Installing an SSL certificate on your server

Contents

Introduction

There are a number of steps in adding a digitally signed certificate. This guide assumes that you have already Created a Certificate Signing request, and have now received your new signed certificate.

Once this is complete, you can add the certificate to your server and set up secured connections on your website.

Preparing your certificate

Once you have received your signed certificate by email you should copy and paste it into a text editor, such as Notepad or Vi.

> **Quick tip:** Ensure that you copy the certificate into a text editor. Word Processors such as Microsoft Word will add hidden formatting characters that will stop your certificate from working when installed on your server.

Your certificate should take the following format:

```
----- BEGIN CERTIFICATE -----
Code
 ----- END CERTIFICATE -----
```

Check that there are 5 dashes to either side of BEGIN CERTIFICATE and END CERTIFICATE and that no whitespace, extra line breaks of additional characters have been added during the copy and paste process.

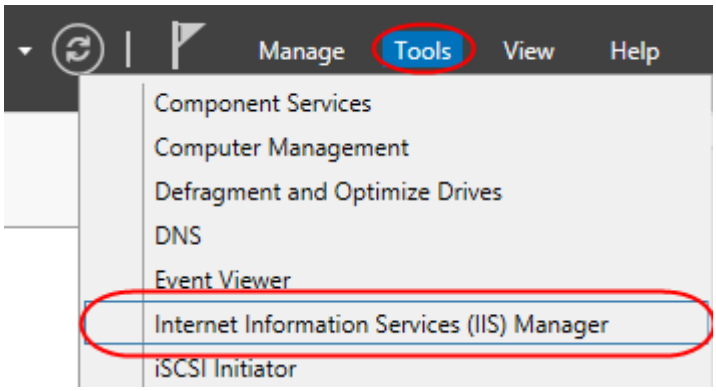
Save the certificate as a .crt file and upload this file to your server. Make a note of the certificate name and location as you will need this when you install your certificate.

Installing your Certificate

IIS 8

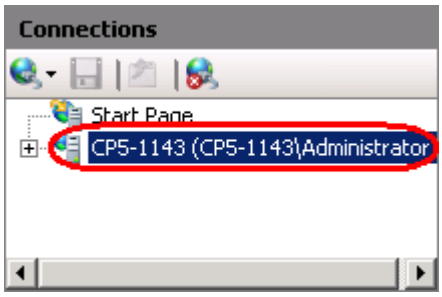
Step 1

From within *Server Manager* select *Internet Information Services (IIS) Manager* from the *Tools* drop-down menu.



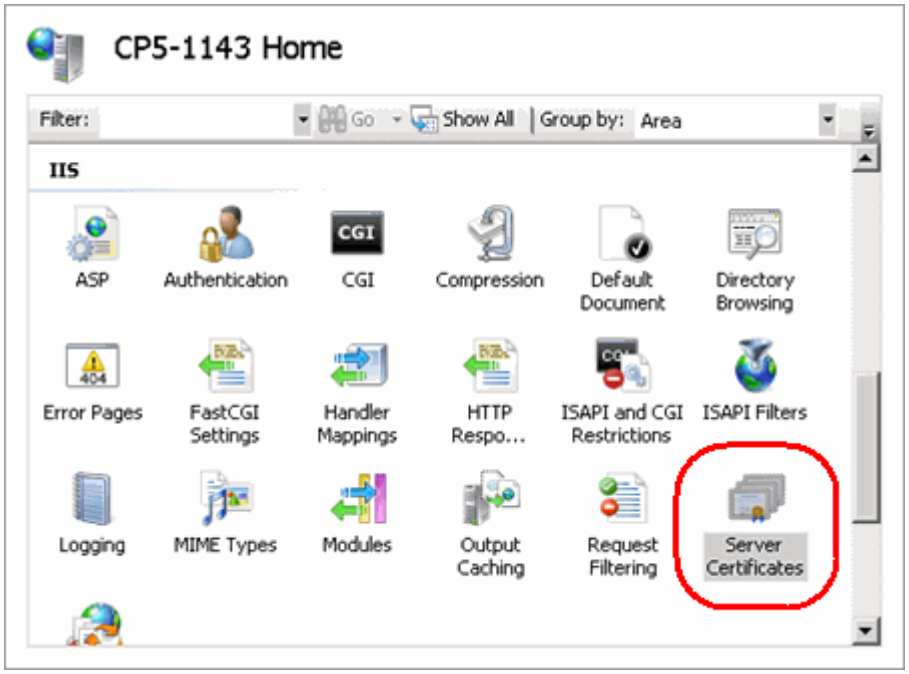
Step 2

In the IIS Manager, choose your server name.



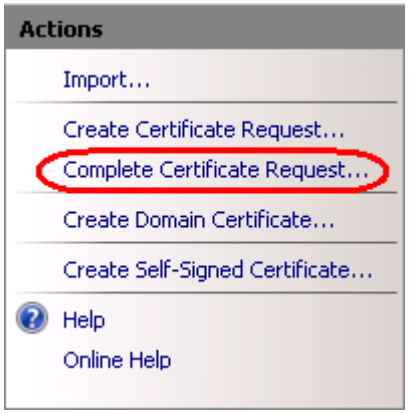
Step 3

Select the **Server Certificates** icon. This will be located in the *IIS* section, or the *Security* section, depending upon how you are grouping your icons.



Step 4

In the right hand *Actions* pane, click **Complete Certificate Request**.



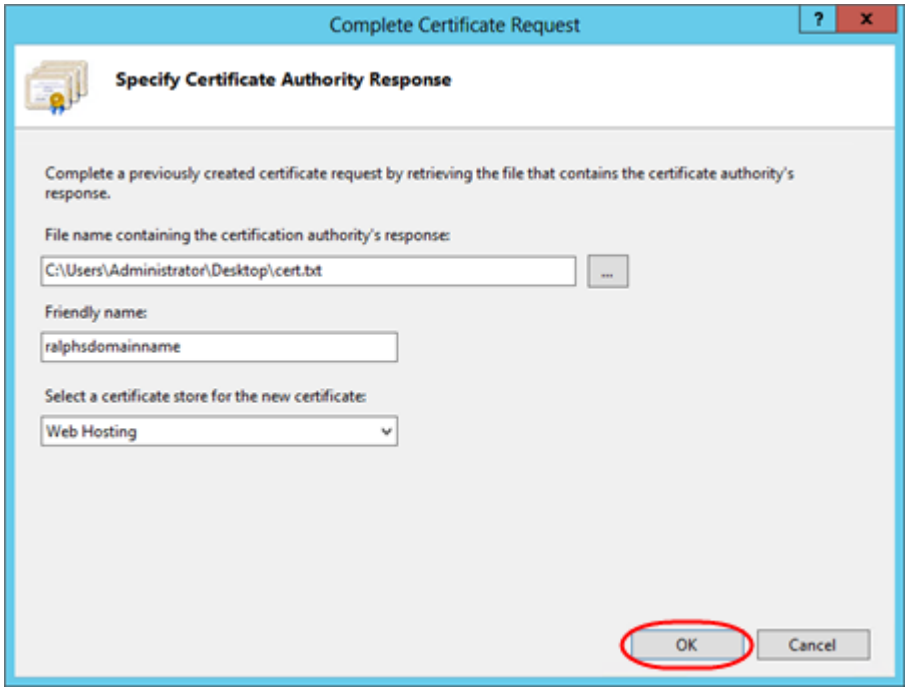
Step 5

In the text boxes provided, enter the path to your new certificate, enter a friendly name and chose a certificate store for this certificate.

Quick tip: The friendly name allows you to quickly identify the certificate. You can choose any name you like.

Step 6

Once done, click **OK**.



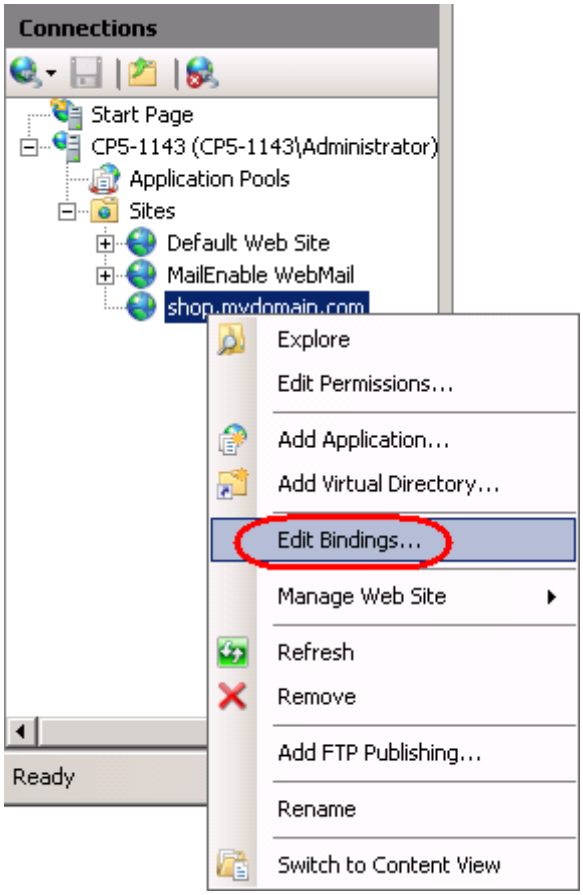
Associating your certificate with your website

Step 1

Leaving IIS open, and using the left hand Connections pane, right click on the website you want to add SSL to.

Step 2

Then click **Edit Bindings**.

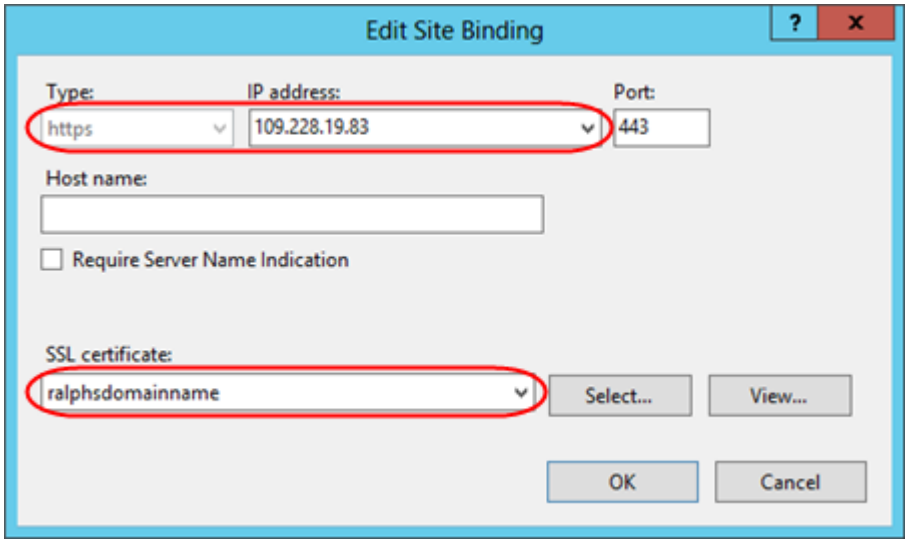


Step 5

A list of your bindings will appear. Click the **Add** button to add a new binding.

Step 6

In the Bindings window select the binding type as https, select an IP address for the secure site to use and select the certificate to be used with the site.



Step 7

Once done, click **OK**.

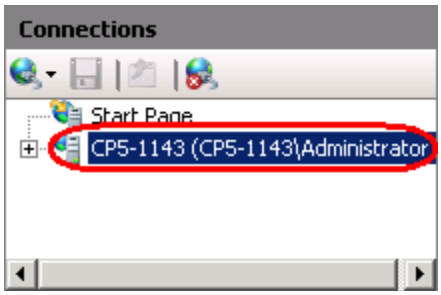
IIS 7

Step 1

Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

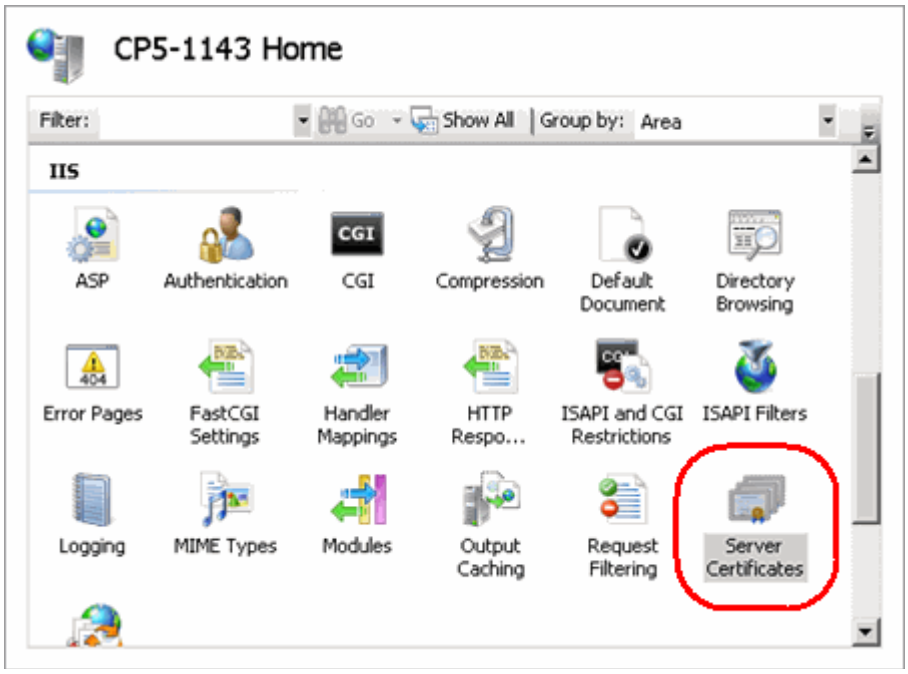
Step 2

In the IIS Manager, choose your server name.



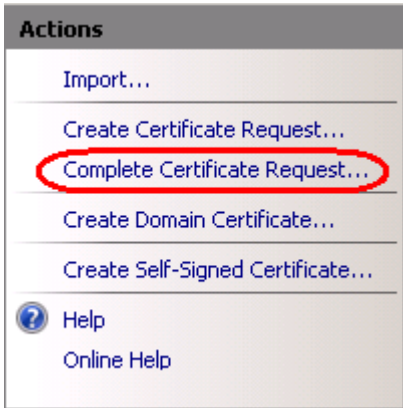
Step 3

In the *Features* pane (the middle pane), open the **Server Certificates** icon. This will be located in the IIS section, or the Security section, depending upon how you are grouping your icons.



Step 4

In the right hand *Actions* pane, click **Complete Certificate Request**.



Step 5

In the text boxes provided, enter the path to your new certificate, and enter a friendly name for this certificate.

The friendly name allows you to quickly identify the certificate. You can choose any name you like.

Oncde done, click **OK**.

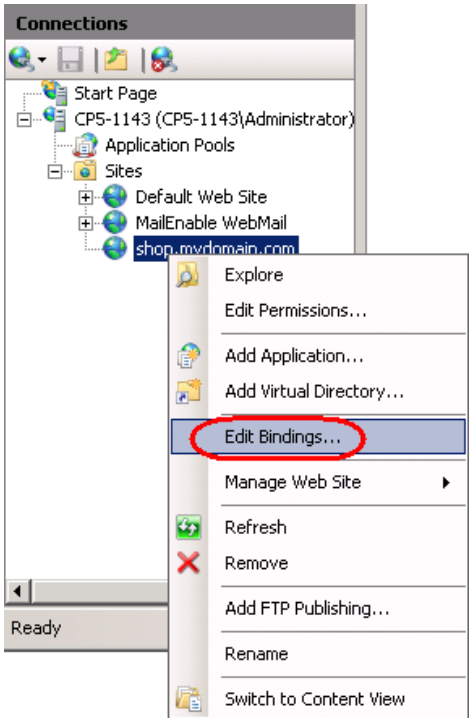
Associating your certificate with your website

Step 1

Leaving IIS open, and using the left hand Connections pane, right click on the website you want to add SSL to.

Step 2

Then click **Edit Bindings**.



Step 3

A list of your bindings will appear. Click the **Add** button to add a new binding.

Step 4

In the Bindings window select the binding type as **https**, then select the certificate to be used with the site.

Step 5

Once done, click **OK**.

Apache

Step 1

Open the *httpd.conf* or file on your server and locate the Virtual Host settings. There should be two directives within these settings. Edit these to match the location of the key parts on your server.

SSLCertificateFile should point towards the location of your newly signed public key. For example:

SSLCertificateFile /usr/local/*ssl*/crt/public.crt

SSLCertificateKeyFile should point towards your private key file. For example:

SSLCertificateKeyFile /usr/local/*ssl*/private/private.key

> **Note:** Alternatively you can paste the contents of your newly generated certificate into the **Certificate** text box under the *Upload certificate as text section*, and click the **Send File** button.

Step 2

Restart the *Apache* service, the commands to do this will be different depending on the Linux OS your server is running.

CentOS

```
service httpd stop
service httpd start
```

Ubuntu

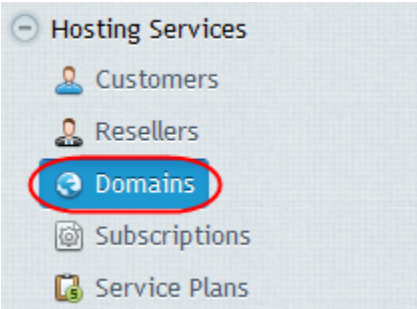
```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
```

Should Apache fail to restart you should check the Apache error logs for further information on the problem.

Plesk 12

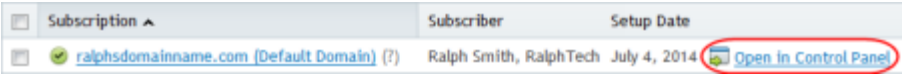
Step 1

Log in to Plesk on your server as the server administrator and click on **Domains** in the *Hosting Services* menu.



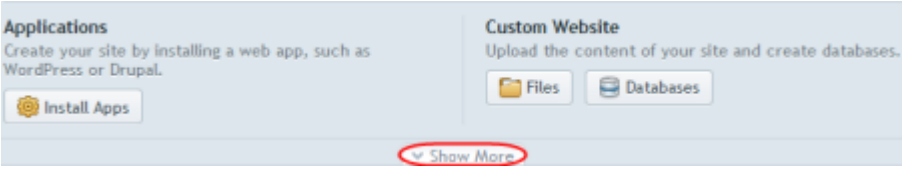
Step 2

Click on the *Open in Control Panel* link next to the domain name you want to add the *SSL* certificate to.



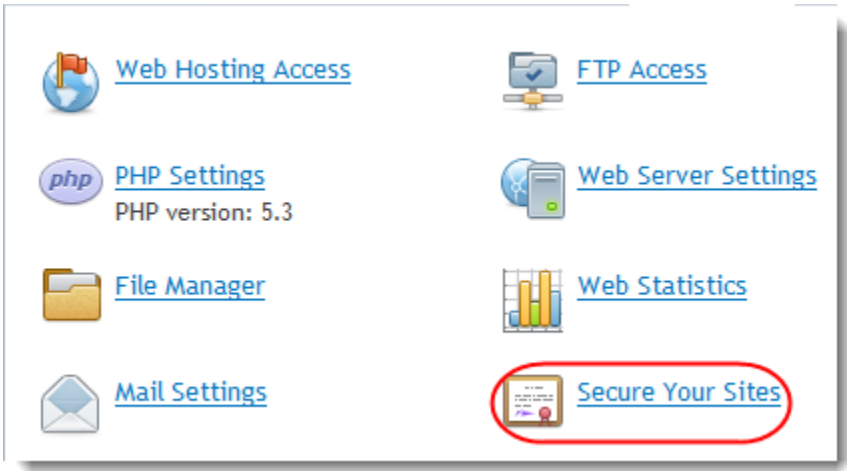
Step 3

Click the **Show More** button at the bottom of the *Websites & Domains* section.



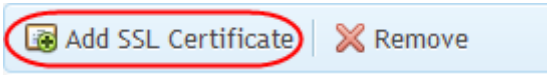
Step 4

Click on the **Secure Your Sites** icon.



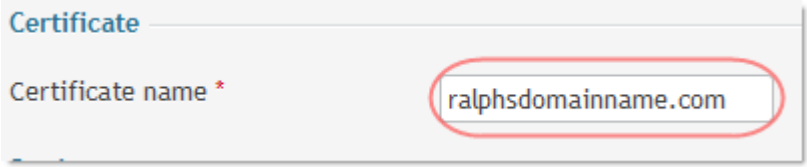
Step 5

Click the **Add *SSL* Certificate** icon.



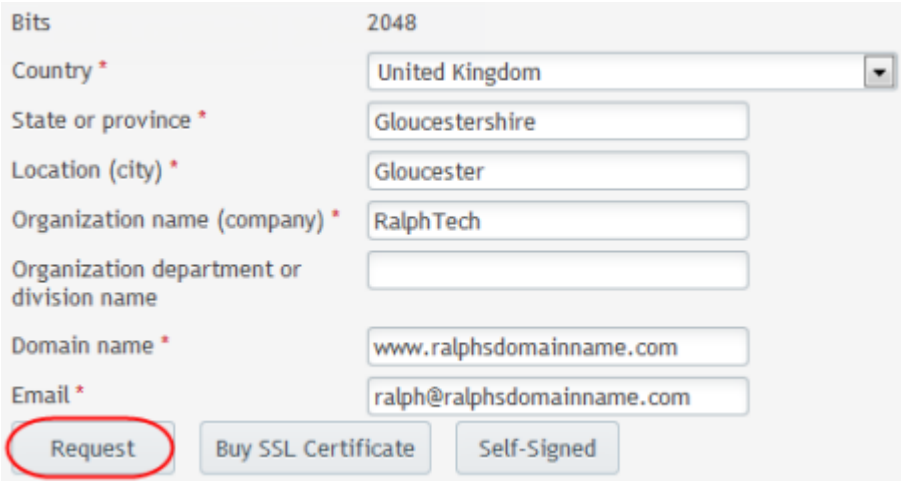
Step 6

Enter a **Certificate Name** to help you identify this certificate. In the example below we've named it after the domain name the certificate is for, to make it quickly and easily identifiable.



Step 7

You also need to enter your company address, the domain name the certificate will protect, and a valid email address. These details must be accurate as they will be used to generate your private key.



Click the **Request** button when you've entered the information. You'll see a confirmation message that the certificate has been created.

Step 8

Locate the newly created certificate in the list and click on it to see it's properties. Scroll down and find the CSR section. Copy all the text that starts with:

-----BEGIN CERTIFICATE REQUEST-----

and ends with

-----END CERTIFICATE REQUEST-----

CSR


```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5TCCAc0CAQAwgZ8xCzAJBgNVBAYTAkdCMRgwFgYDVQQIEw9HbG91Y2VzdGVy
c2hpcmUxEzARBgNVBAcTCkdsb3VjZXN0ZXIxEzARBgNVBAoTC1JhbHBoIFRlY2gx
ITAfBgNVBAMTGHd3dy5yYWxwaHNkb21haW5uYW11LmNvbTEpMCcGCSqGSIb3DQEJ
ARYacmFscGhAcmFscGhsZG9tYWlubmFtZS5jb20wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCqjdDlQ/zNXqRvcYsgPiQt0662oJ2ea412KXfiJQKYB22e
HpBLJXm5njzwHrPcve+N55r92NplM7f3e/KAEKbGGCoEvAyaxRmNANC/tTvHDIOv
Yy9HhaHpxGZ6zEGI1btFLWwFnw6DyORkmxVPdI5kOWH0FQsoaZzvTvyAK01R1Dp8
/X4G8f1evdDQj3xR79TM3hz9JirhuBh8qJIp9ZZG8UPhadXW8kQRouDRo4VikYU4
bWDcPLQHmqNXR4ZF7Xv4PW6GW5JRZex3YIsKg09scPRDzYXj+pN66qqOHOjyjF0O
W1i1wd6aqHX2gZavN+QnKMRZ16JVnx4uVmLboVozAgMBAAGgADANBgkqhkiG9w0B
AQUFAAOCAQEAO7xDoS63QJxN8auw8y21UGzV1GgQfXrHObtBweWAKAzcuEQGI9tG
Ay31OCIalvxMoHGGqNBR87dMwKswz69vhiUhJpQ3HX/Pus3NnIx1OT3W8caK4uE6
pBfKfwCC1Huy5ZhHgbNR8wi3Z1LqXo5/1BUEhyshBguT1eNd4o5/RcIU48UzyKIb
ykozYJ7dIolDAuUOy9aOYA2GGloFibuIK08r2xaD3NfvKk3Ku7OzfkMCQdojs0p+
HrDWPRTwUFtzk/XuUCkJmJoEnUs2evSNj47edd/xDy/JfqMeO98Kog5sarem1cRU
O1/+8TbX8z2KZW81dVp0LofddIHR+c1nig==
-----END CERTIFICATE REQUEST-----
```


Step 9

Visit the web site of your chosen certificate authority and follow their procedures to purchase your certificate. When prompted, paste the CSR text you copied in the previous step into their online form. They will then generate your certificate. Save the generated certificate file to your local machine.

Step 10

Select the *Websites & Domains* tab, and click the ***SSL* Certificates** icon to go back to the *SSL* certificates list. Click on the certificate you just created in the list to view it's properties again.

Step 11

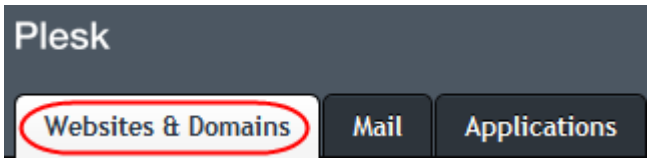
Under the *Upload certificate files* section, click the **Browse** button by the **Certificate** text box and locate the file you just saved to your machine from the certificate authority.

Click the **Send File** button to upload the certificate to your server.

Note: Alternatively you can paste the contents of your newly generated certificate into the **Certificate** text box under the *Upload certificate as text section*, and click the **Send File** button.

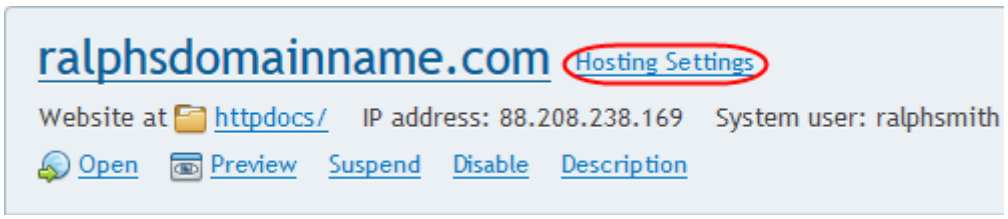
Step 12

Select the **Websites & Domains** tab at the top of the page.



Step 13

Click the *Hosting Settings* link next to your domain name at the top of the page.



Step 14

This will bring up the *Hosting Settings* for the domain. Tick the box labelled *Enable SSL support* and select the certificate from the dropdown menu.

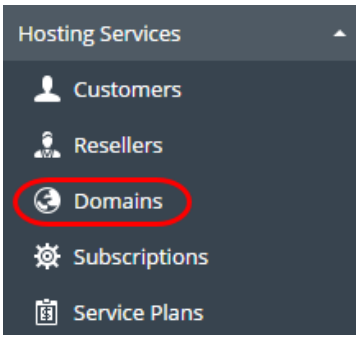
Click **OK** at the bottom of the page to apply the settings.

Quick tip: The CA part of the certificate is optional but it is useful to have for cross-browser compatibility. You can download the Intermediate CA and Root CA from Symantec.

Plesk Onyx

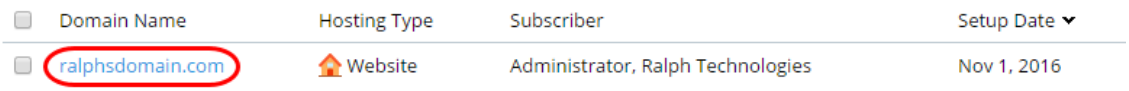
Step 1

In the Plesk control panel, select Domains from the *Hosting Services* section within the left menu bar.



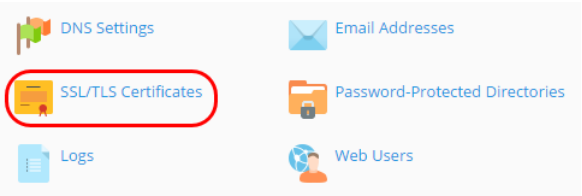
Step 2

Click on the domain you wish to add the certificate to.



Step 3

Select the **SSL/TLS Certificates** icon.

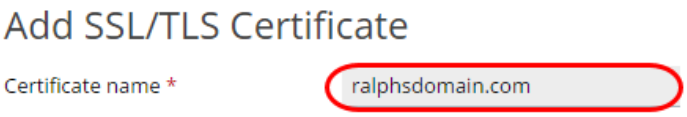


Step 4

Click on the **Add SSL/TLS Certificate** icon.

Step 5

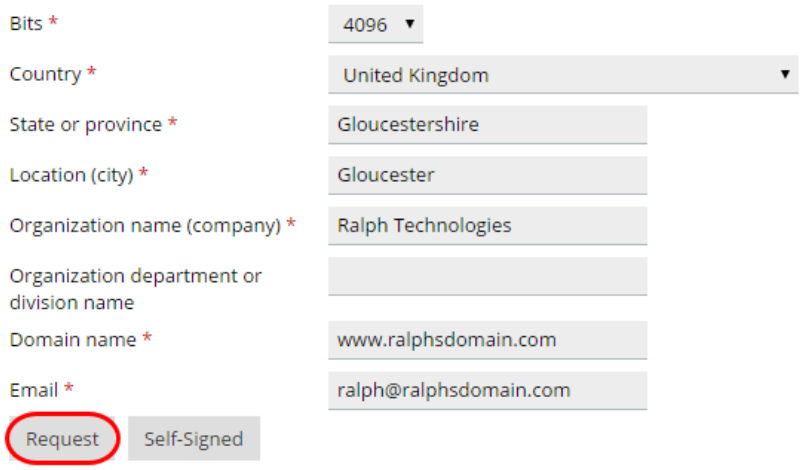
Enter a **Certificate Name** to help you identify this certificate. In the example below we've named it after the domain name the certificate is for, to make it quickly and easily identifiable.



Step 6

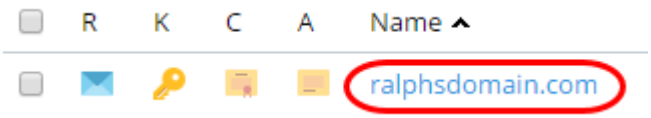
You also need to enter your company address, the domain name the certificate will protect, and a valid email address. These details must be accurate as they will be used to generate your private key.

After the details have been filled in click the Request button.



Step 7

You will be directed back to the **SSL Certificates** section. From here you will need to click on the certificate that has just been created.

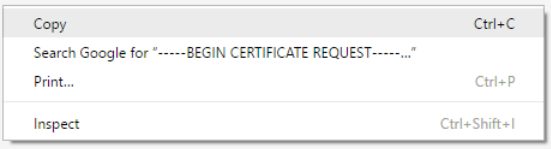


Step 8

Copy the entire CSR part from where the text starts with **-----BEGIN CERTIFICATE REQUEST-----** to where it ends with **-----END CERTIFICATE REQUEST-----** save this to a notepad file.

CSR


```
-----BEGIN CERTIFICATE REQUEST-----
MIIE5TCCAs0CAQAwgZ8xCzAJBgNVBAYTAkdCMRgwFgYDVQQIEw9HbG91Y2VzdGVy
c2hpcmUxEzARBgNVBAcTCkdsb3VjZXN0ZXIxGzAZBgNVBAoTElJhbHBoIFRlY2hu
b2xvZ2llczEdMBsGA1UEAxMUd3d3LnJhbHBoc2RvbWFpbi5jb20xJTAjBgkqhkiG
9w0BCQEWFnJhbHBoQHJhbHBoc2RvbWFpbi5jb20wggIiMA0GCSqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQC+mH9KX6Vn6eMe4Lwf7Z9XK9c5Z3D5Nb/bEoaGUpjuKvhM
G/gmb41C9L6NUAitNa+OQBByTCO8QWciHDUj8N5STp72+ID1vFzN4B/UbJnF25Zo
cgGiBDcVOiifpEnD0ugE/SmSRg3QEwbXaZkK1KJdTAZcwJ1kehlWXGSqjpsFSheh
CG2rqcBSWO0aYvHSiY1yMuY2LinrLO4rmoA1y2DILhEqqkF185BMsPrfz9G8uKwq
+GR53XjWt8goZQQ8uqLP4BMhfrJBHzp7sX1bGn2nymn25Rz1Ga44tHp8vYOgM4z3
QFkt6CipuH7xjFf6gJcVeYkuMU3LK7ny/bnbICAN6sB7wD03y5bM/M7ItWuKbezU
f4omu/dyDQPMte2SjMJf3qHItnFm4XAhhq9G2O77GZzt3ejmamNCse5OTQQVI0w8
DR8EMGW8H5QHuYAYqqyIFb5rPfub+bo7KBekB0sXG5swWhsdnEcOr3T50p75o/6D
gk+clGUR/ZAh9q503ImBr/ypGd+5h/0u/e7EQXb/LJXwf79q25tbG9KqN1j1qnTP
bbGzrHVQh/VG/Qhx2e9jpByLveC4q4PMcYFSuHxGvM21HsvFvIvctiVdsx6VhPMi
6bDWgMLeWLX1
-----END CERTIFICATE REQUEST-----
```

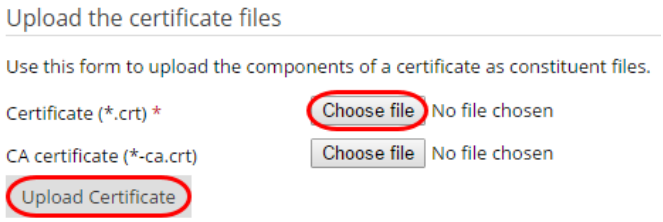



Step 9

You will need to provide this to your chosen certificate authority (the company you are purchasing your SSL certificate from). They will then provide you with at the certificate part to upload to Plesk.

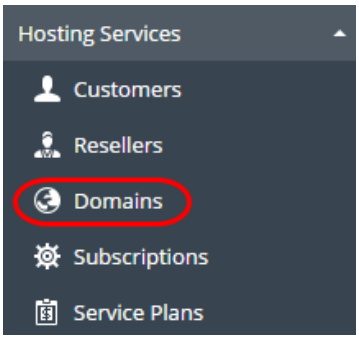
Step 10

Once you have the certificate part from your provider, click the Choose file button and find the certificate file on your computer. Once you have located it, click the Upload Certificate button.



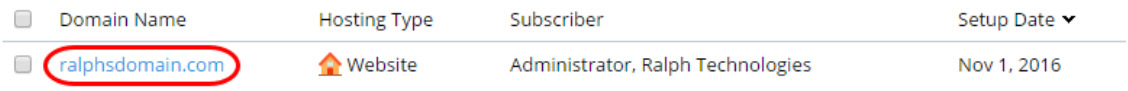
Step 11

Select the Domains from the *Hosting Services* section within the left menu bar.



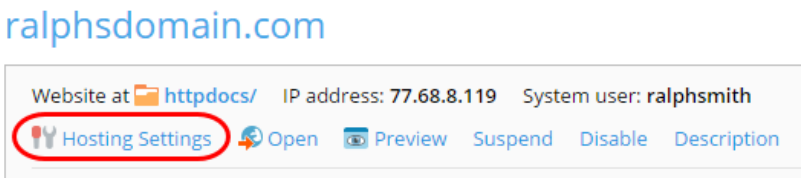
Step 12

Click the domain you wish to apply the certificate to.



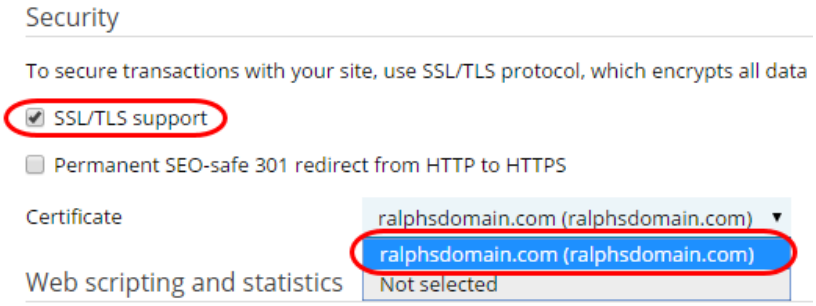
Step 13

Click **Hosting Settings** on the domain overview.



Step 14

This will bring up the *Hosting Settings* for the domain. Tick the box labelled *Enable SSL support* and select the certificate from the dropdown menu.



Quick tip: The CA part of the certificate is optional but it is useful to have for cross-browser compatibility. You can download the Intermediate CA and Root CA from Symantec.

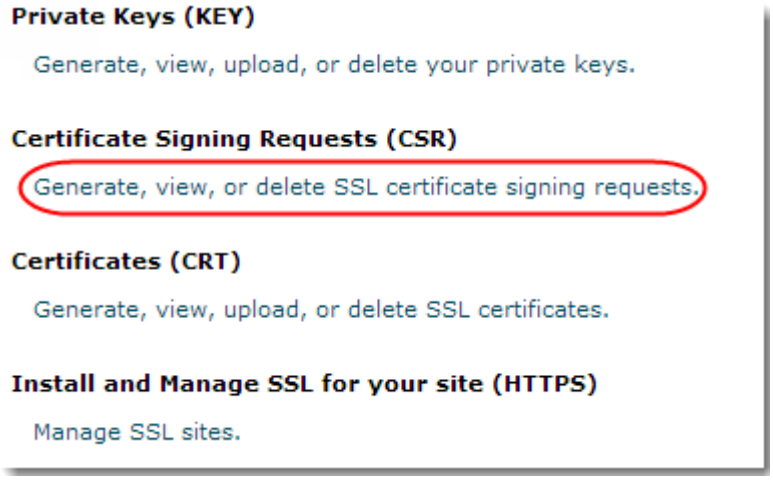
cPanel

Step 1

Log in to cPanel, scroll down to the *Security* section and click the **SSL/TLS Manager** icon.

Step 2

Click the link *Generate, view or delete SSL certificate signing requests*.



Step 3

Fill out the CSR form using the fields provided.

- **Key**: Leave this field set at *Generate a new 2,048 bit key*.
- **Domains**: Enter the domain name that you want to add *SSL* to.
- **City**: Enter the City that the domain's registrant details contain.
- **State**: Enter the State or County that the domain's registrant details contain.
- **Country**: Select the domain registrant's country from the dropdown menu.
- **Company**: Enter your company name.
- **Company Division**: Enter the division within your company.
- **Email**: Enter the domain registrant's email address.
- **Passphrase**: Enter a passphrase (optional).
- **Description**: Enter a description (optional).

Step 4

Copy the entire Encoded Certificate Signing Request from the start of the line reading:

-----BEGIN CERTIFICATE REQUEST-----

To the end of the line reading:

-----END CERTIFICATE REQUEST-----

Paste this into a notepad file for safe keeping.

Step 5

You will need to provide this to your chosen certificate authority (the company you are purchasing your *SSL* certificate from). They will then provide you with the certificate part to upload to cPanel. Paste this into a notepad file for safe keeping.

Step 6

Once you have the gained the CRT from your certificate authority, copy the entire certificate from the start of the line reading:

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

To the end of the line reading:

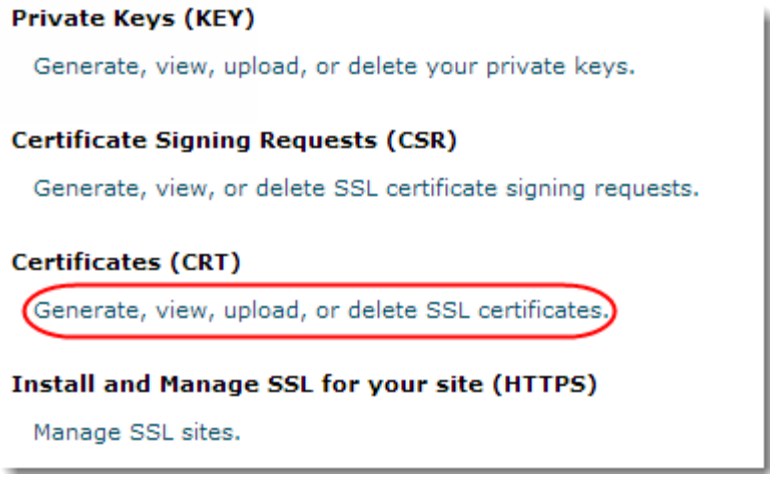
-----END CERTIFICATE-----

Step 7

Scroll down to the *Security* section and select the ***SSL*/TLS Manager** icon.

Step 8

Click the link *Generate, view, upload or delete SSL certificates*.



Step 9

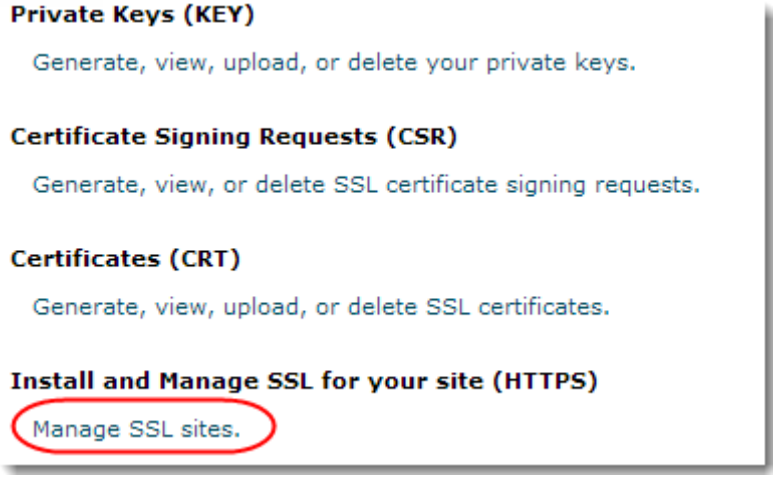
Paste your certificate into the box labelled *Paste your certificate below* and click **Save Certificate**.

Step 10

Scroll down to the *Security* section and select the ***SSL*/TLS Manager** icon.

Step 11

Click the link *Manage SSL Sites*.

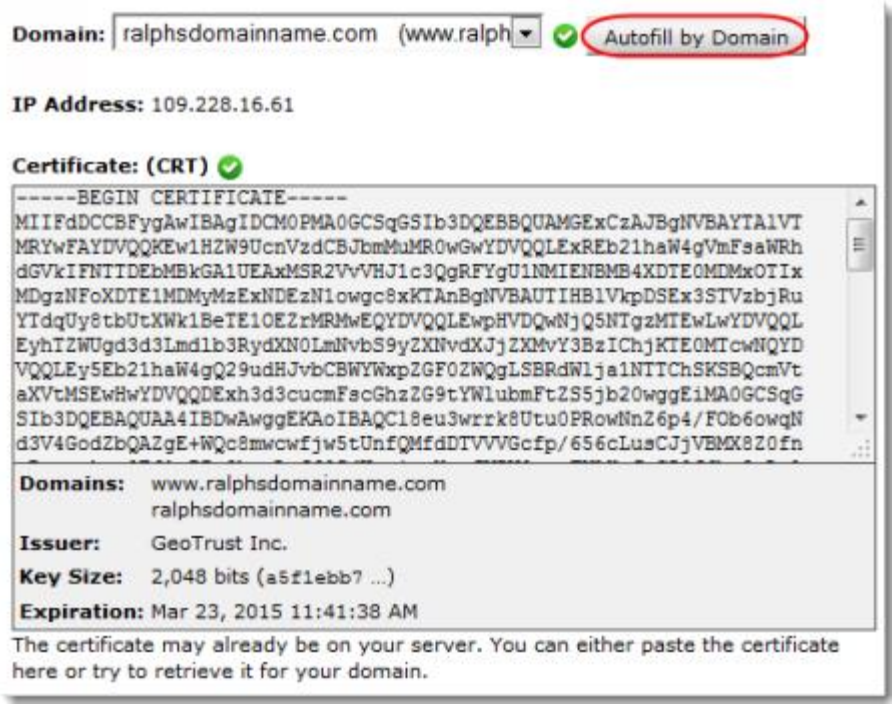


Step 12

Scroll down the page and from the *Domain* drop down menu select the domain name that you want to install the *SSL* certificate on.

Step 13

Click the button that appears labelled **Autofill by Domain**. This will automatically fill in all the key parts for the domain that were installed in previous steps.



Step 14

Scroll to the bottom of the page and click the **Install Certificate** button.

A confirmation screen will appear, click the **OK** button to finish the *SSL* installation.