SSL Certificate – Redhat

Installation Guide

webnic
accelerate your business

Installation Instructions for Red Hat Linux Secure Web Server

Step 1: Download and Install Intermediate CA Bundle Certificates

1. Download the Intermediate CA certificate.
   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. Save the Intermediate CA Certificate as: **/etc/httpd/conf/ssl.crt/intermediate.crt**.
5. Add the following directive to your **/etc/httpd/conf/httpd.conf file**, within the virtual host tags that define your secure Web server and with the other SSL directives:
   SSLCACertificateFile /etc/httpd/conf/ssl.crt/intermediate.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.
   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-----

2. To follow the naming convention for Red Hat, rename the certificate filename with the **.crt** extension. For example: **public.crt**
3. Save the certificate into a file and give the name and path to that file to the SSLCertificateFile directive:

   SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
4. You need to add also the key file in as well (SSLCertificateKeyFile directive).
   SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key

5. Remember to add the Intermediate file in as well (SSLCACertificateFile directive) from **Step 1**.

   SSLCACertificateFile /etc/httpd/conf/ssl.crt/intermediate.crt
6. Verify certificate installation using the Symantec Installation Checker.