**1. Update the system**

As usual make sure the system is fully up to date before installing any packages:

# yum -y update

**2. Install Apache**

We are going to use Apache as our web server, install it using this command:

# yum -y install httpd

**3. Install mod\_ssl**

Install mod\_ssl as well as we are going to need it to configure our Let’s Encrypt SSL certificate:

# yum -y install mod\_ssl

**4. Configure Apache**

Create a document root folder for your site:

# mkdir /var/www/test

Create a virtual host config file for your site by opening it with nano and then pasting the following contents inside:

# nano /etc/httpd/conf.d/test-site.conf

<VirtualHost \*:80>

ServerAdmin admin@test.com

DocumentRoot "/var/www/test"

ServerName test.com

ServerAlias www.test.com

ErrorLog "/var/log/httpd/test.error\_log"

CustomLog "/var/log/httpd/test.access\_log" common

</VirtualHost>

Add a index.html file for testing purposes later with the following contents:

# nano /var/www/test/index.html

It works!

Change owner of the “/var/www/test” directory to the apache user so Apache can read the directory:

# chown -R apache:apache /var/www/test

Remember to change “test” for your site’s name.  
Now that we have Apache installed we can continue by installing certbot.

**5. Install certbot**

To install certbot first we need to make sure we have the EPEL repository enabled, to do that execute the following command:

# yum -y install epel-release

Make sure yum-utils is installed:

# yum -y install yum-utils

Then install certbot for Apache:

# yum -y install certbot-apache

Now that we have certbot installed, run certbot with the following command:

# certbot --apache

Certbot will ask you for the names you would like to activate HTTPS for:

Saving debug log to /var/log/letsencrypt/letsencrypt.log

Plugins selected: Authenticator apache, Installer apache

Starting new HTTPS connection (1): acme-v01.api.letsencrypt.org

Which names would you like to activate HTTPS for?

-------------------------------------------------------------------------------

1: test.com

2: www.test.com

-------------------------------------------------------------------------------

Select the appropriate numbers separated by commas and/or spaces, or leave input

blank to select all options shown (Enter 'c' to cancel):

Press enter to continue and then optionally if you want you can redirect your sites to HTTPS:

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.

-------------------------------------------------------------------------------

1: No redirect - Make no further changes to the webserver configuration.

2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for

new sites, or if you're confident your site works on HTTPS. You can undo this

change by editing your web server's configuration.

-------------------------------------------------------------------------------

Select the appropriate number [1-2] then [enter] (press 'c' to cancel):

If everything goes well you should see the following output:

-------------------------------------------------------------------------------

Congratulations! You have successfully enabled

https://test.com and https://www.test.com

You should test your configuration at:

https://www.ssllabs.com/ssltest/analyze.html?d=test.com

https://www.ssllabs.com/ssltest/analyze.html?d=www.test.com

-------------------------------------------------------------------------------

**6. Configure automatic renewal**

Now we are going to add a cronjob so our Let’s Encrypt SSL certificates can be renewed automatically.

First run the following command so we can have nano as the default editor:

# export EDITOR=/bin/nano

Then execute the following command to edit the crontab:

# crontab -e

Let’s Encrypt recommends the automatic renew cronjob to run twice a day, to do that add the following line and then save and exit the crontab:

\* \*/12 \* \* \* /usr/bin/certbot renew >/dev/null 2>&1

Now you should have successfully installed and configured Let’s Encrypt with Apache.



Of course you don’t have to install Let’s Encrypt on CentOS 7 with Apache, if you use one of our [outsourced Linux server support services](https://linuxhostsupport.com/per-incident-support.html), in which case you can simply ask our expert Linux admins to install Let’s Encrypt SSL certificate on your server with Apache. They are available 24×7 and will take care of your request immediately.

**PS.** If you liked this post, on how to install Let’s Encrypt on CentOS 7 with Apache, please share it with your friends on the social networks using the buttons on the left or simply leave a reply below. Thanks.