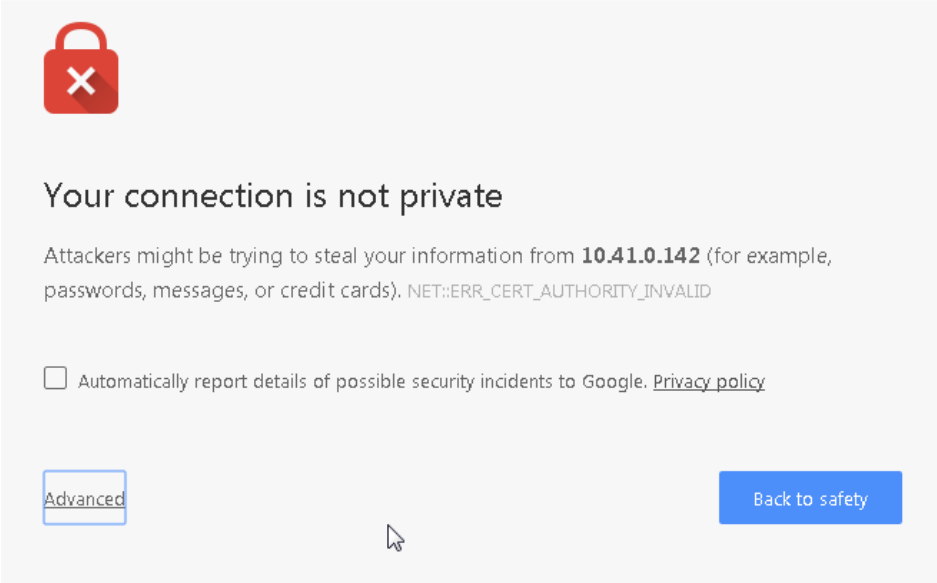
Securing TruView Global Site with SSL/TLS Certificate

Obtain a Certificate

You can purchase an official TLS/SSL certificate from any certification authority (CA). Alternatively, you can create a self-signed certificate for your TruView Global site. Note that when your user opens TruView Global site that uses a self-signed certificate, their browser may display warning messages about possible security issues about the site. An example of such warning is as shown below.



Enable Secure Connection

The following instructions describe how you install a certificate and enable secured connection for TruView Global site.

1. Logon to Ubuntu console.

2. Install an application “nginx” which will handle secured connections.

```
sudo apt-get update
sudo apt-get install nginx
```

3. If you have purchased an official certificate, copy both the key and certificate files to /etc/nginx directory. You should have /etc/nginx/cert.key and /etc/nginx/cert.crt files.

If you don't have an official certificate and want to create a self-signed one, execute these two commands. Once you run the second commend, You should have /etc/nginx/cert.key and /etc/nginx/cert.crt files.

```
cd /etc/nginx

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/nginx/cert.key -out /etc/nginx/cert.crt
```

4. Configure nginx to use the certificate and a reverse proxy for TruView Global. Open the configuration file in an editor:

```
sudo nano /etc/nginx/sites-enabled/default
```

Replace the existing configuration with this new configuration:

```
client_max_body_size 0;

server {

    listen 80 default_server;

    listen [::]:80 default_server ipv6only=on;

    root /usr/share/nginx/html;

    index index.html index.htm;


    # Make site accessible from http://localhost/

    server_name localhost;

    location / {

        proxy_pass http://127.0.0.1:9000;

    }

}

server {

   listen 443;
```

```
ssl_certificate         /etc/nginx/cert.crt;
ssl_certificate_key     /etc/nginx/cert.key;
ssl on;
ssl_session_cache  builtin:1000  shared:SSL:10m;
ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
ssl_prefer_server_ciphers on;
access_log          /var/log/nginx/ssl.access.log;
location / {
  proxy_set_header      Host $host;
  proxy_set_header      X-Real-IP $remote_addr;
  proxy_set_header      X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_set_header      X-Forwarded-Proto $scheme;
  proxy_pass        http://127.0.0.1:9000;
  proxy_read_timeout  90;
 }
}
```

5. Start nginx service.

```
sudo service nginx restart
```

6. Verify your secured TruView Global by opening `https://<ip` address>. A green lock icon followed by https should be present in your browser's address bar.