

Apache + Raven

Installing your Web Server Certificate

Your certificate will be sent to you by email. The email message includes the web server certificate that you purchased in the body of the email message.

Copy the certificate from the body of the email and paste it into a text editor (such as notepad) to create text files.

Start the Raven PKI Certificate Manager, using the command: `/usr/local/raven/bin/ravenctl`

1. Choose **Install CA Signed Certificate**
2. You will be prompted for the location of your web server certificate. Identify the location and the name (domainname.cert) of your web server certificate file. The certificate will be installed in the following directory:
`/usr/local/raven/module/pki/certs/`
3. Choose **Install CA Signed Certificate** using the Raven PKI Certificate Manager.
4. You will be prompted for the location of the Root Certificate. Identify the location and the name (geotrustca.cert) of the root certificate. The certificate will be installed in the following directory:
`/usr/local/raven/module/pki/certs/`
5. **Open** the `httpsd.conf` file in a text editor and ensure that the virtual host that you purchased the certificate for has the following directives and that they point to the correct files:
`SSLCertificateFile /usr/local/raven/module/pki/certs/domainname.cert`
`SSLCertificateKeyFile /usr/local/raven/module/pki/keys/domainname.key`
`SSLCACertificateFile /usr/local/raven/module/pki/certs/geotrustca.cert`
6. **Save the HTTPDS.CONF file.**
7. **Restart** the server: `/usr/local/apache/bin/httpsdctl restart`

Test your certificate by using a web browser to connect to your server. Use the https protocol directive (e.g. `https://your server/`) to indicate you wish to use secure HTTP.

Note: The padlock icon on your browser will be displayed in the locked position if your certificates are installed correctly and the server is properly configured for SSL.