

Apache

- [Reverse proxy](#)
- [Basic authentication](#)
- [HTTPS \(SSL\)](#)

Reverse proxy

Some apache modules have to be enabled:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_balancer
sudo a2enmod proxy_http
```

Virtual hosts files have to be configured

```
<VirtualHost *:*>
    ProxyPreserveHost On
    ProxyPass          "/" "http://192.168.111.2/"
    ProxyPassReverse   "/" "http://192.168.111.2/"
    ServerName hostname.example.com
</VirtualHost>
```

Basic authentication

To protect some directory with basic authentication we have to edit the virtual host file and add some configurations like this:

```
<Directory /home/someuser/somesite/public_html>
    AuthType Basic
    AuthName "Authentication Required"
    AuthUserFile "/home/someuser/.htpasswd"
    Require valid-user
</Directory>
```

Then we have to create the user credentials file (AuthUserFile) with **htpasswd** command, in this example we will be using the file "/home/someuser/.htpasswd"

Using bcrypt

```
htpasswd -nbB USERNAME PASSWORD
```

Using MD5

```
htpasswd -nbm USERNAME PASSWORD
```

Using SHA1

```
htpasswd -nbs USERNAME PASSWORD
```

Using CRYPT

```
htpasswd -nbd USERNAME PASSWORD
```

<https://wiki.apache.org/httpd/PasswordBasicAuth>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-password-authentication-with-apache-on-ubuntu-14-04>

https://httpd.apache.org/docs/2.4/misc/password_encryptions.html

HTTPS (SSL)

```
add-apt-repository ppa:certbot/certbot
```

```
apt install python-certbot-apache
```

```
certbot --apache -d your_domain -d www.your_domain
```

<https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-18-04-pt>

Adding subdomain to existing certificate:

```
root@web2:/etc/letsencrypt# service apache2 stop
root@web2:/etc/letsencrypt# letsencrypt certonly --cert-name diogogl.com -d diogogl.com -d
bank.diogogl.com -d gilberto.diogogl.com -d gilbertoadmin.diogogl.com -d
gilbertomag.diogogl.com -d gilbertomagdev.diogogl.com -d gilbertotemplate.diogogl.com -d
git.diogogl.com -d home.diogogl.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
```

How would you like to authenticate with the ACME CA?

```
- - - - -
1: Apache Web Server plugin (apache)
2: Spin up a temporary webserver (standalone)
3: Place files in webroot directory (webroot)
- - - - -
```

```
Select the appropriate number [1-3] then [enter] (press 'c' to cancel): 2
Plugins selected: Authenticator standalone, Installer None
```

```
- - - - -
You are updating certificate diogogl.com to include new domain(s):
+ diogogl.com
+ gilberto.diogogl.com
+ gilbertoadmin.diogogl.com
+ gilbertomag.diogogl.com
```

```
+ gilbertomagdev.diogogl.com
+ gilbertotemplate.diogogl.com
+ git.diogogl.com
+ home.diogogl.com
```

You are also removing previously included domain(s):
(None)

Did you intend to make this change?

- - - - -
(U)pdate cert/(C)ancel: u

Renewing an existing certificate

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/diogogl.com/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/diogogl.com/privkey.pem
Your cert will expire on 2024-02-21. To obtain a new or tweaked version of this certificate in the future, simply run certbot again. To non-interactively renew **all** of your certificates, run "certbot renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>

Donating to EFF: <https://eff.org/donate-le>

```
root@web2:/etc/letsencrypt# service apache2 restart
```

```
root@web2:/etc/letsencrypt#
```