

Enable HTTPS on Nginx

Join us at SIGNAL
Singapore

Twilio

Sig

Would you like to learn how to install Nginx and configure the HTTPS feature to use a self-signed certificate on a computer running Ubuntu Linux? In this tutorial, we are going to enable the use of HTTPS on the Nginx server and create a self-signed certificate.

- Ubuntu 18
- Ubuntu 19
- Ubuntu 20
- Nginx 1.18.0

Equipment list

The following section presents the list of equipment used to create this tutorial.

Server

Network Switch

Laptop

As an Amazon Associate, I earn from qualifying purchases.

Join us at SIGNAL Sir

Twilio

Nginx - Related Tutorial:

On this page, we offer quick access to a list of tutorials related to Nginx.

List of Tutorials - Nginx

Nginx - Installing the Letsencrypt certificate

Nginx - Disable SSL, TLS 1.0, and TLS 1.1

Nginx - Redirect HTTP to HTTPS

Nginx - Redirect a URL

Nginx - Redirect the error 404

Nginx - Enable HTTP2

Nginx - Enable HSTS

Nginx - ModSecurity installation

Nginx - Kerberos authentication

Nginx - Radius authentication (Freeradius)

Nginx - Basic authentication

Nginx - PAM authentication

Nginx - Prevent Hotlinking

Nginx - Blocking direct access to images

Nginx - Blocking an IP address

Nginx - Blocking a User-agent

Nginx - Blocking a URL

Nginx - Blocking a country

Nginx - Blocking a city

Nginx - Blocking a continent

Nginx - PHP installation

Nginx - Python CGI

Nginx - Perl CGI

Nginx - Shell Script CGI

Nginx - Golang CGI

Nginx - Installation of Http_stub_status_module

Nginx - Disable the Cache

Nginx - Change the server identification header

Nginx - Proxy

Nginx - Docker

[Nginx - Disable directory listing](#)

[Nginx - Monitoring via Zabbix](#)

Tutorial Nginx - Enable HTTPS

Install the Nginx server and the required packages.

```
apt-get update
apt-get install nginx openssl
```

Create a private key and the website certificate using the OpenSSL command.

```
mkdir /etc/nginx/certificate
cd /etc/nginx/certificate
openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out nginx-certificate.crt -keyo
```

Enter the requested information.

```
Generating a RSA private key
.....++++
.....++++
writing new private key to 'nginx.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Rio de Janeiro
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TechExpert
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:200.200.200.200
Email Address []:
```

On the option named COMMON_NAME, you need to enter the IP address or hostname.

In our example, we used the IP address 200.200.200.2000.

Edit the Nginx configuration file for the default website.

```
vi /etc/nginx/sites-available/default
```

Here is the file, before our configuration.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;
    server_name _;
    location / {
        try_files $uri $uri/ =404;
    }
}
```

Here is the file, after our configuration.

```
server {
    listen 443 ssl default_server;
    listen [::]:443 ssl default_server;
    ssl_certificate /etc/nginx/certificate/nginx-certificate.crt;
```

```
    location / {
        try_files $uri $uri/ =404;
    }
}
```

Optionally, you may want to redirect HTTP users to the HTTPS version of your website.

In this case, use the following configuration.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name _;
    return 301 https://$host$request_uri;
}
server {
    listen 443 ssl default_server;
    listen [::]:443 ssl default_server;
    ssl_certificate /etc/nginx/certificate/nginx-certificate.crt;
    ssl_certificate_key /etc/nginx/certificate/nginx.key;
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;
    server_name _;
    location / {
        try_files $uri $uri/ =404;
    }
}
```

Restart the Nginx service.

```
service nginx restart
```

Open your browser and access the HTTPS version of your website.

In our example, the following URL was entered in the Browser:

• https://200.200.200.200

The Nginx server will display the HTTPS version of your website.

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Congratulations! You have finished the configuration of HTTPS on the Nginx server.



Twilio's SIGNAL Conference

Control Panel for Developers

AD management & reporting tool

professional hair coloring

Ad Twilio

Ad Plesk

Ad ADManager Plus

Ad organic hair color

Label Printing Solutions

Realize your vision.

Start 15 Days Free Trial

TE Connectivity |
Specialties 1006
Vibration, Accele
Sensor Voltage 1
PC Pins

Ad Mariteam Technology

Ad Autodesk

Ad Marker.io

Ad DigiKey Singapore

Related Posts

TUTORIAL

TUTORIAL

TUTORIAL

TUTORIAL

TUTORIAL

Nginx - Blocking access from a continent

April 17th, 2021

Nginx - Blocking access from a city

April 17th, 2021

Nginx - Blocking access from a country

April 17th, 2021

Nginx - Shell Script CGI

April 16th, 2021

Nginx - Disable directory listing

April 15th, 2021

Start with
\$50 Free

Invest with fast direct execution

Open an Account

Your capital is at risk. *T&

