

??

???Debian 7.x

?????<https://www.fail2ban.org/wiki/index.php/Downloads>

```
#> tar xzf 0.9.2.tar.gz
#> cd fail2ban-0.9.2/
#> python setup.py install
```

????

```
#> fail2ban-client -h
```

??

Asterisk Logger ??

/etc/asterisk/logger.conf:

```
...
[logfiles]
...
fail2ban => notice,warning,security
```

????

```
#> asterisk -rx "logger reload"
#> asterisk -rx "logger show channels"
```

?? **jail**

for Asterisk)

/etc/fail2ban/jail.d/asterisk.conf

```
[asterisk]
enabled = true
logpath = /var/log/asterisk/fail2ban
maxretry = 5
bantime = 259200
```

for SSH)

/etc/fail2ban/jail.d/sshd.conf

```
[sshd]
enabled = true
bantime = 7200
findtime = 900
maxretry = 4
```

????

```
#> cd fail2ban-0.9.2/  
#> cp files/debian-initd /etc/init.d/fail2ban  
#> chmod 0755 /etc/init.d/fail2ban  
#> update-rc.d fail2ban defaults
```

????

```
#> service fail2ban start
```

Q & A

Q:?? Call Log ??????

Call from " (195.154.134.116:5071) to extension '8011441295298642' rejected because extension not found in context 'public'.

Ans??? Asterisk ? allowguest=no

?? sip.conf

allowguest=no

?????

```
#> asterisk -rx "sip reload"  
#> asterisk -rx "sip show settings" | grep -i "Allow unknown access"  
Allow unknown access: No
```