

Installing an SSL certificate

254 Keira Tait Tue, Feb 11, 2020 [Shared Hosting](#) 1165

Note: You will need to ensure you have one of the following email addresses configured on your mail server as the certificate authorisation will be sent to one of the following of your choice

admin@yourdomain.co.uk
administrator@yourdomain.co.uk
hostmaster@yourdomain.co.uk
webmaster@yourdomain.co.uk
postmaster@yourdomain.co.uk

1. First of all before the order process you need to generate the CSR which can be done by following the below steps
2. Sign into your Plesk control panel (contact support if you are unaware of your login) and navigate the below, note for other vendors please use - <https://knowledge.digicert.com/solution/SO6506.html>
3. **Domains > example.com > SSL Certificates**, fill in the required fields and click **Request**. Such certificate will be Self-Signed and not valid for checks.
4. Go to **Domains > example.com > SSL/TLS Certificates**.
5. Once you have the CSR, email the CSR and your SSL requirements to sales@ic.co.uk
6. **Domains > example.com > SSL Certificates**, fill in the required fields and click **Request**. Such certificate will be Self-Signed and not valid for checks.
7. Go to **Domains > example.com > SSL/TLS Certificates**.

Note: If you are using the SSL It! extension, click **Advanced Settings**.

8. On the **SSL/TLS Certificates** page, add your certificate:

Note: If you are experiencing issues with a certificate installation, contact your certificate seller and ask for certificate installation instructions for Plesk.

- If an SSL certificate is stored in a single *.crt file:

Click **Browse...** to select a certificate file. Then click **Upload Certificate**.

The screenshot shows a web interface for managing SSL/TLS certificates for the domain 'example.com'. At the top, there is a breadcrumb 'Home / Domains' and a title 'SSL/TLS Certificates for example.com' with a dropdown menu. Below the title, there is a text block explaining the process of uploading a certificate. A section titled 'Upload the certificate here' contains a file input field labeled 'Certificate (*.crt) *' with a 'Browse...' button and the text 'No file selected.'. Below this is a prominent blue 'Upload Certificate' button. At the bottom of the section, there are four buttons: '+ Add SSL/TLS Certificate', 'View Certificates', 'Secure Webmail' (with a lock icon), and 'Remove' (with an 'X' icon). A search bar is located to the right of these buttons. The main content area below the buttons is empty, displaying 'No items found.'

If an SSL certificate is stored in the form of *.key and *.crt files:

Click **Add SSL/TLS Certificate** and scroll down to the **Upload the certificate files** section and upload these files. If both the certificate and the private key parts of your certificate are contained in a *.pem file (you can check it by opening the *.pem file in any text editor), just upload it twice, both as the private key and the certificate. Click **Upload Certificate** once finished.

Upload the certificate files

Use this form to upload the components of a certificate as constituent files.

Private key (*.key) *

Browse...

No file selected.

Certificate (*.crt) *

Browse...

No file selected.

CA certificate (*.ca.crt)

Browse...

No file selected.

Upload Certificate

#

If an SSL certificate is stored as a text:

Click **Add SSL/TLS Certificate** and scroll down to the **Upload the certificate as text** section. There, paste the certificate and the private key parts into the corresponding fields. Click **Upload Certificate** when you have finished.

Upload the certificate as text

Use this form to upload the components of a certificate as text. Copy the contents of a file and paste into the corresponding field.

Private key (*.key) *

```
-----BEGIN RSA PRIVATE KEY-----
MIIEKQIBAAKCAgEA3W29+ID6194bH6ejLrIC4hb2Ugo8v6ZC+Mrck2dNYMNPjcOK
ABvxxEtBamnSaeU/IY7FC/giN622LEtV/3oDcrua0+yWuVafyxmZyTKUb4/GUgaf
RQPf/eiX9urWurtIK7XgNGFNUjYPq4dSjQPPhwCHE/LKAykWnZBXRrX0Dq4XyApN
...
VIsCHYTD7HN9tw7whqLg18wB1zomSMVGT4DkkmAzc4zSKI1FNYP8KA3OE1Emwq+0
wRsQuawQVLCUEP3To6kYOWTzJq7jhUK6FnlJjeTrNQSvdoqwoJr1TAHGxVV3q7q
v3TGd3xXD9yQIjmugNgxNiwAZzhJs/ZJy++fPSJ1XQxbd9qPghGoe/ff6G7
-----END RSA PRIVATE KEY-----
```

Certificate (*.crt) *

```
-----BEGIN CERTIFICATE-----
MIIGJzCCBA+gAwIBAgIBATANBgkqhkiG9w0BAQUFADCBSjELMAkGA1UEBhMCRIx
DzANBgNVBAGMBkFsc2FjZTETMBEGA1UEBwwKU3RyYXNib3VyZzEYMBYGA1UECgwP
d3d3LmZyZWVsYW4ub3JnMRAwDgYDVQQLEAdmcmV1bGZuMS0wKwYDVQQDDCRGcmV1
...
CQVqfbscp7evlgjLw98H+5zy1RHAgO2G79aH1jNkMp9B0uq6SnEg1EsiwGVtu21
hnx8SB3sVJZHeer8f/UQQwqbAQ+Kdy70NmbSaqavtp8j0xLiidWkwSyRTsuU6D8i
DiH5uEqBXExjrj0Fs1xcVKdVj5g1VcSmkLwZKbEU1OKw1eT/iXFhvooWhQ==
-----END CERTIFICATE-----
```


CA certificate (*.ca.crt)

Once the certificate is created, go to **Domains > example.com > Hosting Settings** and:

- enable **SSL support**
- select your created SSL certificate click **OK**

Hosting Settings for example.com ...

This is where you configure website hosting settings and select the features available for your site.

Domain name *	www. <input type="text" value="example.com"/>
	The website's domain name like example.com.
Hosting type	Website
Website status	Active [Change]
Document root *	 / <input type="text" value="httpdocs"/>
	The path to the website home directory.
Preferred domain *	<input type="radio"/> www.example.com <input type="radio"/> example.com <input checked="" type="radio"/> None
	Select the URL (either with or without the www. prefix) to which site visitors will be redirected via a SEO-safe HTTP 301 redirect.

Security

To secure transactions with your site, use SSL/TLS protocol, which encrypts all data and transfers it over a secure connection. To employ SSL/TLS, install an SSL/TLS certificate on the site, and then select it below.

SSL/TLS support

Permanent SEO-safe 301 redirect from HTTP to HTTPS

Certificate

Open your website at <https://example.com>.

Note: In case of any issues, make sure that the certificate was properly selected.

Online URL: <https://kb2.ic.uk/article.php?id=254>