

# Post-Installation

## Set root's password for MySQL

```
mysql_secure_installation
```

## Log File Rotation

If this is not done the log files will keep growing indefinitely.

Edit `/etc/logrotate.d/asterisk`

```
/var/spool/mail/asterisk
/var/log/asterisk/*log
/var/log/asterisk/full
/var/log/asterisk/dtmf
/var/log/asterisk/freepbx_dbug
/var/log/asterisk/fail2ban {
    weekly
    missingok
    rotate 4
    #compress
    notifempty
    sharedscripts
    create 0640 asterisk asterisk
    postrotate
        /usr/sbin/asterisk -rx 'logger reload' > /dev/null 2> /dev/null || true
    endsript
    su root root
}
```

## TFTP

If you plan to use hardware SIP phones you will probably want to set up TFTP.

```
yum -y install tftp-server
nano /etc/xinetd.d/tftp
```

```
change server_args = -s /var/lib/tftpboot
to server_args = -s /tftpboot
change disable=yes
to disable=no
```

```
mkdir /tftpboot
chmod 777 /tftpboot
systemctl restart xinetd
firewall-cmd --permanent --zone=public --add-port=69/udp
firewall-cmd --reload
```

## MPG123

This is used in combination with sox to convert uploaded mp3 files to Asterisk compatible wav files.

```
cd /usr/src
wget http://ufpr.dl.sourceforge.net/project/mpg123/mpg123/1.22.4/mpg123-1.22.4.tar.bz2
tar -xjvf mpg123*
cd mpg123*/
./configure --prefix=/usr --libdir=/usr/lib64 && make && make install && ldconfig
```

## Digum addons

To register digium® licenses.

```
cd /usr/src
wget http://downloads.digium.com/pub/register/linux/register
chmod +x register
./register
```

To install the individual addons refer to the README files and ignore the register instructions.

- [http://downloads.digium.com/pub/telephony/codec\\_g729/README](http://downloads.digium.com/pub/telephony/codec_g729/README)
- [http://downloads.digium.com/pub/telephony/res\\_digium\\_phone/README](http://downloads.digium.com/pub/telephony/res_digium_phone/README)
- <http://downloads.digium.com/pub/telephony/fax/README>
- <http://downloads.digium.com/pub/telephony/hpec/README>

## Password protect http access

A simple way to block scanners looking for exploits on apache web servers.

```
mkdir -p /usr/local/apache/passwd
htpasswd -c /usr/local/apache/passwd/wwwpasswd someusername
htpasswd -c /usr/local/apache/passwd/wwwpasswd someotherusername
nano /var/www/html/.htaccess
```

```
# .htaccess files require AllowOverride On in /etc/httpd/conf/httpd.conf
AuthType Basic
AuthName "Restricted Access"
AuthUserFile /usr/local/apache/passwd/wwwpasswd
Require valid-user
```

Alternatively, the above .htaccess config can be added to /etc/httpd/conf/httpd.conf or as a separate file in /etc/httpd/conf.d/ as follows.

```
<Directory /var/www/html>
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /usr/local/apache/passwd/wwwpasswd
Require valid-user
</Directory>
```

## Whitelist protect http access

If http access is only required from certain IP addresses.

NOTE: Apache 2.4 ????????

Edit `/etc/httpd/conf.d/whitelist.conf`

```
<Location />
<RequireAny>
## Uncomment the following line to disable the whitelist
#Require all granted
Require ip x.x.x.x
Require ip x.x.x.x x.x.x.x x.x.x.x
Require ip x.x
Require ip x.x.x.0/255.255.255.0
Require host somedomain.com
#
## See http://httpd.apache.org/docs/2.4/mod/mod_authz_host.html for more examples
```

```
#  
</RequireAny>  
</Location>
```

?? Apache ??

NOTE???????? AllowOverride All ??

.htaccess?

```
order deny,allow  
deny from all  
# Alang's IPs  
allow from 123.123.123.1  
allow from 111.222.222.2  
allow from 192.168.99.
```

## G.729 Codec

- <https://www.asterisk.org/products/add-ons/g729-codec/>
- <http://asterisk.hosting.lv/>

---

Revision #4

Created 28 January 2021 14:15:58 by Admin

Updated 11 August 2024 10:42:35 by Admin