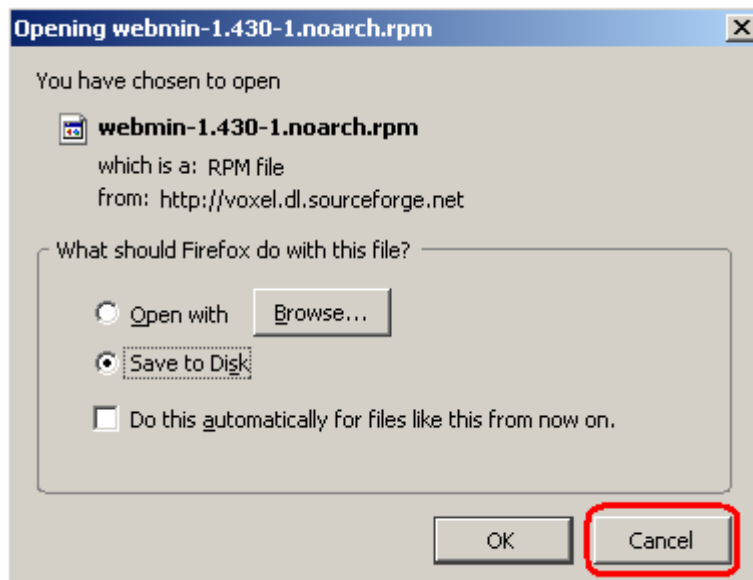
Webmin (Web Administration)

Now, we are going to provide ourselves with an easy way to administer the server graphically. This document will assume you are logged onto your server as a standard user using PUTTY.

- 1) Type **su** to become the super user.
- 2) Now, we need to copy a link from the latest version of webmin. We will get a link to the RPM file since this is a redhat based system. Go to webmin.com, and let's see what the latest version is.



- 3) It looks like the latest version today is 1.430. Click the link for the RPM file.
- 4) Click cancel, because we do not want to save the file to our own machine.



- 5) Right-Click the direct link, and **copy the link location**.

Open Source Software - You are downloading Webmin ...
Problems with the download please use this direct link or try another mirror.

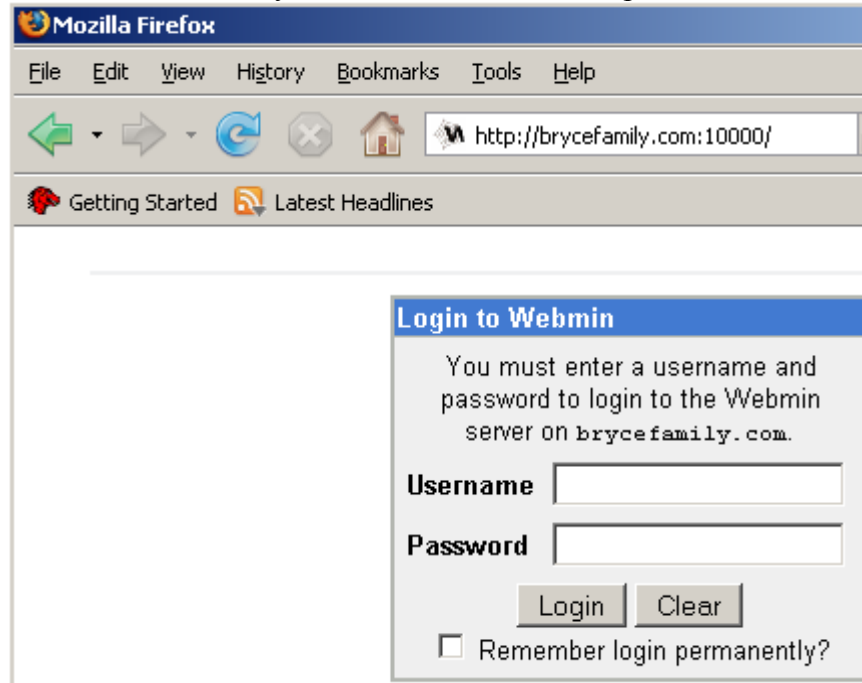
- 6) In PUTTY, type RPM -Uvh (then space) then right click and paste the link location.

```
[root@brycefamily etc]# rpm -Uvh http://internap.dl.sourceforge.net/sourceforge/webadmin/webmin-1.430-1.noarch.rpm
```

- 7) Press **ENTER**, and webmin should install. This could take a very long time (an half hour or so) on slower systems, but when webmin is finished installing, you will be returned to the command prompt.

```
[root@brycefamily etc]# rpm -Uvh http://internap.dl.sourceforge.net/sourceforge/webadmin/webmin-1.430-1.noarch.rpm
Retrieving http://internap.dl.sourceforge.net/sourceforge/webadmin/webmin-1.430-1.noarch.rpm
Preparing... ##### [100%]
Operating system is CentOS Linux
 1:webmin ##### [100%]
Webmin install complete. You can now login to http://brycefamily.com:10000/
as root with your root password.
[root@brycefamily etc]#
```

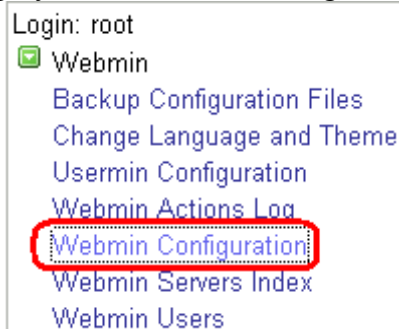
- 8) Now, let's test webmin. Open your web browser, and type <http://brycefamily.com:10000> into your address bar. That's port 10000 (ten thousand) You will substitute your own domain. Be sure to put a colon “:” between your domain name and the port #.



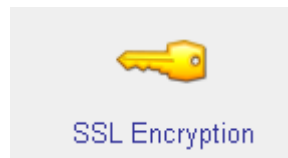
- 9) Enter root as your username, and enter your root password to log into webmin. If you have a small VPS machine, logging in could be slow.

10) Now, let's set up encryption for webmin, so we are not sending out the root password in plain text.

1. Under the Webmin Category, click Webmin Configuration



2. Now click SSL Encryption.



3. Download and install the Net::SSLLeay Pearl module.

[Module Index](#)

SSL E

The Net::SSLLeay perl module does not appear to be installed on your system. To install it, you can have Webmin **download and install** the required Net::SSLLeay Perl

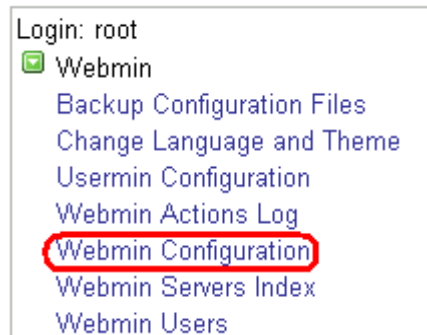
4. Verify the transaction was complete.

```
Transaction Summary
-----
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 297 k
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: perl-Net-SSLLeay                ##### [1/1]

Installed: perl-Net-SSLLeay.i386 0:1.32-1.el5.r
Complete!
```

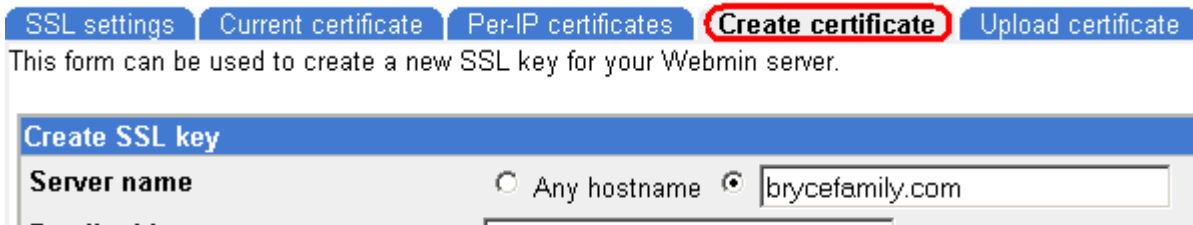
- Now, we need to set webmin to use the encryption we just installed, so go back to Webmin Configuration in the navigation tree on the left.



- Go back to SSL Encryption.



- Choose to Create a Certificate.



- Populate the fields on your form to create the SSL Key, then click “Create Now”

- The key should have been successfully created.

[Module Index](#)

Generate Key

Successfully generated the following SSL key.

- Return to Webmin Configuration

-----END CERTIFICATE-----

[Return to Webmin configuration](#)

11. Go back to SSL Encryption



12. Choose to enable SSL if available.

A dialog box titled "SSL support" with a blue header. It contains the following fields:

- "Enable SSL if available?" with radio buttons for "Yes" (selected) and "No". This section is highlighted with a red rectangle.
- "Private key file" with a text input field containing "/etc/webmin/miniserv.pem" and a browse button "...".
- "Certificate file" with radio buttons for "Same file as private key" (selected).

A "Save" button and a blue arrow pointing left with the text "Return to Webmin configuration".

13. Save your settings.

11) Now, you will be asked to accept the certificate into your web browser. **If your browser complains about the certificate, you may need to add an exception.** Look at your screen closely. There should be a way to continue anyway. If you are using IE, there may be a bar at the top of your browser window to click on. We are not going to worry about getting the certificate signed by a trusted authority for this lesson.

A browser warning dialog box with a yellow warning icon. The text reads:

Unable to verify the identity of brycefamily.com as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be brycefamily.com, possibly to obtain your confidential information.

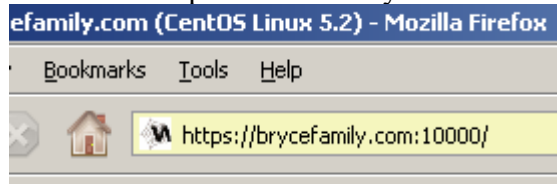
Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site brycefamily.com?

Examine Certificate...

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this Web site

12) Now, access your server by entering <https://brycefamily.com:10000> (substitute your own domain) Notice the letter 's' after http. This means you are accessing a secure site.

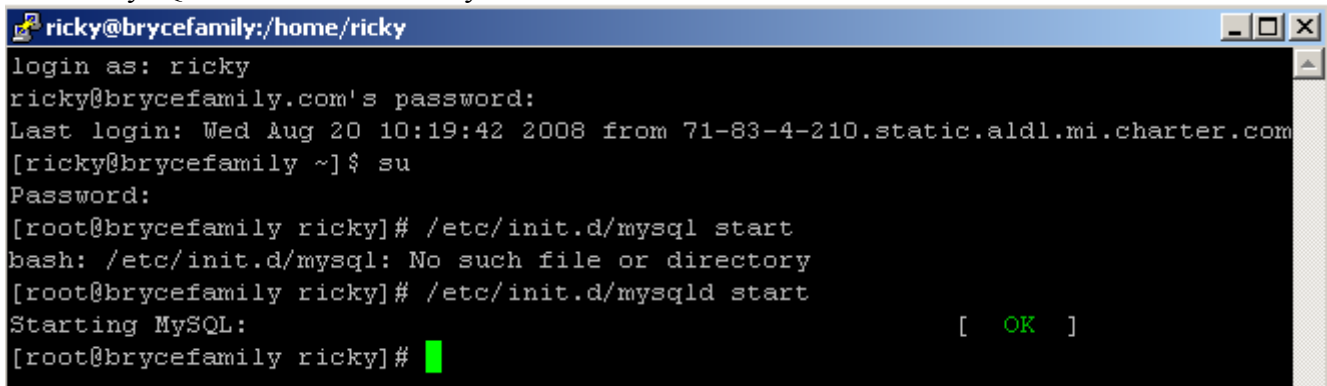


13) Webmin is now configured, and ready for the root user to utilize.

MySQL (Database Server)

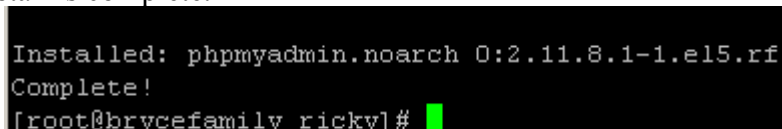
MySQL is a database server, and plays a major role in dynamic web pages, such as guestbooks and forums. This lesson will walk you through how to set up a MySQL Database for your user.

- 1) Before we do anything with MySQL, we need to log into your server using PUTTY, and set the root password for MySQL. This password does not have to be the same password as your Linux system account. I'm going to assume that you are logged in as a standard user.
- 2) Now, type **su** to access super user privileges.
- 3) Now, type **/etc/init.d/mysql start** to start mysql server. Notice the 'd' after mysql (daemon) Here you can see I typed the command incorrectly the first time. Later on, we'll configure MySQL to start automatically when the virtual machine boots.



```
ricky@brycefamily:/home/ricky
login as: ricky
ricky@brycefamily.com's password:
Last login: Wed Aug 20 10:19:42 2008 from 71-83-4-210.static.aldl.mi.charter.com
[ricky@brycefamily ~]$ su
Password:
[root@brycefamily ricky]# /etc/init.d/mysql start
bash: /etc/init.d/mysql: No such file or directory
[root@brycefamily ricky]# /etc/init.d/mysql start
Starting MySQL: [ OK ]
[root@brycefamily ricky]#
```

- 4) Now, type this command. **mysqladmin -u root password Gr8Us7** Obviously, you will substitute Gr8Us7 for the password you wish to use. In the future if you wish to change the root password, just use the same command, but type a -p after mysqladmin, and you will be prompted for the old password before the new password is active.
- 5) Now let's install phpmyadmin into the server, so users can access their databases. Just type **"yum install phpmyadmin"** at the command prompt for root.
- 6) You will be asked to verify it's OK to install the packages, then you should get a message stating the install is complete.



```
Installed: phpmyadmin.noarch 0:2.11.8.1-1.el5.rf
Complete!
[root@brycefamily ricky]#
```

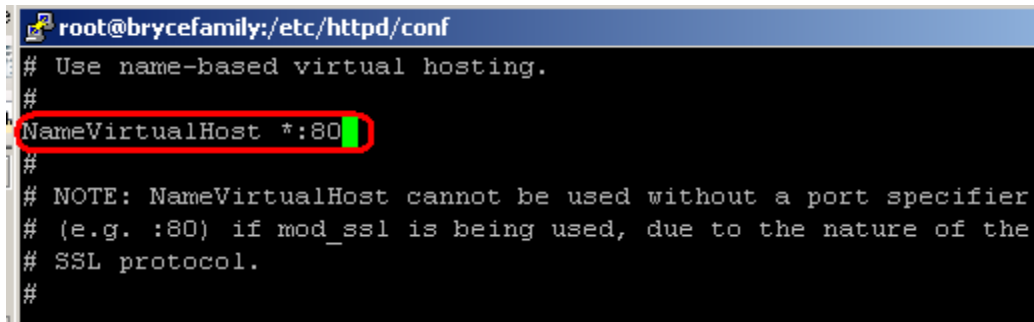

- 7) Next, we will need to set a directive in the apache configuration file to allow users to access the phpmyadmin program we just installed, so they have an easy way to administer their database. Type `cd /etc/httpd/conf/`

```
[root@brycefamily ~]# cd /etc/httpd/conf
```

- 8) type `vi httpd.conf` to edit the apache configuration file.

```
[root@brycefamily ~]# cd /etc/httpd/conf  
[root@brycefamily conf]# vi httpd.conf
```

- 9) Hold **Control + F** (control and F at the same time) until you reach the end of the file. This is where our custom configuration is located for virtual hosting.
- 10) Tap “i” for insert mode.
- 11) Use the up arrow key to move above our first virtual host entry, and the virtual host example we used when configuring the virtual hosts in the Apache lesson. You will place your cursor at the end of the line `NameVirtualHost *:80` as shown.



```
root@brycefamily:/etc/httpd/conf  
# Use name-based virtual hosting.  
#  
NameVirtualHost *:80  
#  
# NOTE: NameVirtualHost cannot be used without a port specifier  
# (e.g. :80) if mod_ssl is being used, due to the nature of the  
# SSL protocol.  
#
```

12) Press the enter key a couple times, and add the directory directive as shown.

```
#
# Use name-based virtual hosting.
#
NameVirtualHost *:80

# This directory entry is required to make phpmyadmin work.
<Directory /usr/share/phpmyadmin>
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>

#
# NOTE: NameVirtualHost cannot be used without a port specifier
# (e.g. :80) if mod_ssl is being used, due to the nature of the
# SSL protocol.
#
```

13) Press the escape key on your keyboard (**esc**) to return to command mode.

14) Type **:wq** (colon, then w for write, and q to quit)

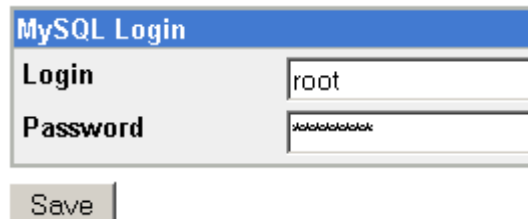
15) Restart apache by typing **/etc/init.d/httpd restart**

```
root@irvingil:/etc/httpd/conf
login as: root
root@irvingil.com's password:
Last login: Wed Aug 20 05:47:36 2008 from 71-83-4-210.static.ald1.mi
[root@irvingil ~]# cd /etc/httpd/conf
[root@irvingil conf]# vi httpd.conf
[root@irvingil conf]# /etc/init.d/httpd restart
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
[root@irvingil conf]#
```

16) Now, let's give our user a database they can access. To do this we can go to webmin, and under servers, click MySQL Database Server. Remember, we set up webmin earlier, and to access webmin, just go to https://brycefamily.com:10000 (substitute your own domain)



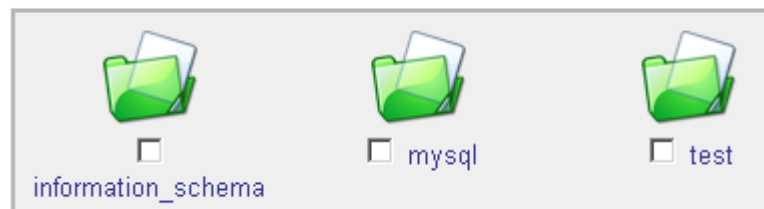
17) Now, login with the root username and password which you set up earlier in this lesson., and save your changes.



18) Create a new database.

MySQL Databases

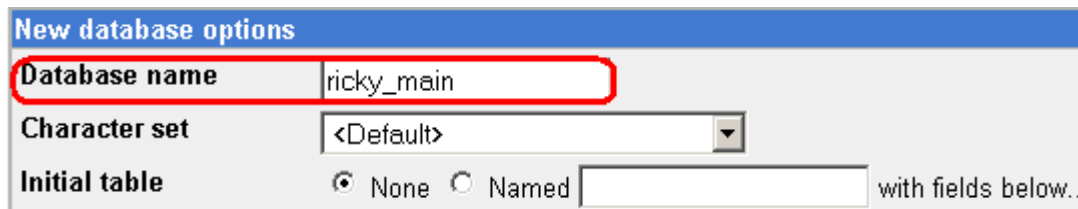
Select all. | Invert selection. | Create a new database.



Select all. | Invert selection. | Create a new database.

Drop Selected Databases

19) I'm going to create this database as ricky_main. This helps me to determine which databases belong to specific users, and also helps to group the databases together by username. We'll let the users create their own tables. Click "Create" once you have the database name in place.



New database options

Database name ricky_main

Character set <Default>

Initial table None Named with fields below..

20) Now, we'll have to relate the user "ricky" to this specific database. Under "Global Options", click "User Permissions"

Global Options



21) Create a new user.

Module Index
Help..

User F

Select all. | Invert selection. [Create new user.](#)

	User	Hosts	Encrypted password
<input type="checkbox"/>	root	localhost	209bedd7613997
<input type="checkbox"/>	root	127.0.0.1	

Select all. | Invert selection. | [Create new user.](#)

[Delete Selected](#)

22) Enter the username and password for the user, and I'm limiting the host to "localhost" with no other privileges. We will configure this user's privileges at the database level. Click "Create" to build the user.

MySQL user details

Username Anonymous user ricky

Password None Set to.. [password field]

Hosts Any localhost

Permissions

- Select table data
- Insert table data
- Update table data
- Delete table data
- Create tables
- Drop tables
- Reload grants
- Shutdown database
- Manage processes
- File operations

23) Verify the new user has been added.

Select all. | Invert selection. | Create new user.

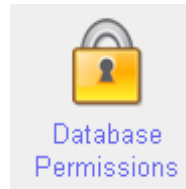
<input type="checkbox"/>	User	Hosts	Encrypted password
<input checked="" type="checkbox"/>	ricky	localhost	686c9af542f6cc62
<input type="checkbox"/>	root	localhost	209bedd7613997a0
<input type="checkbox"/>	root	127.0.0.1	

Select all. | Invert selection. | Create new user.

24) Return to the database list

[← Return to database list](#)

25) Now, let's go to "Database Permissions"



26) Now, we'll "Create New Database Permissions":

[Module Index](#) [Help..](#) **Database Perm**

Select all. | Invert selection. | **Create new database permissions.**

	Databases	User	Hosts	Permissions
<input type="checkbox"/>	test	Anonymous	Any	Select Insert Update Delete temp Lock Create View Show
<input type="checkbox"/>	test_%	Anonymous	Any	Select Insert Update Delete temp Lock Create View Show

Select all. | Invert selection. | [Create new database permissions.](#)

27) Now, we'll grant the user "ricky" all privileges to his database (ricky_main). To select all privileges, select the first item in the privilege list, then hold "shift" on your keyboard, and select the last item in the privilege list. Click "Create" to build the permission.

[Module Index](#)
[Help..](#)

Create Database Perr

Database permission options

Databases Any Selected ricky_main Mat

Username Anonymous user ricky

Hosts From host permissions Any localhost

Permissions

- Reference operations
- Manage indexes
- Alter tables
- Create temp tables
- Lock tables
- Create View
- Show View
- Create Routine
- Alter Routine
- Execute

Create

28) Verify the permission was created:

[Module Index](#)
[Help..](#)

Database Pe

Select all. | Invert selection. | Create new database permissions

	Databases	User	Hosts	Permissions
<input type="checkbox"/>	ricky_main	ricky	localhost	All

29) Now let's reboot the server just to ensure all changes are active. To reboot the server, just go to PUTTY (which is probably still running), and type **reboot**. You will need to be root to reboot the server.

```
[root@brycefamily conf]# reboot
Broadcast message from root (pts/0) (Thu Aug 21 14:56:15 2008):
The system is going down for reboot NOW!
[root@brycefamily conf]# █
```

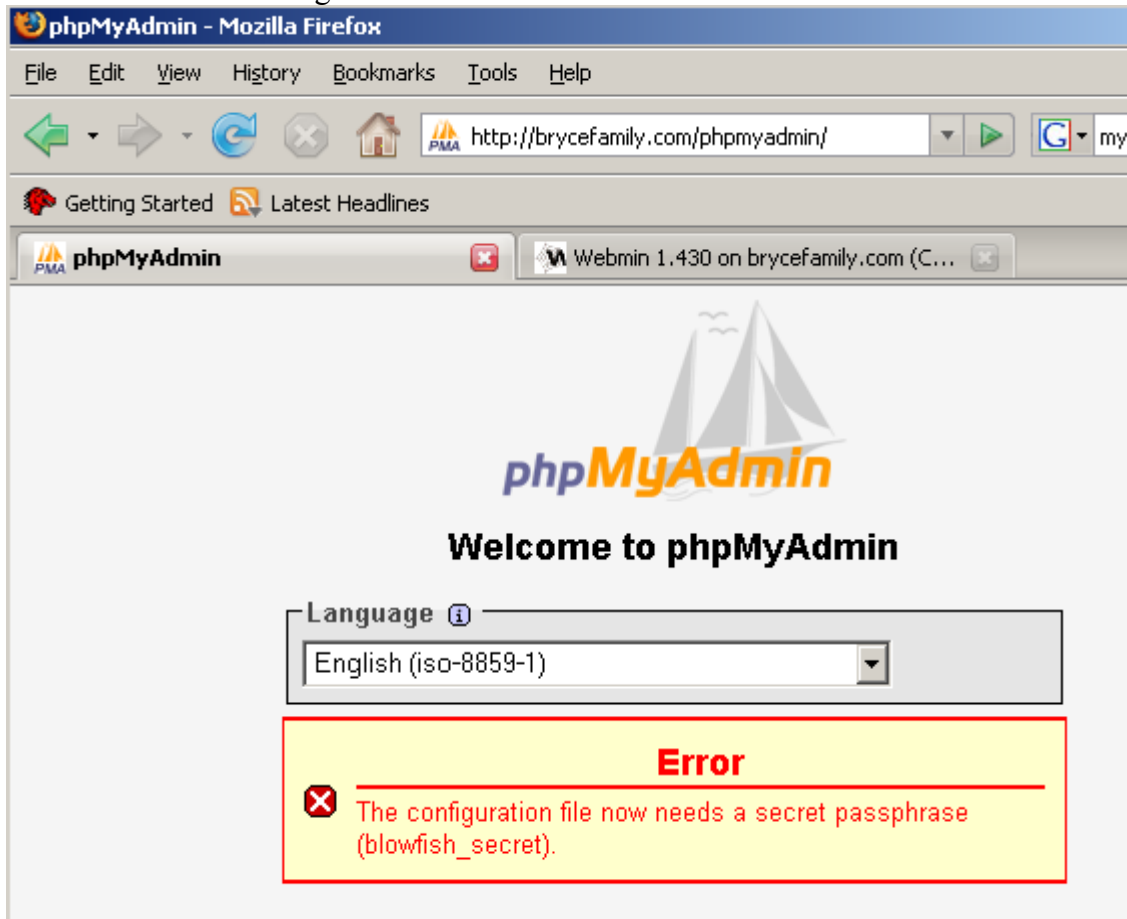
30) Using PUTTY, you need to log back into your server.

31) If you logged in a a standard user, type **su** to become the root user.

32) Type **/etc/init.d/mysql start** to start MySQL (we will set it to automatically start in a later lesson)

```
ricky@brycefamily:/home/ricky
login as: ricky
ricky@brycefamily.com's password:
Last login: Thu Aug 21 11:16:52 2008 from 71-83-4-210.static.ald1.mi.ch
[ricky@brycefamily ~]$ su
Password:
[root@brycefamily ricky]# /etc/init.d/mysql start
Starting MySQL: [ OK ]
[root@brycefamily ricky]# █
```


- 33) Now, go to your web browser, and enter <http://brycefamily.com/phpmyadmin> in the address bar. As you can see, we are getting close, but still not quite there yet. We'll take care of this error in the next step, but you should see something like what is shown in the image below. If not read the notice below the image.



Notice!! If you are forbidden from accessing the directory, the `/usr/share/phpmyadmin` line in the `<directory>` directive in the `httpd.conf` file is case sensitive. I noticed in CentOS 5, `phpmyadmin` is all lower case when installing with YUM, but Fedora was `phpMyAdmin`. To check this, log onto the server with root privileges in PUTTY. Type `cd /usr/share` Then type `ls` to list the contents of the directory. Make note exactly how the `phpmyadmin` directory is spelled (case sensitive), and ensure this is what you used in step 12 above. If you still have trouble, be sure `phpmyadmin` is installed (type `yum install phpmyadmin`) Also, be sure the `<directory>` directive is entered exactly as shown in step 12. You can also try to reboot the server if you still have issues.

34) Now, let's take care of this error we are getting. We need to enter a secret passphrase just for the purpose of encryption.

35) In putty (as root), type `cd /usr/share/phpmyadmin` If you get an error, try `cd /usr/share/phpMyAdmin` (if that is how your directory is cased)

36) Now, type `vi config.inc.php` (This will allow us to edit the config file for phpmyadmin)

37) type `/blowfish` (forward slash, then blowfish. This will search for the blowfish text)

38) Tap “i” to get to insert mode.

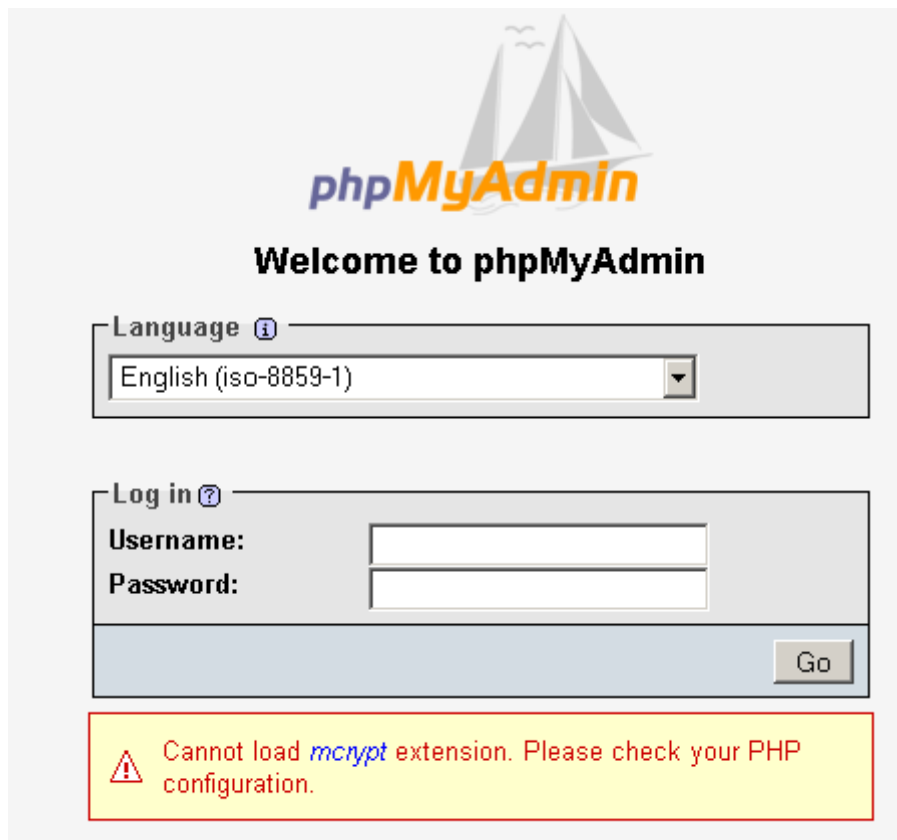
39) Cursor over between the two apostrophes, and enter a passphrase of your own. **(be sure the passphrase is between the two apostrophes!!!)**

```
/*
 * This is needed for cookie based authentication to encrypt password in
 * cookie
 */
$config['blowfish_secret'] = 'hola'; /* YOU MUST FILL IN THIS FOR COOKIE AUTH
```

40) Press `esc` on your keyboard to escape to command mode.

41) Now type `:wq` (colon, then w for write, and q for quit)

42) Now, I'm going to `brycefamily.com/phpadmin`, and I at least get a login screen, but I still get another error. We are taking this one step at a time. In the next step, we will resolve this error.



43) In PUTTY, type `yum install php-mcrypt` as the root user. You will be asked to confirm the installation. You will be informed when the installation is complete.

```
Transaction Test Succeeded
Running Transaction
  Installing: php-mcrypt #####
Installed: php-mcrypt.i386 0:5.1.6-15.el5.centos.1
Complete!
[root@brycefamily etc]# █
```

- 44) Now, I'm going to go back to <http://brycefamil.com/phpmyadmin>, and should get a login screen without errors (again, use your own domain)
- 45) .If so, login to phpmyadmin If you still have errors, you might try a google search to figure out how to correct them. You are using the password you gave the user when you assigned them database permissions.



phpMyAdmin

Welcome to phpMyAdmin

Language ⓘ

English (iso-8859-1)

Log in ⓘ

Username: ricky

Password: *

Go

- 46) The user can now create tables. Again, you are responsible for verifying security, but if you are the only user, and you are the administrator of all the web pages, you will have less to worry about!

VSFTP (FTP Server)

Now we'll configure the Very Secure File Transfer Protocol Server (VSFTP). VSFTP is already installed on your virtual CENTOS machine. We just have to configure it to be able to accept passive FTP on certain ports, and limit users to their own directory.

- 1) Log on to your server as a standard user.
- 2) Type **su** to gain root access. (You will be prompted for the root password)
- 3) Type **yum install vsftpd** to install the vsftpd server. You will be prompted to confirm the installation.
- 4) Type **cd /etc/vsftpd/** to enter the configuration directory for the server.
- 5) Type **vi vsftpd.conf** to edit the configuration file.
- 6) Type **/anonymous_enable** to locate code that enables anonymous users.
- 7) Hit **"i"** for insert mode within the vi editor
- 8) Cursor to the end of the line, and set the anonymous_enable directive to the value of NO as shown:

```
# READ THIS: This example
# Please read the vsftpd.c
# capabilities.
#
# Allow anonymous FTP? (Be
anonymous_enable=NO
#
# Uncomment this to allow
local_enable=YES
```

- 9) Hit **esc** on your keyboard.
- 10) Type **/connect_from_port_20**
- 11) Tap **"i"** for insert mode.
- 12) Using your mouse keys, go to the end of the line, then press **enter**.

- 13) Add the passive min and max port as shown. This sets up the random ports which are used for passive connections. (sixty-thousand to sixty-thousand five hundred)

```
dirmessage_enable=YES
#
# Activate logging of uploads/downloads
xferlog_enable=YES
#
# Make sure PORT transfer connects from
connect_from_port_20=YES
pasv_min_port=60000
pasv_max_port=60500
#
# If you want, you can arrange for
# a different user. Note! Using "
```

- 14) Next, we are going to jail users to the own home directory using a chroot directive, so press **esc** on your keyboard to get back to command mode.

15) Type **/chroot** to search for the chroot section of the vsftpd configuration file.

16) Tap **"i"** for insertion mode

- 17) Using your cursor keys you must add the `chroot_local_user=YES` directive at the location as shown below. This line does not exist, so you must add it at the appropriate location for the purpose of organization within the configuration file.

```
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
```

18) Press **esc** to exit to command mode.

19) Now hit **:wq** (colon, then w for write, and q to quit)

20) Now, we'll start the vsftpd server. Type `/etc/init.d/vsftpd start` (We'll configure this to start automatically later when the machine boots)

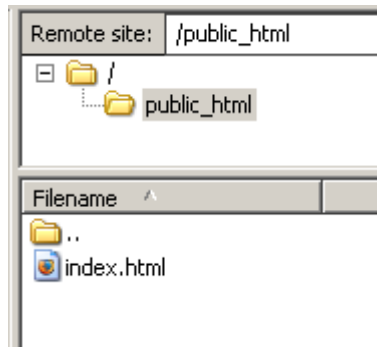
```
[root@brycefamily vsftpd]# vi vsftpd.conf
[root@brycefamily vsftpd]# /etc/init.d/vsftpd start
Starting vsftpd for vsftpd: [ OK ]
[root@brycefamily vsftpd]#
```

21) Next, let's test the FTP server. You can download your favorite FTP client. I like to use FileZilla. You can download from filezilla-project.org

22) Run FileZilla, and enter the hostname, username and password of your standard user. Here you can see that the FTP client is working fine, and if you double click the `public_html` folder, you will see the `index.html` file which we created earlier.



23) The user can now drag files into the `public_html` folder for use on his web page



Postfix (Mail Server)

Postfix is a mail server which I far prefer to the default program SendMail because of ease of configuration (and other things). Postfix is responsible for delivering mail when you send a message, and receiving mail from the Internet, and placing that mail into your mailbox.

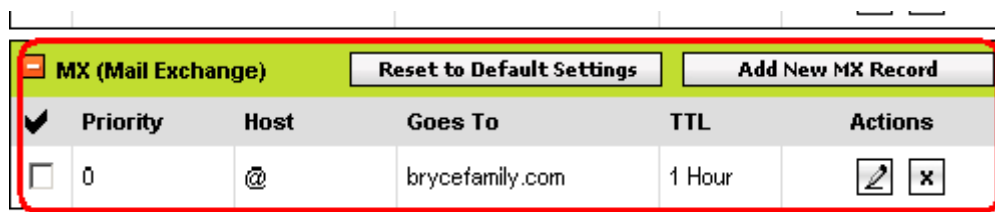
We are also going to configure Postfix to use the **Procmail** filter, which will call **SpamAssassin** to rate messages for Spam.

We also must set up support for **SASL** authentication. This is so only authenticated users can send mail through the server. We don't want someone using the server to send spam. That would be called an "Open Relay" An ISP does not usually configure SASL authentication because you are on one side of their server (the side they allow mail from), and the Internet is on the other side of the server. In our case, you will be accessing the server from the Internet side just like everyone else, so we have to be careful about who we accept messages from.

When a user connects to the server with a mail client, such as Thunderbird, or Outlook, the **Dovecot** server will deliver the mail to them.

As you can tell, quite a bit is going on, but it's really pretty easy to configure. Be sure you followed the procedure for configuring your DNS servers, and that you have set up the mx entry under Total DNS Control

With this configuration, any unix user you added using the adduser command will be able to receive mail from the system using their username and password, so if other users want to use your domain as their email address, you simply add them with the **adduser username** and **passwd username** commands as we did earlier.



MX (Mail Exchange)		Reset to Default Settings		Add New MX Record	
Priority	Host	Goes To	TTL	Actions	
<input checked="" type="checkbox"/>	0	@	brycefamil.com	1 Hour	<input type="checkbox"/>

- 1) If you haven't done so already, log into your server, and become the root user with the **su** command.
- 2) We are going to first erase sendmail from your server. Type **yum erase sendmail**
- 3) Now, we'll install postfix, spamassassin, and procmail if they are not already on our system. Type **yum install postfix spamassassin procmail dovecot**

- 4) Next, we'll configure Postfix. Type `cd /etc/postfix` (This will change to the postfix configuration directory)
- 5) Now type `vi main.cf` (We are using the vi text editor to edit the main postfix configuration file.)
- 6) Type `/#myhostname` to search for the first entry we must modify.
- 7) Tap “i” for insert mode.
- 8) Change the entry to read `myhostname = mail.brycefamily.com` (substitute your own domain name) Be sure to remove the # sign at the beginning to make the line active. This is called “uncommenting” the line. Any text after the # sign is ignored by the program, such as comments the author of the file might write to help you understand the purpose of an entry..

```
# INTERNET HOST AND DOMAIN NAMES
#
# The myhostname parameter specifies the internet hostname of this
# mail system. The default is to use the fully-qualified domain name
# from gethostname(). $myhostname is used as a default value for many
# other configuration parameters.
#
myhostname = mail.brycefamily.com
#myhostname = virtual.domain.tld
```

- 9) Now press `esc` on your keyboard to take the editor into command mode.
- 10) Type `/#inet_interfaces` to search for the entry where we configure which interfaces to accept mail from.
- 11) Tap “i” for insert mode.
- 12) Uncomment the line “`inet_interfaces = all`”
- 13) Place a # sign before the line “`inet_interfaces = localhost`” (Thus, commenting out the line so it is ignored)

```
#
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost
```

- 14) Now press **esc** on your keyboard to take the editor into command mode.
- 15) Type **"/mydestination ="** (Without the quotes) to search for the entry where we configure which domains for which this server will accept mail.
- 16) Tap **"i"** for insert mode.
- 17) Comment out the first line (by placing a # before it), and uncomment the second line (by removing the # sign). Notice the second line contains the variable \$mydomain which is by default what you used for myhostname, minus the first component. Since I used mail.brycefamily.com as myhostname, mydomain will be considered to be brycefamily.com.

```
# Specify a list of host or domain names, /file/name or type:table
# patterns, separated by commas and/or whitespace. A /file/name
# pattern is replaced by its contents; a type:table is matched when
# a name matches a lookup key (the right-hand side is ignored).
# Continue long lines by starting the next line with whitespace.
#
# See also below, section "REJECTING MAIL FOR UNKNOWN LOCAL USERS".
#
#mydestination = $myhostname, localhost.$mydomain, localhost
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
# mail.$mydomain, www.$mydomain, ftp.$mydomain
```

- 18) *Note: If other domains are pointing to your server, and you wish to accept mail to those domains, simply add a comma after \$mydomain on the line you commented out, and add those other domains (separated by commas) Postfix will ONLY accept mail for domains specified under mydestination, even of the DNS for other domains are configured to point to your server.*
- 19) Now press **esc** on your keyboard to take the editor into command mode.
- 20) Type **/procmail** to locate the entry where we configure procmail to act as our mail filter. For my purpose, I want to mark mail as spam if it has a spam rating of 5, and drop the mail if it has a spam rating of 10. We'll configure Procmail later, but for now, we are just going to configure Postfix to use Procmail for processing mail.
- 21) Tap **"i"** for insert mode.

22) Uncomment the mailbox_command line, and change the path to /usr/bin/procmail as shown.

```
# IF YOU USE THIS TO DELIVER MAIL SYSTEM-WIDE, YOU MUST SET UP AN
# ALIAS THAT FORWARDS MAIL FOR ROOT TO A REAL USER.
#
# mailbox_command = /usr/bin/procmail
# mailbox_command = /some/where/procmail -a "$EXTENSION"
```

23) Now press **esc** on your keyboard to take the editor into command mode.

24) Now hold **CTRL + F** to go to the end of the file (CTRL and F at the same time)

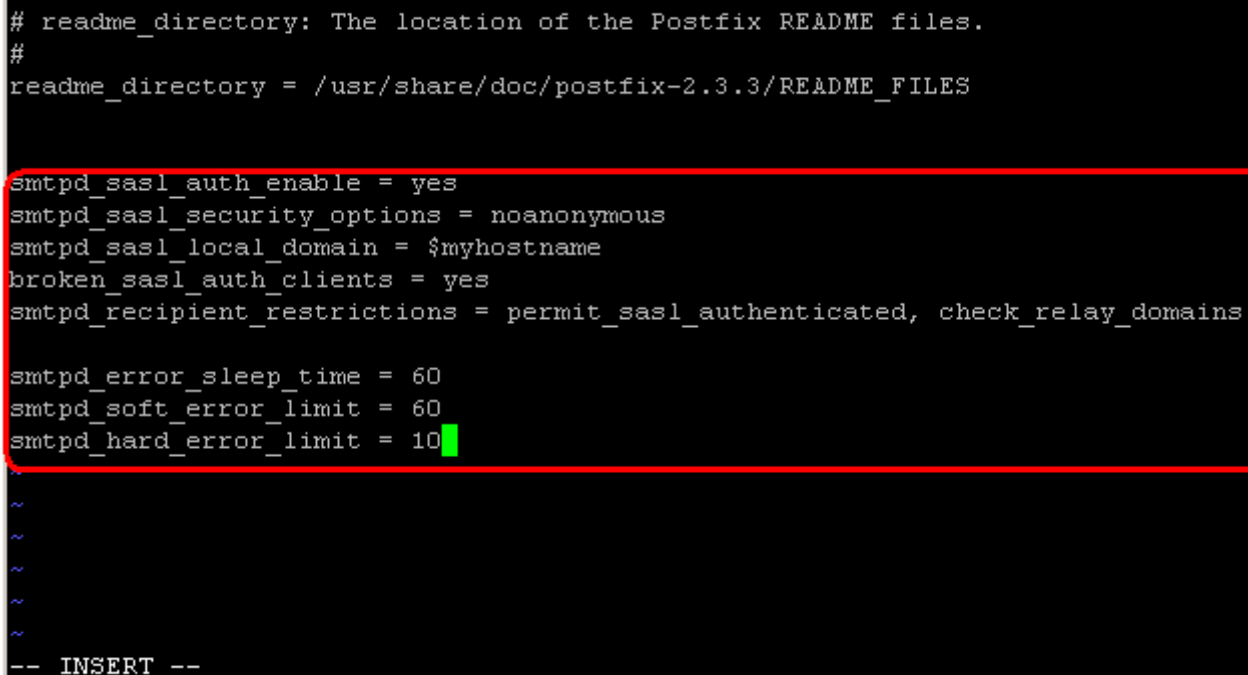
25) Tap **"i"** for insert mode.

(Next page)

26) Using your mouse keys, go to the end of the last line, then press enter, to add the following text to the end of the file. The purpose of this entry is to set up SASL authentication, so only valid users can send mail. (You can actually copy this text, and paste it at the bottom of your file if you wish. Be careful to paste it to the very end of the file, and not to corrupt the rest of the mail.cf file. As soon as you right click on the end of the file, the text will automatically be pasted if you copied it from here. Other options are available, and you can find them with a search engine.

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated, check_relay_domains

smtpd_error_sleep_time = 60
smtpd_soft_error_limit = 60
smtpd_hard_error_limit = 10
```



```
# readme_directory: The location of the Postfix README files.
#
readme_directory = /usr/share/doc/postfix-2.3.3/README_FILES

smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated, check_relay_domains

smtpd_error_sleep_time = 60
smtpd_soft_error_limit = 60
smtpd_hard_error_limit = 10

-- INSERT --
```

27) Press **esc** on your keyboard.

28) Now press **:wq** (colon, then w for write, and q to quit)

29) Note: Now Postfix is configured, but we need to configure the **procmail** filter. Procmail will call **SpamAssassin** to mark messages as Spam. This will allow us to easily manage Spam on our email client such as Thunderbird or Outlook by setting spam rules. SpamAssassin itself will not filter out junk mail, but just marks messages as spam which have a rating of 5 or more. Procmail will then be instructed to drop messages with a spam rating of 10 or more, which would almost certainly be junk mail. Keep in mind that no spam filter is 100% accurate, so it's not impossible that you could mark or drop some messages that were not really spam. (take that as a warning!) If you don't want this to happen, simply do not use the last part of the configuration file. I've found, however, that this configuration works out very well for me.

30) Type **cd /etc**

31) Type **vi procmailrc** (You will actually be creating the configuration file here)

32) Tap “i” on your keyboard for insert mode.

33) Set up your procmailrc file as follows. (You can copy and paste the text below if you wish)

Uncomment the following 3 lines and use tail -f procmail.log to debug

```
#LOGFILE=$HOME/procmail.log
```

```
#VERBOSE=yes
```

```
#LOGABSTRACT=all
```

```
# Send all mail through SpamAssassin
```

```
:0fw: spamassassin.lock
```

```
* < 256000
```

```
| spamassassin
```

```
# Mail that is very likely spam (>15) can be dropped on the floor.
```

```
# Move the # up one line to save it on the server instead.
```

```
# Note that dropping mail on the floor is a *bad*
```

```
# idea unless you really, really believe no false positives will
```

```
# have a score greater than 15.
```

```
:0
```

```
* ^X-Spam-Level: \*\*\*\*\*\*\*\*\*\*
```

```
/dev/null
```

```
#almost-certainly-spam
```

34) Hit esc on your keyboard

35) Type **:wq** (colon, w to write, and q to quit)

36) Now, you can check the configuration with Webmin. Open your web browser, and type <https://brycefamily.com:1000> (substitute your own domain)

37) I'm using firefox, so I'm going to add an exception since I didn't pay for a certificate from a trusted authority. You can download firefox from mozilla.org. Depending on your version of Firefox, the procedure may be a bit different. *If you are running Internet Explorer, the procedure will be a bit different from below.* If webmin came up automatically, then you can ignore the next few steps where I'm accepting the certificate. (skip down to where we log into webmin.)

(Error code: sec_error_untrusted_issuer)

- This could be a problem with the server's config trying to impersonate the server.
- If you have connected to this server successfully temporary, and you can try again later.

[Or you can add an exception...](#)

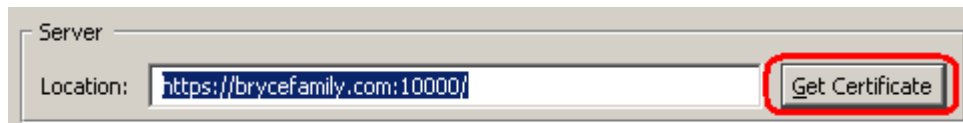
38) Now, we click “Add Exception”

You should not add an exception if you are using an internet connection completely or if you are not used to seeing a warning for

Get me out of here!

Add Exception...

39) Then, we'll get the certificate.

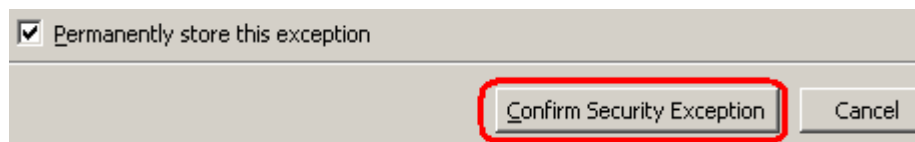


Server

Location:

Get Certificate

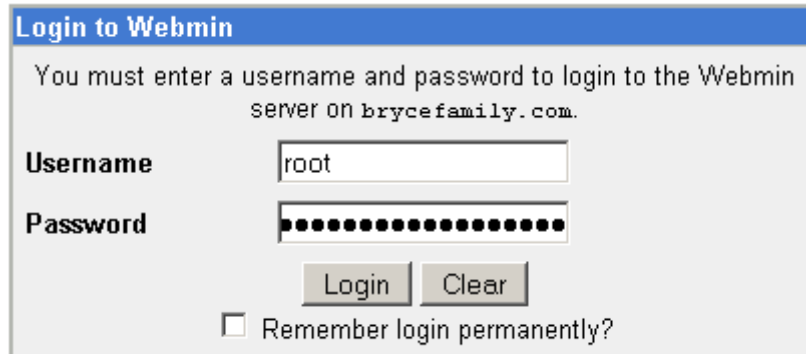
40) Now, we'll confirm the security exception.



Permanently store this exception

Confirm Security Exception Cancel

41) Now let's log into webmin with your root username and password



42) Under “Servers” choose the procmail filter

- Servers
 - Postfix Mail Server
 - PostgreSQL Database Server
 - ProFTPD Server
 - Procmail Mail Filter**

43) Now, you can see the configuration we just created in the procmailrc file, and you can manage your configuration from webmin.

Module
Config

Procmail Mail Filter

[Select all.](#) | [Invert selection.](#) | [Add a new filter action.](#) | [Add a new conditional block.](#)
[Add a new variable setting.](#) | [Add a new include file.](#)

	Action to take	Conditions	Move	Add
<input type="checkbox"/>	Feed to program <code>spamassassin</code>	Size is < 256000	↓	↑ ↓
<input type="checkbox"/>	Append to file <code>/dev/null</code>	Match regexp <code>^X-Spam-Level: ****************</code>	↑	↑ ↓

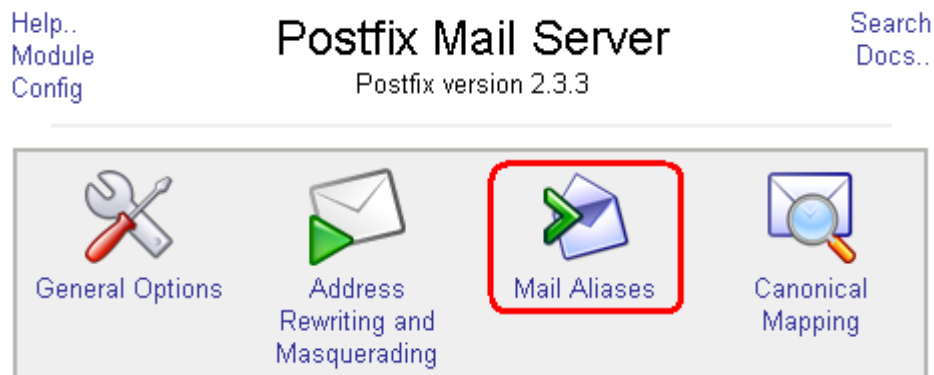
[Select all.](#) | [Invert selection.](#) | [Add a new filter action.](#) | [Add a new conditional block.](#)
[Add a new variable setting.](#) | [Add a new include file.](#)

Delete Selected Actions

44) Next, we'll configure the mail aliases. Aliases simply point fake usernames such as sales, info, support, etc to another email address such as ricky@brycefamil.com This means that if someone sends a message to support@brycefamil.com, that message will be redirected to ricky@brycefamil.com To configure the Aliases, click "Postfix Mail Server" under "Servers" in webmin.



45) Now, click on "Mail Aliases"



46) Click the text for "Support" (not the checkbox, but the text)

<input type="checkbox"/>	info	Address postmaster
<input type="checkbox"/>	marketing	Address postmaster
<input type="checkbox"/>	sales	Address postmaster
<input type="checkbox"/>	support	Address postmaster

47) Set the address to forward to, then save your changes. (Note: support can be forwarded to more than one email address)

The screenshot shows a dialog box titled "Edit Alias". It contains the following fields and controls:

- Description:** An empty text input field.
- Address:** A text input field containing the word "support".
- Enabled?:** Radio buttons for "Yes" (selected) and "No".
- Alias to:** A dropdown menu currently showing "Email address". To its right is a text input field containing "ricky@brycefamilay.com", which is highlighted with a red rectangular border.
- Alias to:** A second dropdown menu currently showing "<None>".
- At the bottom are two buttons: "Save" and "Delete".

48) Let's go back to PUTTY, and type **reboot** at the command prompt.

49) Wait a few minutes, then log back into your server.

50) Type **su** to become superuser if you logged in as a standard user.

51) Type **/etc/init.d/postfix status**

52) If postfix is not running, type **/etc/init.d/postfix start** (We'll configure services to run at startup later on.)

53) Type **/etc/init.d/spamassassin status**

54) If spamassassin is not running, type **/etc/init.d/spamassassin start**

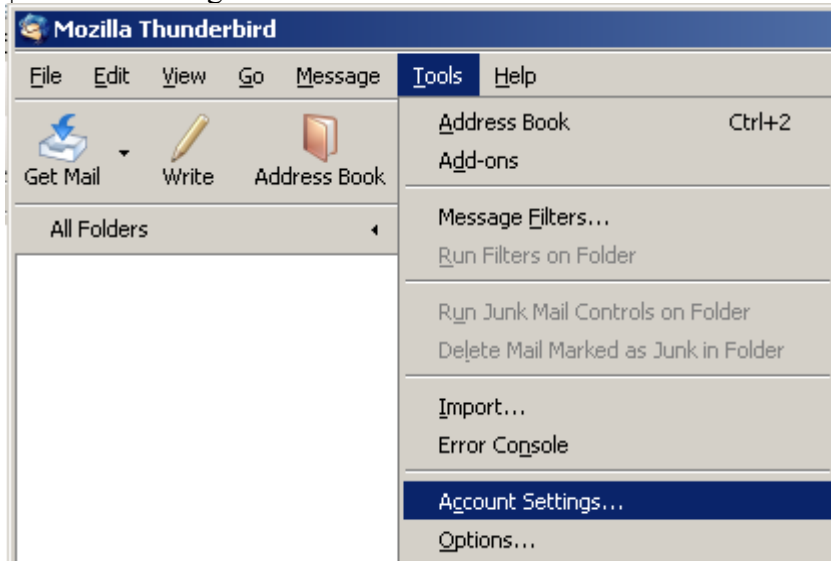
55) We'll do the same with dovecot. Type **/etc/init.d/dovecot status**

56) If dovecot is not running, type **/etc/init.d/dovecot start**

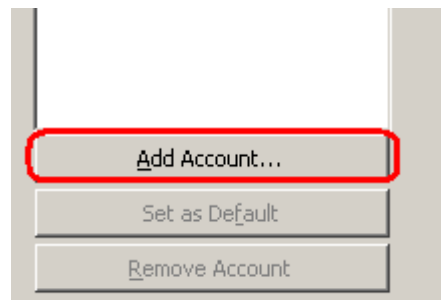
57) Now, we are going to test the email client. You can use Thunderbird, Outlook, or another client of your choice that supports SASL authentication. For this example, we are going to use Thunderbird, which can be downloaded from <http://www.mozilla.com/en-US/thunderbird/>

58) Here, I've canceled the account wizard, so I can configure the account manually.

59) Click Tools | Account settings.



60) Then, add an account.



61) This will be an email account. Click Next



62) Populate your name and your email address. Click “Next”.

Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").

Your Name:

Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").

Email Address:

63) Configure your incoming, and outgoing mail servers. Click “Next”:

Select the type of incoming server you are using.

POP IMAP

Enter the name of your incoming server (for example, "mail.example.net").

Incoming Server:

Uncheck this checkbox to store mail for this account in its own directory. That will make this account appear as a top-level account. Otherwise, it will be part of the Local Folders Global Inbox account.

Use Global Inbox (store mail in Local Folders)

Enter the name of your outgoing server (SMTP) (for example, "smtp.example.net").

Outgoing Server:

64) Set your username. (You will be using the username and password you added in an earlier lesson (adduser and passwd commands) Click “Next”

Enter the incoming user name given to you by your email provider (for example, "jsmith").

Incoming User Name:

Your outgoing (SMTP) server, "brycefamily.com", is identical to your incoming server, your incoming user name will be used to access it. You can modify outgoing server settings by choosing Account Settings from the Tools menu.

65) Here, I'm using the default account name. Again, click "Next".

Enter the name by which you would like to refer to this account (for example, "Work Account", "Home Account" or "News Account").

Account Name:

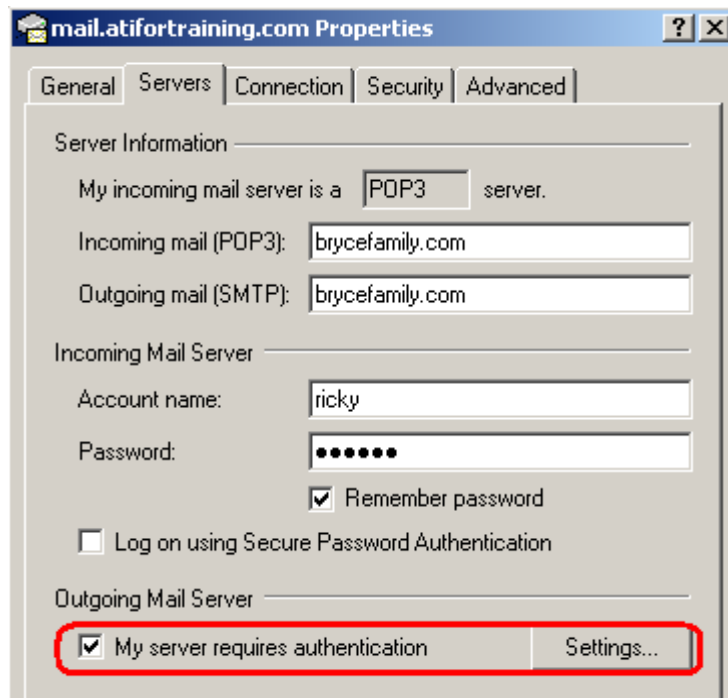
66) Verify your information, then hit "Finish" Then press "OK"

Please verify that the information below is correct.

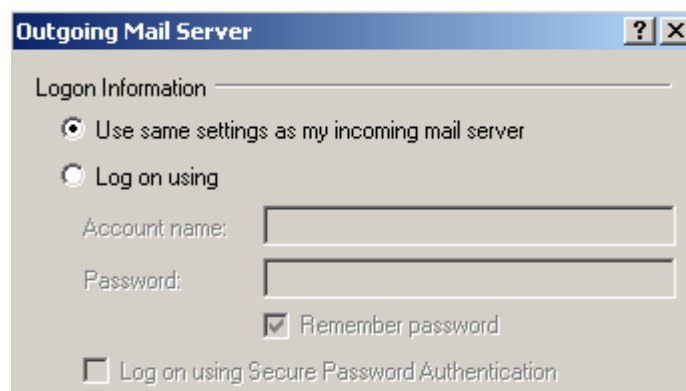
Account Name:	ricky@brycefamily.com
Email Address:	ricky@brycefamily.com
Incoming User Name:	ricky
Incoming Server Name:	brycefamily.com
Incoming Server Type:	POP3
Outgoing User Name:	ricky
Outgoing Server Name (SMTP):	brycefamily.com

67) Your email client should be set up. You can now test your email by sending to another email account. You will also want to test your email by having the other account send a message to your username on this server. You will be asked for the password. This will be the Unix system password from when you added the user with the adduser and passwd commands in an earlier lesson.

68) You can also try to send a message to yourself on your own server. If you can send a message to yourself, but other's aren't getting messages you send, be sure the reverse DNS is properly set up. You can google sites that will do a reverse DNS lookup on your IP address. Reverse DNS is necessary so other servers can verify your server is who it says it is. This will minimize the chance of your messages being dropped by the remote server. In the "Configuring DNS" Section, I'm showing you how to generate a reverse DNS request with VPSLink. You can't configure Reverse DNS on your own. You need to contact support, and have them do it for you. If you are using Outlook Express, be sure to check the box that states your mail server requires authentication. No encryption such as SSL is used... Just Authentication. See the image below...



69) Here's the settings screen:



SquirrelMail (Webmail)

Squirrelmail is a web based email client. Not much configuration is required for Squirrelmail.

- 1) First, let's make sure squirrelmail is installed. Type **yum install squirrelmail**
- 2) Now, let's make sure some services are running. (We'll configure these later to start automatically)
 1. Type **/etc/init.d/postfix status**.
If postfix is not running, type **/etc/init.d/postfix start**
 2. Type **/etc/init.d/dovecot status**.
If dovecot is not running, type **/etc/init.d/dovecot start**
 3. Type **/etc/init.d/spamassassin status**.
If spamassassin is not running, type **/etc/init.d/spamassassin start**
- 3) Now, we need to set the host name in the squirrelmail configuration file. Type **cd /etc/squirrelmail/**
- 4) Type **vi config.php** (This will allow us to edit the config.php file in the vi editor)
- 5) Type **/domain** to search for the domain entry.
- 6) Tap **"i"** on your keyboard for Insert mode.
- 7) Configure your domain as shown:

```
$provider_name      = 'SquirrelMail';  
  
$motd = "";  
  
$squirrelmail_default_language = 'en_US';  
$domain              = 'brycefamily.com';  
-- INSERT --
```

- 8) Press **esc** on your keyboard for command mode.
- 9) Type **:wq** (colon, w for write, and q to quit)

10) Now, we'll configure the Apache web server to serve the webmail directory for Squirrelmail. Type `cd /etc/httpd/conf/` to enter the Apache configuration directory.

11) Type `vi httpd.conf` to edit the Apache Configuration file

```
[root@brycefamily conf]# cd /etc/httpd/conf
[root@brycefamily conf]# vi httpd.conf
```

12) Tye `/NameVirtualHost` to locate our custom directives for Apache.

13) Tap “i” for insert mode. Type or paste the following text beneath the NameVirtualHost line

```
# This directory entry is required to make Squirrelmail work.
<Directory /usr/share/squirrelmail>
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
```

14) Your text should appear like this:

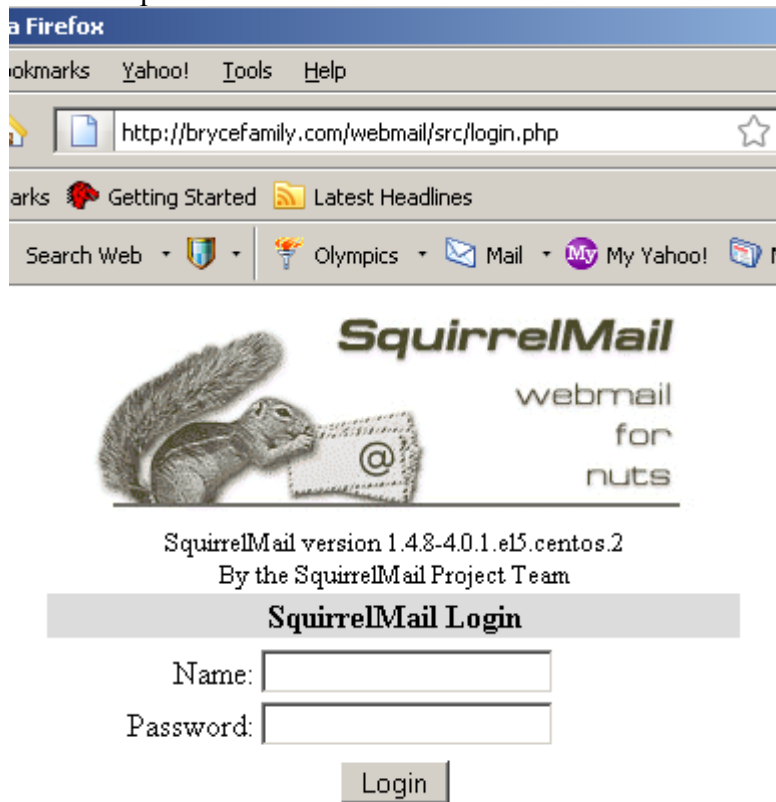
```
# Use name-based virtual hosting.
#
NameVirtualHost *:80
# This directory entry is required to make Squirrelmail work.
<Directory /usr/share/squirrelmail>
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
# This directory entry is required to make phpmyadmin work.
<Directory /usr/share/phpmyadmin>
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
```

15) Hit `esc` on your keyboard to go to command mode.

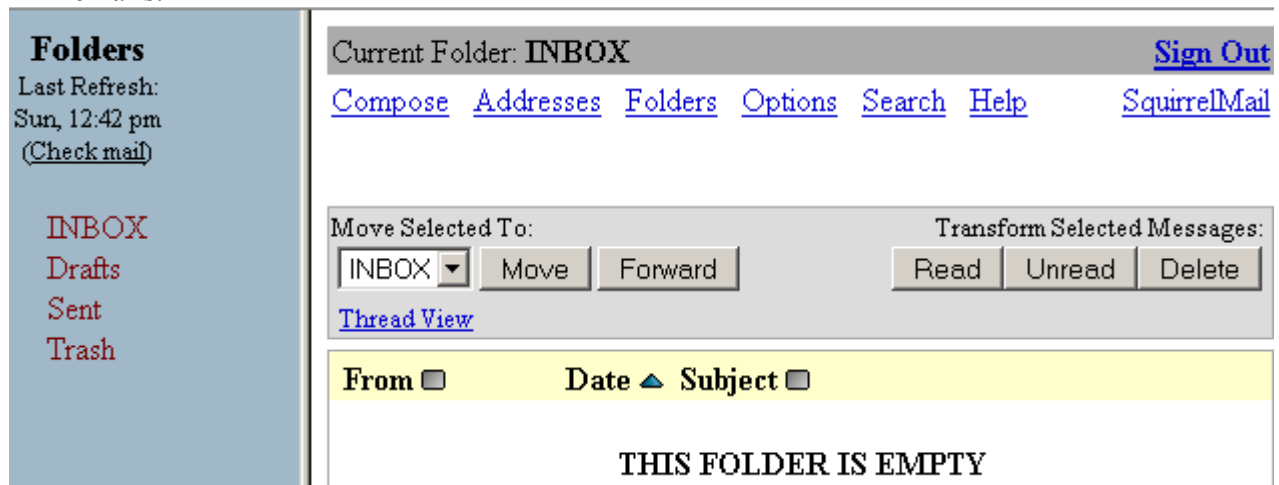
16) Now type `:wq` (colon, then w to write, and q to quit)

17) Restart apache: `/etc/init.d/httpd restart`

- 18) Now bring up your web browser, and we'll test your work! Enter <http://brycefamil.com/webmail> into your address bar. (substitute your domain). You should get a log in screen for Squirrelmail!



- 19) Log into squirrelmail using a standard user name, and you should be able to check and send emails.

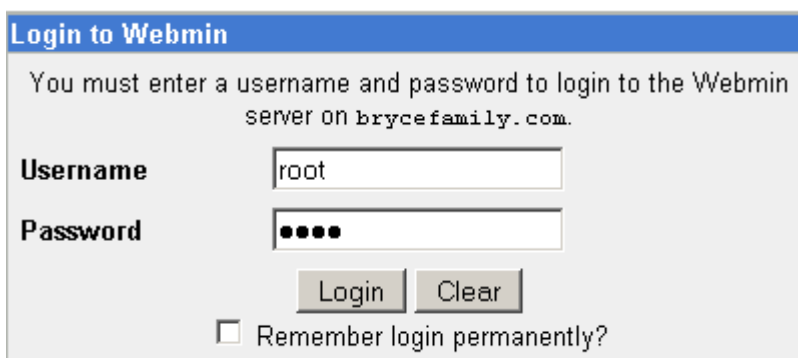


- 20) Note: With this configuration, all domains will be able to access the webmail folder.

IPTables (Firewall Configuration)

Next, we'll configure the IPTables firewall. We can do this graphically. A firewall is useful for blocking the ports of services which do not need to be accessible from the Internet. This makes your server more secure. IPTables can also be used to drop abusive IP addresses, and hinder "brute force" attacks, where the attacker will attempt to gain access to your system by sending random usernames and passwords.

- 1) We are going to set up our initial firewall configuration from webmin, so in your browser's address bar, go to <https://brycefamily.com:10000> (You may have to force the browser to accept the security certificate as we did in earlier lessons).
- 2) Log in with your root username and password.



Login to Webmin

You must enter a username and password to login to the Webmin server on brycefamily.com.

Username

Password

Remember login permanently?

- 3) Under "Networking", choose "Linux Firewall"



- 4) We are going to chose “Block all except ports used for virtual hosting, on interface: Eth0”, then hit “Setup Firewall”

Block all except SSH and IDENT on external interface:

Block all except SSH, IDENT, ping and high ports on interface:

Block all except ports used for virtual hosting, on interface:

- 5) Next, we'll need to open a few more ports, and customize the firewall to minimize the chance of “brute force” or “dictionary” attacks. The easiest way to do this is to manually edit the iptables firewall configuration file. Go to PUTTY, and login. Type **su** to become the root user if you are logged in as a standard user.
- 6) Type **cd /etc/sysconfig/** to enter the directory where our firewall configuration is stored.
- 7) Type **vi iptables** to open the file for editing with the vi text editor.
- 8) Cursor down about 21 lines until you are immediately after the *filter section. You will be sitting on the line that reads # Accept traffic from internal interfaces.
- 9) Tap “i” on your keyboard to get into Insert mode.
- 10) Press enter 5 times to give yourself some blank space above the line you are on.

```
root@brycefamil:/etc/sysconfig
# Completed on Sun Aug 24 18:17:30 2008
# Generated by iptables-save v1.3.5 on Sun Aug 24 18:17:30 2008
*filter
:FORWARD ACCEPT [0:0]
:INPUT DROP [0:0]
:OUTPUT ACCEPT [0:0]

# Accept traffic from internal interfaces
-A INPUT ! -i eth0 -j ACCEPT
# Accept traffic with the ACK flag set
-A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
# Allow incoming data that is part of a connection we established
-A INPUT -m state --state ESTABLISHED -j ACCEPT
```

11) Cursor up (with your up arrow key) 3 times.

12) Copy the following rules, and paste them into your text editor:

```
#####This is the custom rules#####  
# A few more things. Let's drop Brute force attacks....  
  
#Now Let's deal with Brute Force SSH Attacks  
  
-I INPUT -p tcp -i eth0 --dport 22 -m state --state NEW -m recent --set  
-I INPUT -p tcp -i eth0 --dport 22 -m state --state NEW -m recent --update --seconds 300 --hitcount 3 -j  
DROP  
  
-A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH -j ACCEPT  
-A INPUT -p tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j LOG --  
log-prefix "SSH_brute_force "  
-A INPUT -p tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j DROP  
  
#Now Let's deal with Brute Force FTP Attacks  
  
-I INPUT -p tcp -i eth0 --dport 21 -m state --state NEW -m recent --set  
-I INPUT -p tcp -i eth0 --dport 21 -m state --state NEW -m recent --update --seconds 300 --hitcount 10  
-j DROP  
  
-A INPUT -p tcp --dport 21 -m state --state NEW -m recent --set --name FTP -j ACCEPT  
-A INPUT -p tcp --dport 21 -m recent --update --seconds 20 --hitcount 10 --rttl --name FTP -j LOG --  
log-prefix "FTP_brute_force "  
-A INPUT -p tcp --dport 21 -m recent --update --seconds 20 --hitcount 10 --rttl --name FTP -j DROP  
  
#Block Bad Guys  
#-A INPUT -s IPAddressOfBadGuyHere -j DROP  
  
#Now, let's set up EchoLink Proxy Ports (For Ham Radio Operators only)  
-A INPUT -p udp -m udp --dport 5198:5199 -j ACCEPT  
-A INPUT -p tcp -m tcp --dport 5200 -j ACCEPT  
-A INPUT -p tcp -m tcp --dport 8100 -j ACCEPT  
  
#Open passive ports for VSFTPD  
-A INPUT -p tcp -m tcp --dport 60000:60500 -j ACCEPT  
  
#####End of the custom rules#####
```

13) Note: You may want to check out other common attacks as well, so you are prepared to set up your firewall to defend against them if you have a problem.

- 14) Hit esc on your keyboard to take the editor back to command mode.
- 15) Press **:wq** (colon, w for write, and q to quit)
- 16) Now, let's see if the firewall will restart. Type **/etc/init.d/iptables restart**

```
root@brycefamily:/etc/sysconfig
login as: root
root@brycefamily.com's password:
Last login: Sun Aug 24 10:28:16 2008 from irvingil.com
[root@brycefamily ~]# cd /etc/sysconfig
[root@brycefamily sysconfig]# vi iptables
[root@brycefamily sysconfig]# /etc/init.d/iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: nat mangle filter [ OK ]
Applying iptables firewall rules: [ OK ]
[root@brycefamily sysconfig]# █
```

- 17) It looks like our configuration was successful!! Contratulations.

Configure Services (for startup)

Next, we'll configure some essential services to start when the system starts. Since the VPS will default to Run Level 3 (text mode only), this is the run level we will configure. The Run Levels for CentOS are as follows:

Run Level 0 – Halt (shutdown)

Run Level 1 – Single-user Text Mode

Run Level 2 – Multi-User without NFS

Run Level 3 – Full Multi-User Text Mode

Run Level 4 – Not used (User Defined)

Run Level 5 – Full Multi-User Graphical Mode (With graphical login screen)

Since we can't actually be at the VPS, we can just stay in Run Level 3, and the graphical interface will not start on the local system when the computer boots, although we will still have web pages we can administer the server through.

We don't need to go there right now, but the run level configuration can be edited in the `/etc/inittab` file on your VPS system. Since a graphical interface is not installed, and we definitely need networking, we will **NOT** edit the file at this time.

```
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
```

Let's configure the services.

- 1) Login as a standard user
- 2) Type **su** to become the root user

3) Type **cd /etc/rc.d**

4) type **ls** to list the subdirectories

```
[root@brycefamily init.d]# cd /etc/rc.d
[root@brycefamily rc.d]# ls
init.d  rc.local          rc.sysinit  rc1.d  rc3.d  rc5.d
rc      rc.local.original rc0.d       rc2.d  rc4.d  rc6.d
[root@brycefamily rc.d]#
```

5) Since we are editing run level 3, we need to go into the rc3.d folder. Type **cd rc3.d**

6) Type **ls** to see how the services are configured.

```
[root@brycefamily rc3.d]# ls
K05sasauthd      K50vsftpd      K89rdisc       S22messagebus  S99killnash
K30spamassassin  K50xinetd      S08iptables    S55sshd        S99local
K35dovecot       K75netfs       S10network     S64mysqld      S99webmin
K35smb           K87named       S10restorecond S80postfix
K35winbind       K87portmap     S12syslog      S85httpd
K50netconsole    K89netplugd    S13mcstrans    S90crond
[root@brycefamily rc3.d]#
```

7) *Services beginning with a K are killed during this run level. Services beginning with an S are started during this run level. It's important to know the K and S are capitalized. The number immediately following the K or S indicates what order the service is Killed or Started. We need several services to start which are not already configured, so we will use the mv (move) command to rename some of the services, so they will be started instead of killed during this run level.*

- 8) Type **mv K05saslauthd S05saslauthd** (This will authenticate smtp messages if you are using a mail server)
- 9) Type **mv K30spamassassin S30spamassassin** (This will check and mark messages for spam)
- 10) Type **mv K35dovecot to S05dovecot** (This will allow users to receive email through their email client)
- 11) Type **mv K50vsftpd S50vsftpd** (This is the FTP server, which will allow users to upload web pages.)
- 12) Now type **ls** to verify all needed services will run at startup.

```
[root@brycefamily rc3.d]# mv K05saslauthd S05saslauthd
[root@brycefamily rc3.d]# mv K30spamassassin S30spamassassin
[root@brycefamily rc3.d]# mv K35dovecot S35dovecot
[root@brycefamily rc3.d]# mv K50vsftpd S50vsftpd
[root@brycefamily rc3.d]# ls
K35smb          K87portmap      S10restorecond  S50vsftpd      S99killnash
K35winbind     K89netplugd    S12syslog       S55sshd        S99local
K50netconsole  K89rdisc       S13mcstrans     S64mysqld     S99webmin
K50xinetd      S05saslauthd   S22messagebus  S80postfix
K75netfs       S08iptables    S30spamassassin S85httpd
K87named       S10network     S35dovecot     S90crond
[root@brycefamily rc3.d]#
```

- 13) Now you can reboot your machine, and all needed services (so far) should be running. Just type **reboot**.

EchoLink Proxy (for ham radio)

EchoLink Proxy can be used by licensed amateur radio operators only. If you are a licensed amateur radio operator, you can use the VPS Server to connect to EchoLink if you are behind a firewall, or do not have a public IP address. For example: Licensed amateur radio operators who travel would greatly benefit from EchoLink Proxy since each room in a motel has a private IP address, and the operator does not have control of the router, so cannot direct EchoLink traffic to his computer.

This document will assume you have opened the appropriate ports on your server. We did this earlier in this document under the section “IPTables”.

- 1) Be sure you are logged in, and type **su** if you are not the root user.
- 2) Now we need to install Java, since the EchoLink proxy is written in Java. To install java support, type **yum install java**
- 3) Be sure all packages are complete. I had to run **yum install java** twice when building this example.

```
Dependency Installed: alsa-lib.i386 0:1.0.14-1.
atk.i386 0:1.12.2-1.fc6 cairo.i386 0:1.2.4-5.e
.i386 0:2.10.4-20.el5 hicolor-icon-theme.noarch
i386 0:1.4.2.0-40jpp.115 jpackage-utils.noarch
1.0.1-2.1 libSM.i386 0:1.0.1-3.1 libXcursor.i38
1-2.1 libXfixes.i386 0:4.0.1-2.1 libXft.i386 0:
libXinerama.i386 0:1.0.1-2.1 libXrandr.i386 0:
1 libart_lgpl.i386 0:2.3.17-4 libgcj.i386 0:4.1
15 centos zip.i386 0:2.31-1.2.2
Complete!
[root@brycefamily ~]#
```


4) Now, we need to get the EchoLink packages. Go to echolink.org, and click “Download”



- [Take a Tour](#)
- [Download](#)
- [Validation](#)
- [Interfaces](#)

5) Enter your callsign and email address, then submit.

Callsign:

E-Mail Address:

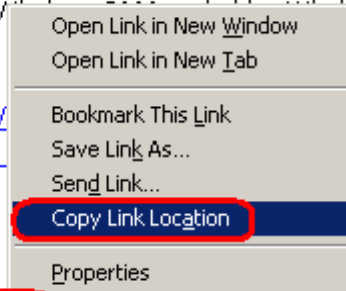
6) Under “Other Downloads”, right click the http link for EchoLink Proxy, and choose “Copy Link Location”.

Note: If you have difficulty installing on Windows 95/98/NT, you can run one of the links below.

- [Windows Installer for Windows 95/98](#)
- [Windows Installer for Windows NT](#)

Other Downloads

EchoLink Proxy Software v 1.2.3 [FTP](#) [HTTP](#)
Works together with EchoLink (version 1.9 or above) to allow access to the EchoLink other areas. Please see [EchoLink Proxy](#) for more info and installation instructions.



- 7) Now, back in PUTTY, type **cd /** to enter the root directory. (cd to change directory, then a space, then a forward slash)
- 8) Now, in PUTTY, type **wget** then hit the space bar.
- 9) Right click just after your cursor in PUTTY to paste the Link of the EchoLink Proxy file that we copied earlier.

```
[root@brycefamily ~]# cd /  
[root@brycefamily /]# wget http://www.echolink.org/downloads/EchoLinkProxy_1_2_3.zip
```

- 10) Press “Enter” within PUTTY, and verify your file downloaded properly.

```
--14:49:09-- http://www.echolink.org/downloads/EchoLinkProxy_1_2_3.zip  
Resolving www.echolink.org... 68.178.144.151  
Connecting to www.echolink.org|68.178.144.151|:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 18336 (18K) [application/zip]  
Saving to: `EchoLinkProxy_1_2_3.zip'  
  
100%[=====>] 18,336      --.-K/s   in 0.05s  
  
14:49:10 (389 KB/s) - `EchoLinkProxy_1_2_3.zip' saved [18336/18336]  
[root@brycefamily /]#
```

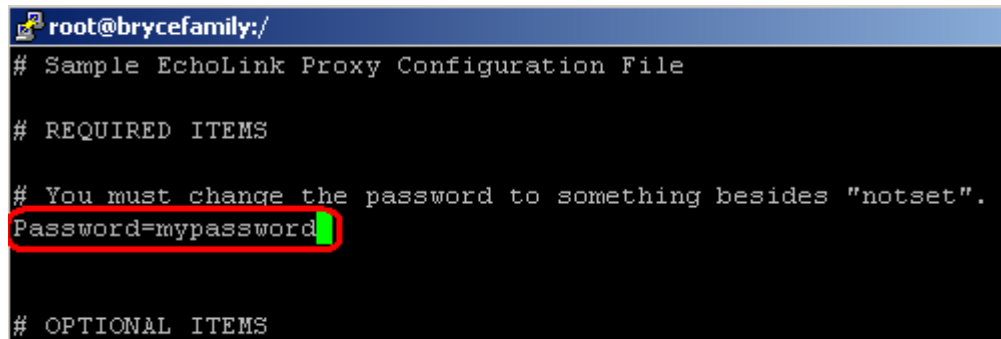
- 11) Now we need to unzip the EchoLink Proxy file. Type **unzip Echo*** (Note: the text is case sensitive.)
- 12) Verify the files did unzip.

```
[root@brycefamily /]# unzip Echo*  
Archive:  EchoLinkProxy_1_2_3.zip  
  inflating: EchoLinkProxy.jar  
  inflating: ELProxy.conf  
[root@brycefamily /]#
```

- 13) Now, the ELProxy.conf file must be configured with a password. Type **vi ELProxy.conf** (This will edit the ELProxy.conf file with the vi editor)

14) Tap “i” on your keyboard for insert mode.

15) Cursor down about 5 lines, and set the password.



```
root@brycefamilly:/  
# Sample EchoLink Proxy Configuration File  
  
# REQUIRED ITEMS  
  
# You must change the password to something besides "notset".  
Password=mypassword  
  
# OPTIONAL ITEMS
```

16) Hit esc on your keyboard to exit to command mode.

17) Press :wq (colon, then w to write, and q to quit)

18) Next, we'll set EchoLink to run as a service when the computer boots. Type **cd init.d**

19) Type **vi EchoLinkProxy** to create a new file with the vi editor.

20) Tap “i” for insert mode.

21) Paste the following text into your editor.

```
#!/bin/sh  
# description: Echo Link Proxy (java file)  
# chkconfig: 2345 99 00  
  
case "$1" in  
'start')  
    java -jar /EchoLinkProxy.jar /ELProxy.conf &  
    touch /var/lock/subsys/EchoLink  
    ;;  
'stop')  
    rm -f /var/lock/subsys/EchoLink  
    ;;  
*)  
    echo "Usage: $0 { start | stop }"  
    ;;  
esac  
exit 0
```

22) Hit **esc** on your keyboard to enter command mode.

23) Type **:wq** (colon, then w to write, and q to quit)

24) Now, we have to set permissions on the file. Type **chmod 755 EchoLinkProxy**

```
[root@brycefamily /]# vi ELProxy.conf
[root@brycefamily /]# cd /etc/init.d
[root@brycefamily init.d]# vi EchoLinkProxy
[root@brycefamily init.d]# chmod 755 EchoLinkProxy
[root@brycefamily init.d]#
```

25) Next, we'll create a symlink to the script in the rc3.d file. Type **cd /etc/rc3.d/** to enter the directory for run level 3

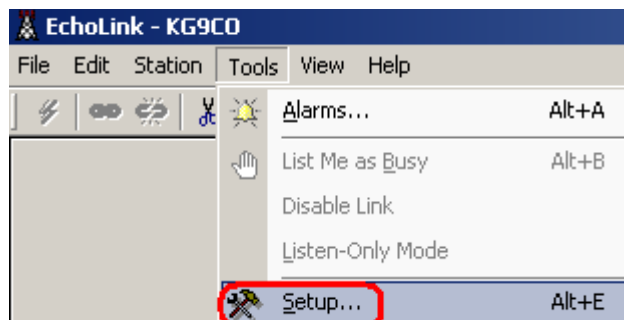
26) Type **ln -s /etc/init.d/EchoLinkProxy S99EchoLinkProxy**

```
[root@brycefamily rc3.d]# ln -s /etc/init.d/EchoLinkProxy S99EchoLinkProxy
[root@brycefamily rc3.d]#
```

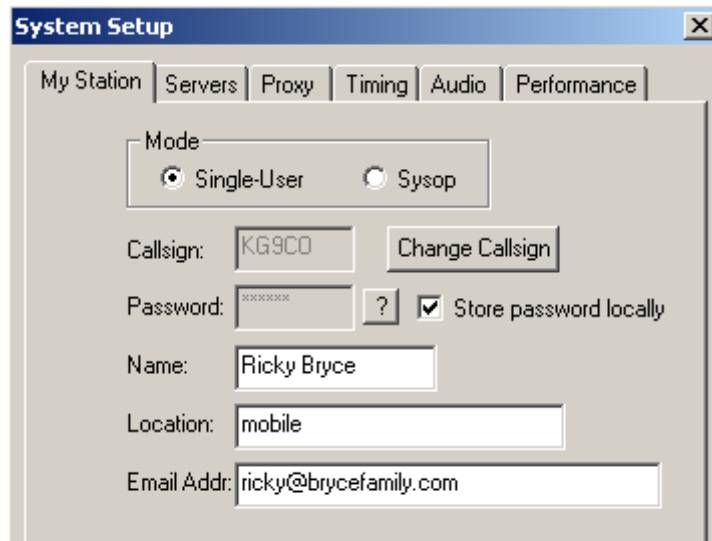
27) Type **reboot**, and we'll see if EchoLinkProxy starts.

28) If you haven't done so, go back to EchoLink.org, and download the main EchoLink program. You will have to register, and get validated if you haven't already done so. That could take a couple days.

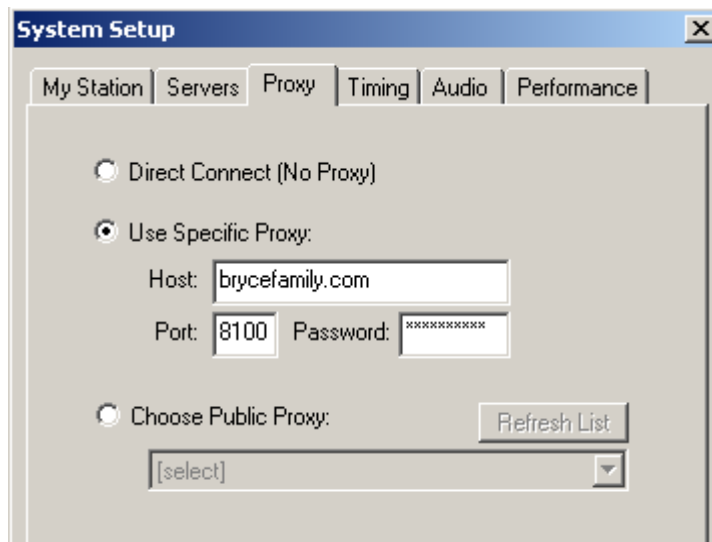
29) Click Tools | Setup from the menu bar



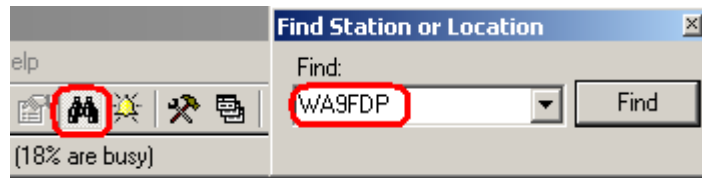
30) Be sure all fields are populated on “My Station” tab.



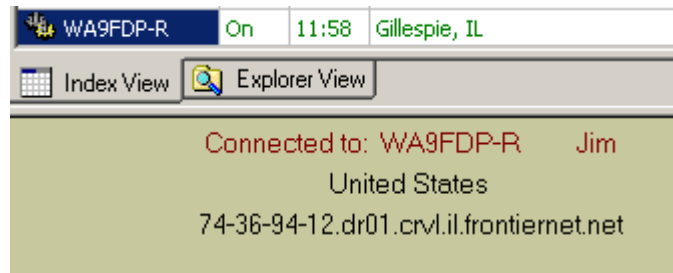
31) Click the Proxy Tab, and enter the hostname of your server, and the password you specified in ELProxy.conf. Then hit “ok”.



32) You should now be connected. I'm going to test my connection by searching for a station:



33) I can verify I've successfully connected through the proxy. You need to actually test this by voice to verify communication is possible through the proxy.



34) More information can be found at EchoLink.org