Red Hat Linux – Guide to Installing Root Certificates, Generating CSR and Installing SSL Certificate

Trustis Limited

Building 273 New Greenham Park Greenham Common Thatcham RG19 6HN

E: info@trustis.com W: www.trustis.com

Registered in England No: 03613613

Table of Contents

1 Introduction

This document specifies instructions for Installing the Root and Intermediate certificates, generating your CSR, and Installing your certificate.

2 Install Root and Intermediate CA Certificates

You will need to install the CA certificates in order for your webserver to use your SSL certificate properly. **Apache users do not need to install these certificates individually. Instead you can install the CA certificates using a 'bundle' method.**

In the Virtual Host settings for your site, in the httpd.conf file, you will need to complete the following:

1. Copy the PEM format Bundled CA certificate file (full CA chain) found at http://www.trustis.com/pki/healthcare/ops/healthcarett-chain-pem.txt to the directory in which ca-bundled files are stored e.g. /etc/httpd/conf/ssl.crt/
2. Add the following line to the SSL section of the httpd.conf (assuming /etc/httpd/conf/ssl.crt/ is the directory to where you have copied the CA Bundle file). if the line already exists amend it to read the following:

SSLCACertificateFile /etc/httpd/conf/ssl.crt/cachainpem.txt

If you are using a different location and certificate file names you will need to change the path and filename to reflect your server.

The SSL section of the updated httpd config file should now read something similar to this example (depending on your naming and directories used):

SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt

SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key

SSLCACertificateFile /etc/httpd/conf/ssl.crt/cachainpem.txt

Save your httpd.conf file and **restart** Apache.

3 Certificate Signing Request (CSR) Generation

The process of creating a key and a CSR is straightforward and should only take a few minutes. Please note that the correct commands will depend upon whether you own the Official Red Hat Linux Professional boxed set or the Official Red Hat Linux Professional, International Edition, boxed set.

3.1 Generating a Key

1. Use the cd command to move to the /etc/httpd/conf directory.
2. As root, type in one of the following three commands to generate your key:
3. If you're using Official Red Hat Linux Professional and you want to use the included password feature, type in the following command:

   make genkey

   Your key will be generated and you will be asked to enter and confirm a password. Your password should be at least eight characters, should include numbers or punctuation and should not be a word in a dictionary. Also, remember that your password is case sensitive.

   Please note that you will need to remember and enter this password every time you start your secure Web server, so don't forget it.

4. If you're using Official Red Hat Linux Professional and you don't want to be required to type in a password every time you start your secure Web server, use the following command instead of make genkey to create your key (note that the following command should be typed in all on one line):

   /usr/sbin/sslgenrsa -rand /dev/urandom -out ssl.key/server.key 2048

   Then use the following command to set the correct permissions on your key:

   chmod go-rwx ssl.key/server.key

   If you use the above commands to create your key, you will not need to use a password to start your secure Web server. However, we don't recommend that you disable the password feature for your secure Web server, since it decreases the level of security for your server.

5. If you're using Official Red Hat Linux Professional, International Edition, type in the following single command, all on one line:

   /usr/bin/openssl genrsa -rand /dev/urandom -out /etc/httpd/conf/server.key 2048

   You will not be required to enter a password if you're using Official Red Hat Linux Professional, International Edition.

6. Your key will be created and saved to a file named server.key. If you're using Official Red Hat Linux Professional, server.key will be located in the /etc/httpd/conf/ssl.key directory. If you're using Official Red Hat Linux Professional, International Edition, server.key will be located in /etc/httpd/conf.

   The server.key file should be owned by root and should not be accessible to any other user. Make a backup copy of this file and keep the backup copy in a safe, secure place. You need the backup copy because if you lose the server.key file after using it to create your CSR and purchase a certificate, your certificate will no longer work and we will not be able to help you. Your only option would be to apply for a new certificate.

3.2 Generating a CSR

After you've created a key, you can create a CSR.

1. In the /etc/httpd/conf directory, become root and type in one of the following two commands:

   If you're using Official Red Hat Linux Professional, type in the following command:

   make certreq

   If you're using Official Red Hat Linux Professional, International Edition, type in the following single command (all on one line):

   /usr/bin/openssl req -new -key /etc/httpd/conf/server.key -out /etc/httpd/conf/server.csr

2. You will be prompted for your password (if you used a password when you generated your key). Type in the password, if necessary.

3. You'll see some instructions and you will be prompted for responses. Your inputs will be incorporated into the CSR. The complete display, with example responses, will look like this:

   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) [US]: **GB**
   State or Province Name []: **UK installations can use County name**
   Locality (City) Name []: **Your city or . if not desired**

Company (Organisation) Name []: Your organisation name
Department Name []: **Your Department name or . if not desired**
Server Host Name []: **fully qualified domain name e.g. test.mydomain.com**
Administrators E-mail address []: leave this blank
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

The default answers appear in brackets [] immediately after each request for input. For example, the first information required is the name of the country where the certificate will be used:

Country Name (2 letter code) [US]:

The default input, in brackets, is US. To accept the default, just press Enter or fill in the correct two-letter ISO code for your country.

You will have to type in the rest of the inputs (State or Province Name, Locality (City) Name, Company (Organisation) Name, Department Name, Server Host Name and Administrator's e-mail address). All of these should be self-explanatory but you need to follow these guidelines:

- For Server Host Name, make sure you type in the **real** name of your secure Web server (a valid DNS name) and not any aliases which the server may have.
- **Avoid any special characters like @, #, &, !,** etc. Special characters can sometimes cause problems in CSRs. So if your company name includes an ampersand (&), spell it out as "and" instead of "&."
- You don't need to use either of the extra attributes (A challenge password and An optional company name). To continue without entering these fields, just press Enter to accept the blank default for both inputs.

4. When you've finished entering your information, a file named server.csr will be created. If you're using Official Red Hat Linux Professional, server.csr will be located in the /etc/httpd/conf/ssl.csr directory. If you're using Official Red Hat Linux Professional, International Edition, server.csr will be located in /etc/httpd/conf. The server.csr file contains your certificate request, ready to be included in the enrolment web form

   When you insert the certificate request into the enrolment web form, be sure to get the entire text of the certificate, including the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- lines, but don't include any leading or trailing whitespace before the beginning and ending hyphens.
5. If you need more information, see the documentation included with your boxed set.

4 Installing your SSL Server Certificate

You will receive an email from the Registration Authority when your certificate request has been approved that contains a link to a location where your certificate may be obtained. Clicking on this link will bring up a browser window that contains the details of your issued certificate and includes a section that looks something like the following:

-----BEGIN CERTIFICATE-----
MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCAmowggHXA
hAF
UbM77e50M63v1Z2A/5O5MA0GCSqGSIb3DQEOBAUAMF8xCzAJBgNVBAYTAIVTMS
Aw
(.....)
E+cFEpf0WForA+eRP6XraWw8rTN8102zGrcJgg4P6XVS4l39+l5aCEGGbauLP5W6
K99c42ku3QrlX2+KeDi+xBG2cEIsdSiXeQS/16S36ITclu4AADEAAAAAAAAA
-----END CERTIFICATE-----

Copy everything you see **between and including** the lines that look like
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----

and paste it into an appropriately named text file e.g. **server.crt**

Copy this certificate file into the directory that you will be using to hold your certificates.

e.g. /etc/httpd/conf/ssl.crt/

In this example we will use:

- /etc/httpd/conf/ssl.crt/ as the location where certificates will be stored
- /etc/httpd/conf/ssl.key/ as the location where the server's private key is stored.
- /etc/httpd/conf/ca-bundle/ as the location where the CA bundle file will be stored

It is recommended that you make the directory that contains the private key file only readable by root.