# SSL Certificate – WHM11.x

## Installation Guide

webnic
accelerate your business

# SSL Certificates CSR Creation in WHM

## CSR Creation for WebHost Manager (WHM) SSL Certificates

If you already have your SSL Certificate and just need to install it, see WHM SSL Certificate Installation.

### How to generate a CSR in WHM

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 control panel.
2. On the left menu click on **Generate a SSL Certificate and Signing Request**.
3. In the **Generate a New Certificate Signing Request** section, enter the following information:

   **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 enetered or selected when generating the private key.

   **City** - The city in which your organization is located.

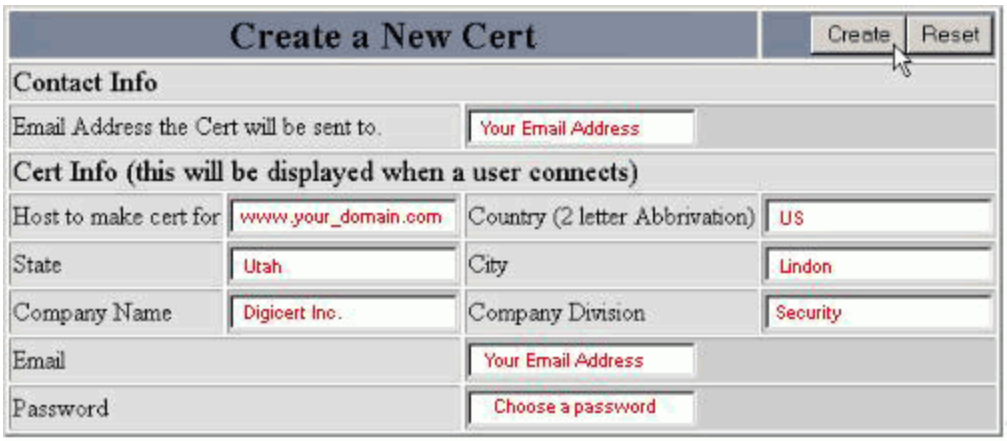
   **State** - The state in which your organization is located. Do not use an abbreviation.

   **Country** - If needed, you can find your two-digit country code in this 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).

4. Click the **Create** button.



5. Copy and paste the entire CSR (including the BEGIN and END lines) into the DigiCert order form.
6. After you receive your SSL Certificate from DigiCert, you can install it.

# WHM SSL Certificate Installation

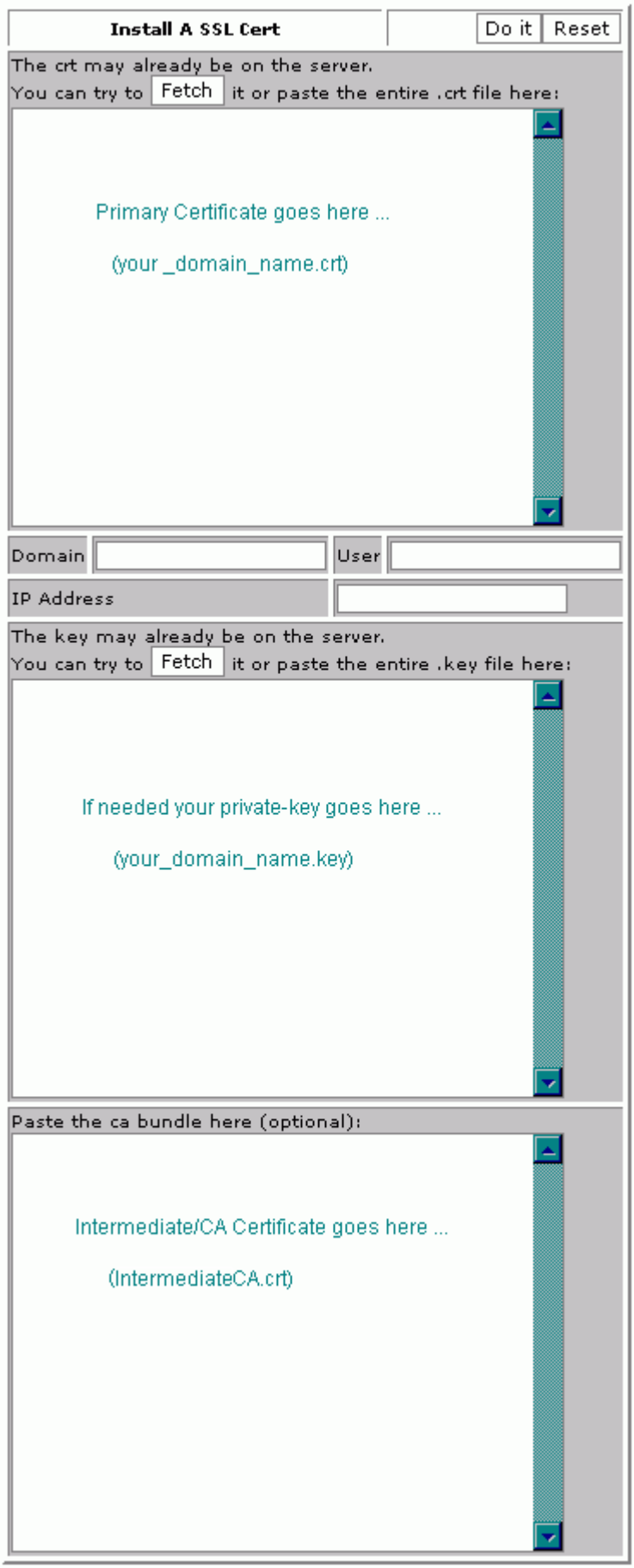
## SSL Certificate Installation in WebHost Manager

If you have not yet created a Certificate Signing Request (CSR) and ordered your certificate, see SSL Certificates CSR Creation in WHM.

### 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. Download your Intermediate and Primary Certificate files from your Certificate Issuer to the directory where you will keep your certificate and key files.
2. Login to your WebHost Manager (WHM) control panel.
3. On the left menu, click on **Install a SSL Certificate and Setup the Domain**.
4. In the first box, you will need to paste the contents of your Primary Certificate (yourdomain.crt) that you downloaded from DigiCert. 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.
5. 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.
6. 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.
7. In the bottom box you will need to paste the contents of the Intermediate Certificate (intermediateCA.crt).


Install A SSL Cert
Do it
Reset
The crt may already be on the server.
You can try to
Fetch
it or paste the entire .crt file here:
Primary Certificate goes here ...
(your _domain_name.crt)
Domain
User
IP Address
The key may already be on the server.
You can try to
Fetch
it or paste the entire .key file here:
If needed your private-key goes here ...
(your_domain_name.key)
Paste the ca bundle here (optional):
Intermediate/CA Certificate goes here ...
(IntermediateCA.crt)

8. 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:

   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.

2. Identify the secure Virtual Host for your site:

   Locate the Virtual host configuration for the site you are securing. It will have the proper name and IP address (including port 443).

3. Configure the Virtual Host For SSL:

   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.

4. Save the changes to your configuration file.
5. Save the Intermediate Certificate file to the Server:

   Verify that the Intermediate Certificate file (DigiCertCA.crt) is saved to the path you configured above.

6. Restart Apache.

# Troubleshooting:

1. If your web site is publicly accessible, SSL Certificate Tester tool can help you diagnose common problems.
2. Open a web browser and visit your site using https. It is best to test with both Internet Explorer as well as Firefox, because Firefox will give you a warning if your intermediate certificate is not installed. You should not receive any browser warnings or errors. If you immediately receive a browser message about the site not being available, then Apache may not yet be listening on port 443. If your web request takes a very long time, and then times out, a firewall blocking traffic on TCP port 443 to the web server.

   If you receive a "not trusted" warning, view the certificate to see if it is the certificate you expect. Check the Subject, Issuer, and Valid To fields. If the certificate is issued by DigiCert, then your SSLCertificateChainFile is not correctly configured.