How to Install Let's Encrypt SSL on Ubuntu with Certbot

Updated on February 28, 2022 by InMotion Hosting Contributor

3 Minutes, 1 Second to Read

Let's Encrypt provides free SSL certificates for your websites to use secure connections. Certbot is free open source software that allows you to easily create Let's Encrypt SSLs on your unmanaged Linux server. Log into SSH as root to begin.

Install Certbot in Ubuntu 20.04

Instead of the older python-certbot-apache package, Certbot now recommends using the snapd package manager to install Certbot in Ubuntu. InMotion Cloud Server Hosting is incompatible with snapd at this time, but Python Installs Packages (PIP) works just as well.

Install Certbot in Ubuntu with PIP

Cloud server users can install Certbot in Ubuntu with PIP.

Step 1. First, install PIP:

Copy

```
sudo apt install python3 python3-venv libaugeas0
```

Step 2. Set up a virtual environment:

Copy

```
sudo python3 -m venv /opt/certbot/
```

Copy

```
sudo /opt/certbot/bin/pip install --upgrade pip
```

Step 3. Install Certbot on Apache (or NGINX):

Copy

```
sudo /opt/certbot/bin/pip install certbot certbot-apache
```

Copy

```
sudo /opt/certbot/bin/pip install certbot certbot-nginx
```

Step 4. Create a symlink to ensure Certbot runs:

Website & Server Help Topics

- Website Tutorials
- Domain Names
- DNS and Nameserver Changes
- Email
- Zend Framework
- Search Engine Optimization
- Secure Socket Layer (SSL)
- Security
- Server Usage
- Software
- SSH and Root Access
- Troubleshooting Hacked Websites
- Web Analytics
- Website Error Numbers

Related Articles

- The Complete Guide to cPanel's Free AutoSSL
- Migrate and Transfer SSLs
- Installing SSLs and Generating CSRs in cPanel
- Force HTTPS with the .htaccess File
- What Is SSL and Why Is It Important?
- How to Disable Older TLS Versions in Apache and Nginx
- How to Enable a WordPress SSL
- How to Manage AutoSSL Certificates in cPanel
- AutoSSL with Cloudflare
- Purchasing an SSL Certificate from eNomCentral

Popular Tutorials

- Backups and Restorations
- cPanel
- Databases
- DNS and Nameserver Changes
- eCommerce
- Email Basics
- Git
- Google Tools
- Hosting Product Guides
- NGINX
- Secure Socket Layer (SSL)
- Security
- Softaculous
- SSH and Root Access
- WebHost Manager (WHM)
- WordPress
- WooCommerce

Copy

```
sudo ln -s /opt/certbot/bin/certbot /usr/bin/certbot
```

Install Certbot in Ubuntu with snapd

Our Dedicated Server Hosting users can use snapd.

Step 1. Install snapd:

Copy

```
sudo apt install snapd
```

Step 2. Ensure you have the latest snapd version installed:

Copy

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

Step 3. Install Certbot with snapd:

Copy

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

Step 4. Create a symlink to ensure Certbot runs:

Copy

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

Create an SSL Certificate with Certbot

Run Certbot to create SSL certificates and modify your web server configuration file to automatically redirect HTTP requests to HTTPS. Or, add “certonly” to create the SSL certificates without modifying system files (recommended if hosting staging sites that should not be forced to use an SSL).

Step 1. Choose the best option for your needs.
Create SSL certs for all domains and configure redirects in the web server:

Copy

```
sudo certbot --apache
```

Copy

```
sudo certbot --nginx
```

Create SSL certs for a specified domain (recommended if you’re using your system hostname):

Copy

```
sudo certbot --apache -d example.com -d www.example.com
```

Only install SSL certs:

Copy

```
sudo certbot certonly --apache
```

Copy

```
sudo certbot certonly --nginx
```

Step 2. Enter an email address for renewal and security notices.

Step 3. Agree to the terms of service.

Step 4. Specify whether to receive emails from EFF.

Step 5. If prompted, choose whether to redirect HTTP traffic to HTTPS – **1** (no redirect, no further changes to the server) or **2** (redirect all HTTP requests to HTTPS).

SSL Maintenance and Troubleshooting

After you install a Let's Encrypt certificate on your Ubuntu Certbot setup, you can test your website SSL status at https://WhyNoPadlock.com to identify mixed content errors.

The certificate files for each domain is stored in:

Copy

```
cd /etc/letsencrypt/live
```

Let's Encrypt certificates expire after 90 days. To prevent SSLs from expiring, Certbot checks your SSL status twice a day and renews certificates expiring within thirty days. You can view settings with Systemd or cron.d.

Copy

```
systemctl show certbot.timer
```

Copy

```
cat /etc/cron.d/certbot
```

Ensure the renewal process works:

Copy

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

SSL Improvements

Having an SSL cert and 301 redirects to force HTTPS aren't always enough to prevent hacks. Cyber attackers have found ways to bypass both security practices to infiltrate server communications.

HTTP Strict Transport Security (HSTS) is a security HTTP header that addresses this by telling web browsers to only serve your website when received with a valid SSL cert. If the browser receives an insecure connection, it rejects the data altogether to protect the user. It is easy to configure HSTS within your web server (e.g. Apache and NGINX).

This entry was posted in Secure Socket Layer (SSL).

Related Articles

← Infographic-How to Implement SSL Certificates

Purchasing an SSL Certificate from eNomCentral →

Was this article helpful? Let us know!

Blog token not found.

Need More Help?

Search our Help Articles

Search InMotion Hosting Suppo

Current Customers

Chat: Chat with Sales
Call: 757-416-6575 x2
Ticket: Submit a Support Ticket

Get Reliable Web Hosting

Chat: Chat with Sales
Email: sales@inmotionhosting.com
Call: 757-416-6575 x1

Get web hosting that grows with your business. Our all-in-one hosting platform gives you everything your website needs to scale - so you can focus on the next big thing for you and your business.

555 S. Independence Blvd., Virginia Beach, VA 23452