# **Guide to Setting Up a Self-Signed SSL Certificate**

This guide explains how to create and use a self-signed SSL certificate for secure connections in internal networks or development environments. It assumes the following setup:

1. **SSL Create OS**: Ubuntu
2. **Server OS**: SUSE
3. **Reverse Proxy**: Nginx
4. **Client OS**: Windows
5. **Browser**: Google Chrome

## **Step 1: Generate a Self-Signed SSL Certificate on the Server**

### 1.1 Install Necessary Tools

Ensure that OpenSSL is installed on your system(You can do it by Centos, Windows..etc, This Example uses Ubuntu):

sudo apt update  
sudo apt install openssl

### 1.2 Create the Certificate and Private Key

Run the following command to generate the private key and self-signed certificate, this certificate’s will expire in 365 days :

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout ./test.key -out ./test.crt -config ssl.conf

You can find ssl.conf in this project for test.

You may want to change this required details in ssl.conf :

* **Country Name**: Enter your country code (e.g., TW).
* **State or Province Name**: Enter your state or province.
* **Locality Name**: Enter your city name.
* **Organization Name**: Enter your organization name.
* **Common Name**: Enter the domain (e.g., mydomain or internal IP).

## **Step 2: Configure Nginx to Use the Self-Signed Certificate**

### 2.1 Edit Nginx Configuration

Open your Nginx site configuration file (e.g., ./nginx.conf):

sudo vim /etc/nginx/conf.d/myconf.conf

You can find an example in nginx.conf of this project.

### 2.2 Test and Reload Docker

sudo docker compose --file docker-compose.yml down  
sudo docker compose --file docker-compose\_https.yml up

## **Step 3: Install the Self-Signed Certificate on Windows**

### 3.1 Copy the Self-Signed Certificate to Windows

Copy the certificate from the server to your Windows machine(You May need administer auth!):

scp user@your-server:/etc/ssl/certs/selfsigned.crt C:\path\to\save\selfsigned.crt

### 3.2 Install the Certificate as a Trusted Root Certificate

1. **Double-click** the selfsigned.crt file on Windows.
2. Click **“Install Certificate”**.
3. In the wizard, choose **“Local Machine”** and click **Next**.
4. Select **“Place all certificates in the following store”** and click **Browse**.
5. Choose **“Trusted Root Certification Authorities”** and click **OK**.
6. Complete the wizard to install the certificate.

## **Step 4: Enable Support for Self-Signed Certificates in Chrome**

Chrome generally supports trusted self-signed certificates. If issues persist, perform the following:

1. Restart Chrome to ensure the newly installed root certificate is loaded.
2. If security warnings persist, navigate to chrome://flags, search for and enable **“Allow invalid certificates for resources loaded from localhost”** (for local development only).

## **Step 5: Test the SSL Configuration**

1. Access your server using the HTTPS protocol:

* https://mydomain
* or
* https://your-internal-ip

1. Verify that the browser no longer shows a “Not Secure” warning.

After completing these steps, your internal network or development environment should securely utilize the self-signed SSL certificate. If you have further questions or issues, feel free to ask!