

# Config Fail2Ban for Apache2

---

## Install the package

---

```
apt install fail2ban
```

## Show the status of the active rules

---

```
fail2ban-client status
```

## Block error 403 (Forbidden)

---

Create a file on `/etc/fail2ban/jail.d` named `apache-forbidden.conf` and write the following:

```
[apache-forbidden]
enabled = true
filter = apache-forbidden
logpath = /var/log/apache2/access.log
bantime = 2m
maxretry = 3
findtime = 2m
port = 80,443
banaction = iptables-multiport
```

In folder `/etc/fail2ban/filter.d` create a custom filter named `apache-forbidden.conf`

```
[Definition]
failregex = <HOST> - - .*HTTP/[0-9]+(.[0-9]+)?" 403
```

This will block for 2 minutes the hosts who try to access 3 times in 2 minutes to a content that is not allowed with error 403 (Forbidden)

Once we have created the config file and the custom filter we have to restart the service to activate the new rule

```
systemctl restart fail2ban
```