
CPanel SSL Certificate Deployment Guide



StartCom CA Limited

Contents

1. The environment for installing the SSL certificate	3
1.1 Brief introduction of SSL certificate installation environment	3
1.2 Network environment requirements	3
2. Installation of SSL certificate	4
2.1 Get SSL certificate	4
2.2 Extract SSL certificate	4
2.3 Install SSL certificate	4
2.4 Test the SSL certificate	7
3. Backup of SSL certificate	8
4. Restore of SSL certificate	8

1. The environment for installing the SSL certificate

1.1 Brief introduction of SSL certificate installation environment

Cpanel Control Panel.

SSL certificate(Note: this guide uses the class 3 SSL certificate which the domain name is startssl.com to operate, other class of the certificate are also common.)

1.2 Network environment requirements

Please ensure the site is a legitimate e domain address, which can normal access by typing it's domain name `http://XXX`.

2.Installation of SSL certificate

2.1 Get SSL certificate

You will get a zip file after you apply the certificate from startcom successfully. You should to extract the file and you will get 4 files: Apache Server, IIS Server, Nginx Server, Other Server, These are different formats for different servers. We will need to use the certificate from Apache Server.zip.

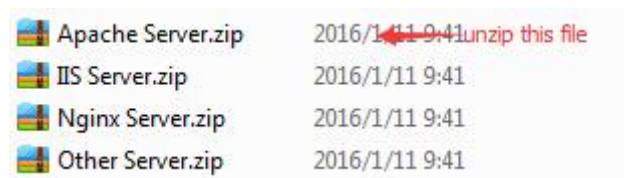


Figure 1

2.2 Extract SSL certificate

Open the file for Apache; you can see two files, including public key, certificate chain, as shown in Figure 2

Name	Date modified	Type	Size
1_root_bundle.crt ← chain file	2016/1/7 10:27	Security Certificate	3 KB
2_startssl.com.crt ← public.crt	2016/1/7 10:27	Security Certificate	3 KB

Figure 2

2.3 Install SSL certificate

1. Import certificate

Enter the Cpanel Control Panel, find the ssl/tls button, as shown below:



CPANEL 11

SSL/TLS Manager

The SSL/TLS Manager will allow you to generate SSL certificates, certificate signing requests, and private keys. These are all parts of using SSL to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card numbers, etc are sent encrypted instead of plain text. It is important to secure your site's login areas, shopping areas, and other pages where sensitive information could be sent over the web.

Private Keys (KEY)
Generate, view, upload, or delete your private keys.

Certificate Signing Requests (CSR)
Generate, view, or delete SSL certificate signing requests.

Certificates (CRT)
Generate, view, upload, or delete SSL certificates.

Install and Manage SSL for your site (HTTPS)
Manage SSL sites.

Under Install/Update a SSL Host, select the domain(you want to binding) from the Domain drop down list and open public key(public.crt) file with notepad , copy it and paste.

Install/Update A SSL Host

Domain

Ip Address **10.10.10.10**

Certificate (CRT)

The crt may already be on the server.
 You can try to it or paste the entire .crt file here:

Paste the public key in here!

2. Import certificate private key and CA certificate chain

Find certificate chain in for Apache Server.zip. and your private.key open with notepad. Copy and paste. The private key is created when you generate CSR

Key (KEY)

The key may already be on the server.
 You can try to it or paste the entire .key file here:

Paste the private key in here!

Ca Bundle (CABUNDLE)

Paste the ca bundle here (optional):

Paste the certificate chain in here!

Once all the fields are populated click "Install Certificate".

2.4 Test the SSL certificate.

Input the address in browser address bar: <https://domain.com> (the domain of the applied SSL certificate) Test your SSL certificate is installed successfully or not. If successful, the browser address bar will display a safety lock sign.

You could test your website's certificate and configuration by <https://www.ssllabs.com/ssltest/>.

3.Backup of SSL certificate

Please save the file you receive, key file and password.

4.Restore of SSL certificate

Repeat 2.3 operation.