SSL Certificate - Apache

Installation Guide

webnic
accelerate your business

Installation Instructions for Apache

Watch Symantec's Tutorial Videos for a more visual experience!

Video link: https://www.youtube.com/watch?v=naZpU6g2bEg

Note: If you are unable to view the video player, please click **here** to view from the video's web page.

Step 1: Install the SSL Certificate

1. The Symantec certificate will be sent by email.
2. Copy the certificate imbedded in the body of the email and paste it into a text file using Vi or Notepad.
   Do not use Microsoft Word or other word processing programs that may add characters.
   The text file should look like:

   -----BEGIN CERTIFICATE-----
   [encoded data]
   -----END CERTIFICATE-----

3. To follow the naming convention for Apache, rename the certificate filename with the **.crt** extension.
   For example: **public.crt**
4. Do the same for the Intermediate CA certificate, save the Intermediate CA certificate as **CA.crt**.
5. Copy the Certificate **[public.crt, CA.crt, domain.key** (convert the private key used for generating CSR into domain.key)**]** into the directory that you will be using to hold the certificates. In For example: **/usr/local/ssl/crt/**.

Step 2: Configure the Server

NOTE: Some instances of Apache contain both a **httpd.conf** and **ssl.conf file**. Please enter or amend the httpd.conf or the ssl.conf with the bellow directives. **Do not enter both** as there will be a conflict and Apache may not start.

1. In order to use the key pair, the **httpd.conf or ssl.conf** file will need to be updated.
2. In the Virtual Host section of the **httpd.conf or ssl.conf** file, verify that there are the following 3 directives within this Virtual Host.

   Please add them if they are not present:

   SSLCertificateFile /usr/local/ssl/crt/public.crt

   SSLCertificateKeyFile /usr/local/ssl/private/private.key

   SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt

   NOTE: Some versions of Apache will not acceptthe **SSLCertificateChainFile** directive. Try using **SSLCACertificateFile** instead.

   For example

```
#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile /usr/local/ssl/crt/public.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /usr/local/ssl/private/private.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt
```

   NOTE: The first directive tells Apache how to find the Certificate File, the second one where the private key is located, and the third line the location of the intermediate certificate.

If you are using a different location and certificate file names than the example above (which most likely you are) you will need to change the path and filename to reflect your server.

3. **Save** your **httpd.conf or ssl.conf** file and **restart** Apache. You can most likely do so by using the apachectl script:

   apachectl stop

   apachectl startssl

4. You should now be set to start using your Symantec certificate with your Apache-SSL Server.
5. To verify if your certificate is installed correctly, use the Symantec Installation Checker.

Apache-SSL

For more information, see the Apache Support website.