How to Install an SSL Certificate for SimpleRisk

Introduction

This guide is going to cover the use of an SSL certificate with SimpleRisk. If you already have a certificate. You may tto skip to the second section or continue you on and the guide will include creating a self-signed SSL certificate for use with your instance. Please note that users accessing the site will have to manually trust the certificate for your instance using a self-signed certificate is generally only suitable for instances that are locked down when it comes to long-term use. If you are using a self-signed long term the instance would be better off closed off from the internet and accessed from the local network only, otherwise you may want to look into purchasing a trusted certificate.

Instruction

Creating a Self-Sign Certificate

First we will cover creation of a self-signed cert. This method will guide you through the use of HTTPS (HTTP over TLS) to secure your Apache HTTP server, and does not require that your certificate is signed by a CA although if you are using one you may skip this section as mentioned above..

1) First login in to the terminal on the server and gain root privileges for your server using:

```
sudo bash
```

2) Next we need to choose a directory to store our cert and key pair, in this example we will create the directory if it does not already exist at “/etc/apache2/ssl/” and work from there. You can adjust this command to fit your O/S so if you are using CentOS as an example we would suggest “/etc/httpd/ssl”.

```
mkdir /etc/apache2/ssl/ && cd /etc/apache2/ssl/
```

3) Create the certificate using the following:

```
openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out simplerisk.crt -keyout simpleriskkey.key
```

The following is a breakdown of the OpenSSL options used in this command. There are many other options available, but these will create a basic certificate which will be good for a year. For more information, see `man openssl` in your terminal.

•`-newkey rsa:4096`: Create a 4096 bit RSA key for use with the certificate. RSA 2048 is the default on more recent versions of OpenSSL but to be sure of the key size, you should specify it during creation.

•-x509: Create a self-signed certificate.

•`-sha256`: Generate the certificate request using 265-bit SHA (Secure Hash Algorithm).

•-days: Determines the length of time in days that the certificate is being issued for. For a self-signed certificate, this value can be increased as necessary. •`-nodes`: Create a certificate that does not require a passphrase. If this option is excluded, you will be required to enter the passphrase in the console each time the application using it is restarted.

Once completed you should see something like this in your terminal.

4) You will be asked for a few details to be stored in your certificate and finally once completed we will change the file permissions of the key to be accessible only by root. This is an important step and should not be skipped.

```
chmod 400 /root/certs/simpleriskkey.key
```

5) Backup your certificate and key to an external storage that can be secured. This completes the process of generating a new self-signed key.

Updating the VirtualHost for HTTPS

Configuring SimpleRisk for use with your SSL certificate is a simple process consisting of updating a single configuration file for the virtual host which apache uses to determine details about how to make connections.

1) Open /etc/apache2/sites-enabled/ ssl-default.conf or your virtualhost configuration using:

```
vi /etc/apache2/sites-enabled/default-ssl.conf
```

2) Next we need to add a few new lines to your SSL virtualhost, if it was configured as shown in the Ubuntu install guide it should look like the following. Lines being edited are

in blue. If you are using a cert from a CA then you will need to also edit the following line just under the blue lines in the example below.

“**SSLCertificateChainFile /path/to/insertcerthere.crt** “

<VirtualHost *:443>

DocumentRoot "/var/www/simplerisk/"

<Directory "/var/www/simplerisk/">

AllowOverride all

Allow from all

Options -Indexes

</Directory>

SSLEngine on

SSLCertificateFile /etc/apache2/ssl/NewCertName.crt

SSLCertificateKeyFile /etc/apache2/ssl/NewKeyName.key

</VirtualHost>

3) The final step is to go ahead and save your apache configuration and close the file and restart apache using:

sudo systemctl restart apache2

Summary

You have now successfully configured your SSL Cert for use with SimpleRisk, if you have any questions or run into issues please contact us at support@simplerisk.com