

CSR Creation and Installation for WebHost Manager (WHM)

How to generate a CSR in WHM

1. The following instructions are for WHM 11. If you have a different version of WHM, you will go through a similar process but you may need to ask your web host for specific instructions.
2. Login to your WebHost Manager control panel.
3. On the left menu click on Generate a SSL Certificate and Signing Request.
4. In the Generate a New Certificate Signing Request section, enter the following information:
 1. Email - Your email address where the CSR will be sent.
Password - Make up a password to be associated with the certificate. You will need to remember this password later.

Host - The domain that you entered or selected when generating the private key.

City - The city in which your organization is located.

State - The state in which your organization is located. Do not use an abbreviation.

Country - If needed, you can find your two-digit [country code](#) in our list.

Company Name - The legally registered name of your organization/company.

Company Division - The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).
5. Click the Create button.
6. Copy and paste the entire CSR (including the BEGIN and END lines) into text file and [submit to us](#).

Installing your WebHost Manager (WHM) SSL Certificate

The following instructions are for WHM 11. If you have a different version of WHM, you will go through a similar process but you may need to ask your web host for specific instructions.

1. Login to your WebHost Manager (WHM) control panel.
2. On the left menu, click on Install a SSL Certificate and Setup the Domain.
3. In the first box, you will need to paste the contents of your Primary Certificate (yourdomain.crt) that you received. To access the text version of your certificate, open it with a text editor. When copying and pasting your certificate, include the BEGIN and END tags.
4. Fill in the required Domain / User / IP address information. The domain and IP address may fill in automatically. Type your WHM username in the User field.
5. In the middle box you will need paste the correct RSA private key that was generated with the CSR. This private key was sent to your email address when you generated your CSR. The private key may fill in automatically if the server recognizes your Certificate or if you click the Fetch button.
6. In the bottom box you will need to paste the contents of the Intermediate Certificate.
7. Press the Do it button. Your SSL Certificate should now be installed, and the website configured to accept secure connections. You or your web host may need to restart Apache before it will work.

****Note:** If your "Do it" button is not active, try clicking the Fetch button for the private key only. This will activate the "Do it" button. DO NOT click the fetch button that corresponds to the Certificate itself. If you do this, the certificate will be replaced with an invalid self-signed certificate.

Manual Intermediate Certificate Installation

If the Intermediate certificate was not correctly installed using the above instructions you may need to install it directly in Apache. If you do not have access to the Apache configuration files you will need to have your web host or administrator follow these instructions to install the Intermediate certificate:

1. Locate the Virtual Host File:
2. On most Apache servers the Virtual Sites are configured in the `/etc/httpd/conf/httpd.conf` file. However, the location and name of this file can vary from server to server -- Especially if you use a special interface to manage your server configuration. Another common name for the file is `'SSL.conf'`. If you open the file with a text editor, you will see the configurations for the virtual hosts that are housed on the server. The virtual host configurations are probably found near the end of the file.
3. Identify the secure Virtual Host for your site:
4. Locate the Virtual host configuration for the site you are securing. It will have the proper name and IP address (including port 443).
5. Configure the Virtual Host For SSL:
 - a. WHM has already setup the first three SSL configuration lines for you. Now you will edit your Virtual Host configuration by adding the `'SSLCertificateChainFile'` line below (this line is bolded).

```
<VirtualHost 192.168.0.1:443>
DocumentRoot /var/www/html2
ServerName www.yourdomain.com
SSLEngine on
SSLCertificateFile /etc/ssl/crt/your_domain_name.crt
SSLCertificateKeyFile /etc/ssl/crt/your_private.key
SSLCertificateChainFile /etc/ssl/crt/IntermediateCA.crt
< /VirtualHost>
```

Of course, the path and names of your certificate files may be different. When typing the path for your `SSLCertificateChainFile`, type the path and filename you plan to use when saving your intermediate certificate. It is generally advised to save your intermediate certificate in the same directory that WHM already saved your primary certificate to.
6. Save the changes to your configuration file.
7. Save the Intermediate Certificate file to the Server:
8. Verify that the Intermediate Certificate file is saved to the path you configured above.
9. Restart Apache.