Previous Next

Install an SSL Certificate

Here you will learn the steps of installing an SSL certificate on your web server.

Installation of an SSL certificate depends on many things such as where you generated the CSR, the type of certificate files you got from the CA, the types of certificate files your web server supports etc.

The following are the steps involves in the process:

1. Gather the necessary files
2. Find out the certificate file type and format your web server requires
3. Convert the certificate file type with the web server compatible files
4. Install the certificates on your web server
5. Bind the installed SSL certificate to your web site
6. Test the certificate

1 - Gather the necessary files:

In order to install an SSL certificate on your web server and bind it to your domain, you should have the following files:

1. SSL Certificate for your domain
2. Intermediate certificates or CA bundle (optional)
3. Private key

You should have a certificate file for your domain and intermediate certificate files from the CA where you submitted the CSR. The CA may not have issued an intermediate certificate or may have issued more than one intermediate certificate. Most likely you will have an intermediate certificate(s).

You may have the private key stored in a .key file type. However, it depends on where you generated the CSR and where you want to install it. If you generated the CSR from the same web server where you want to install an SSL certificate, then you will not have a private key file because it is secretly stored by the web server. If you generated the CSR using a browser or SSL tools, then you should have a saved private key in a separate .key file. If the web server where you generate the CSR is different from the web server where you are going to install the certificate, then you need to export the private key from where you generated the CSR because the private key is generated at the same time when the CSR is generated.

So, gather all the required files before proceeding.

2 - Find out the certificate file type and the format your web server requires

Once you have the necessary certificate files, you need to check the certificate file type and the format your web server supports. Different web servers and hosting platforms support different formats and types of certificate files. For example, Apache and other similar web servers support certificates in PEM format, whereas Microsoft Windows support certificates in PKCS#7 format.

Some web servers and hosting platforms require separate certificate, intermediate certificate and private key files, whereas others require a single file for all. For example, Microsoft Azure cloud platform requires all files in a single PKCS#12/PFX format.

So, find out the appropriate format and file type that your web server supports.

3 - Convert the certificate file into the web server compatible file

If the certificate files and format you got from the CA are not supported on your web server or hosting provider then you have to convert the certificates to your web server supported format using OpenSSL.

Convert your SSL certificate files as per your web server supported format using OpenSSL. Some web servers require a single file for your domain certificate, intermediate certificate and private key while other web servers require a separate file for each. For example, azure app service requires PKCS#12 format in a .pfx file with certificate, intermediate certificate and private key. So, you need to consider that too.

Learn about OpenSSL conversion commands in the next chapter.

4 - Install the certificates on your web server

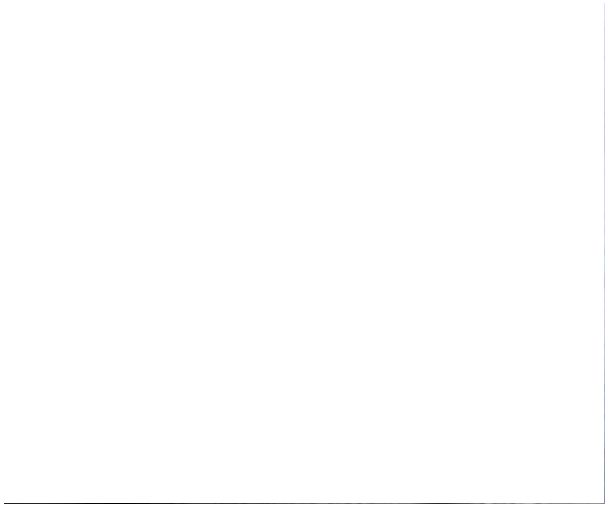
So, once you have certificate files in the required format and type, you can install your SSL certificate on your web server. Go to https://www.thesslstore.com/knowledgebase/ssl-install/ and click on the link of your web server to know how to install an SSL certificate.

5 - Bind the installed SSL certificate to your web site

Once you have installed your SSL certificate, it's time to bind it to your website. Again, this depends on the web server or hosting provider.

6 - Test the https website

In this last step, you should test your SSL certificate with the SSL tools and check whether it is working fine or not.



Previous
Next

feedback@tutorialsteacher.com

TUTORIALS

- ASP.NET Core
- ASP.NET MVC
- IoC
- Web API
- C#
- LINQ
- Entity Framework
- AngularJS 1
- Node.js
- D3.js
- JavaScript
- jQuery
- Sass
- Https

E-MAIL LIST

Subscribe to TutorialsTeacher email list and get latest updates, tips & tricks on C#, .Net, JavaScript, jQuery, AngularJS, Node.js to your inbox.

Email address GO

We respect your privacy.