EFF

certbot instructions

What's your HTTP website running on?

Apache

CentOS/RHEL 8

Help, I'm not sure!

Apache on CentOS/RHEL 8

To use Certbot, you'll need...

comfort with the command line

...and an HTTP website

that is already online

with an open port 80

...which is hosted on a server

which you can access via SSH

with the ability to sudo

*optional if you want a **wildcard cert** : **DNS credentials***

default wildcard *

Snap Support

The Certbot snap supports the x86_64, ARMv7, and ARMv8 architectures. While we strongly recommend that most users install Certbot through the snap, you can find alternate installation instructions here.

SSH into the server running your HTTP website as a user with sudo privileges.

2. Install snapd

You'll need to install snapd and make sure you follow any instructions to enable classic snap support.
Follow these instructions on snapcraft's site to install snapd.

install snapd

3. Ensure that your version of snapd is up to date

Execute the following instructions on the command line on the machine to ensure that you have the latest version of **snapd**.

```
$ sudo snap install core; sudo snap refresh core
```

4. Remove certbot-auto and any Certbot OS packages

If you have any Certbot packages installed using an OS package manager like **apt**, **dnf**, or **yum**, you should remove them before installing the Certbot snap to ensure that when you run the command **certbot** the snap is used rather than the installation from your OS package manager. The exact command to do this depends on your OS, but common examples are **sudo apt-get remove certbot**, **sudo dnf remove certbot**, or **sudo yum remove certbot**.

If you previously used Certbot through the certbot-auto script, you should also remove its installation by following the instructions here.

5. Install Certbot

Run this command on the command line on the machine to install Certbot.

```
$ sudo snap install --classic certbot
```

6. Prepare the Certbot command

Execute the following instruction on the command line on the machine to ensure that the **certbot** command can be run.

```
$ sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

7. Choose how you'd like to run Certbot

Either get and install your certificates...

Run this command to get a certificate and have Certbot edit your Apache configuration automatically to serve it, turning on HTTPS access in a single step.

```
$ sudo certbot --apache
```

Or, just get a certificate

If you're feeling more conservative and would like to make the changes to your Apache configuration by hand, run this command.

8. Test automatic renewal

The Certbot packages on your system come with a cron job or systemd timer that will renew your certificates automatically before they expire. You will not need to run Certbot again, unless you change your configuration. You can test automatic renewal for your certificates by running this command:

```
$ sudo certbot renew --dry-run
```

The command to renew certbot is installed in one of the following locations:

```
/etc/crontab/
/etc/cron.*/*
systemctl list-timers
```

9. Confirm that Certbot worked

To confirm that your site is set up properly, visit **`https://yourwebsite.com/`** in your browser and look for the lock icon in the URL bar.

Troubleshooting? Encountering an error?

Get help

Need more options to customize your setup?

See how to work with Certbot

Like Certbot?

Donate to Certbot and EFF