SSL Certificate – Covalent

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for Covalent Apache ERS v 2.4 or earlier

Installation Instructions for Covalent Apache ERS v 3.0 and above

Installation Instructions for Covalent Apache ERS v 2.4 or earlier

Step 1: Download the updated Symantec Intermediate CA certificate

1. Download the Root CA certificate for your SSL product.
   Copy the Intermediate CA certificate and paste it on a Notepad.
2. Save the file as intermediate.crt.
3. This file can be placed in the same directory as the SSL Certificate. For example**:**
   /usr/local/ssl/crt

Step 2: Obtain and Install the SSL Certificate

1. The Symantec certificate will be sent by email. If the certificate is included as an attachment (**Cert.cer**), you may use the file.
   If the certificate is imbedded in the body of the email, copy and paste it into a text file using Vi or Notepad.

   The text file should look like:

   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

2. To follow the naming convention for Apache, rename the certificate filename with the **.crt** extension. For example: **public.crt**
3. After you receive your signed Server Certificate, copy it to a temporary directory.
4. Select **Install CA Signed Certificate** from the Covalent SSL Certificate and Key Management Tool. You are prompted for the path to
   the temporary directory that contains the signed server certificate file. Covalent SSL installs the signed server certificate:
   - The signed server certificate is stored in the directory **/path/to/ssl1.5/certs**.
     Its name is the same as it was as a temporary server certificate,
     yourserver.domain.cert

(for example: www.covalent.net.cert).

NOTE: The process of signing your server certificate has no effect on your private key.

It is necessary and valid for its corresponding server certificate.

- The Private Key is stored in the directory **/path/to/ssl1.5/keys**

  Its name is yourserver.domain.key (for example: www.covalent.net.key).

6. In the Virtual Host settings for your site, in the **httpd.conf** file, you will need to add the following SSL directive:

   SSLCACertificateFile /path/to/ssl1.5//intermediate.crt

   NOTE: This directive specifies the location of the intermediate certificate. If you are using a different location or certificate file name than
   the example above (which most likely you are) you will need to change the path and/or filenames.

7. If your server is running, stop the server by executing: **/path/to/apache1.3/bin/covalent-faststart-ctl stop**
8. Start the server with Covalent SSL by executing: **/path/to/apache1.3/bin/covalent-faststart-ctl startssl**
9. During server start-up, you will be prompted to enter the pass phrase for the server certificate.
10. Back up the signed server certificate and store it with a backup of its corresponding private key.
11. Verify your installation with the Symantec SSL Certificate Checker.

Installation Instructions for Covalent Apache ERS v 3.0 and above

Watch a video demo to easily install an SSL Certificate on an Apache server

http://www.symantec.com/tv/products/details.jsp?vid=1452855338001

Step 1: Download the updated Symantec Intermediate CA certificate

1. Download the **Intermediate CA certificate** from here.
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as **intermediate.crt**.
4. This file can be placed in the same directory as the SSL Certificate. For example**:**
   /usr/local/ssl/crt

Step 2: Install the SSL Certificate

1. The Symantec certificate will be sent by email. If the certificate is included as an attachment (**Cert.cer**), you may use the file.
   If the certificate is imbedded in the body of the email, copy and paste it into a text file (save as **public.crt**) using Vi or Notepad.
   The text file should look like:

-----BEGIN CERTIFICATE-----

[encoded data]

-----END CERTIFICATE-----

2. To follow the naming convention for Apache, rename the certificate filename with the **.crt** extension. For example: **public.crt**
3. Copy the Certificate into the directory that you will be using to hold the certificates. In For example: **/usr/local/ssl/crt/**.

Step 3: 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 above 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 accept the **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. Verify certificate installation using the Symantec Installation Checker.