

How to configure free SSL on your Cloudflare account

What is SSL?

SSL (Secure Socket Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This secure link helps ensure that all data transferred between the browser and the server remains private. It's also called TLS (Transport Layer Security), in its more modern versions. Millions of websites use SSL encryption everyday to secure connections and keep their customer's data safe from monitoring and tampering.

This guide will show you how to take advantage of CloudFlare's free Full (strict) SSL at Vivio. Please note: it may take up to 24 hours to activate your SSL within CloudFlare.

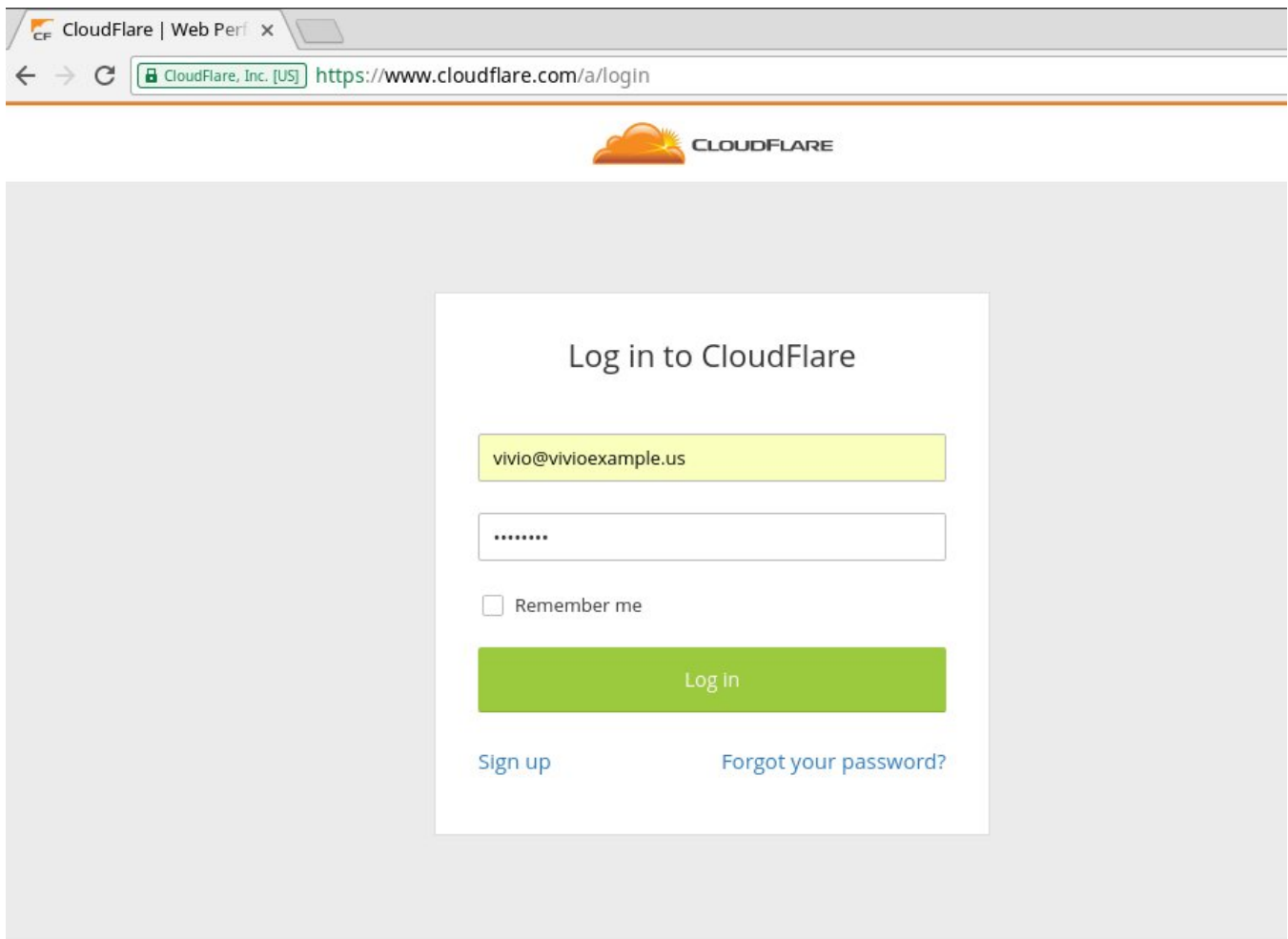
Assumptions

This guide assumes that you have already set up your web site within CloudFlare. If you have not yet set up your site to use CloudFlare, please follow [these instructions](#) to setup your cPanel domains to use CloudFlare.

Step 1: Login to Your CloudFlare Account:

You can access your CloudFlare portal from your cPanel account or directly from the CloudFlare website located at:

<https://www.cloudflare.com/a/login>

A screenshot of a web browser showing the CloudFlare login page. The browser's address bar displays 'https://www.cloudflare.com/a/login'. The page features the CloudFlare logo at the top. The main content area is a white box with the heading 'Log in to CloudFlare'. Below the heading, there is a text input field containing 'vivio@vivioexample.us', a password input field with masked characters, and a 'Remember me' checkbox. A green 'Log in' button is positioned below these fields. At the bottom of the white box, there are two links: 'Sign up' and 'Forgot your password?'.

CloudFlare | Web Perf x

CloudFlare, Inc. [US] <https://www.cloudflare.com/a/login>

CLOUDFLARE

Log in to CloudFlare

☐ Remember me

[Sign up](#) [Forgot your password?](#)

Step 2: Access the SSL Configuration Screen

Next you'll need to click the 'Flexible' text link next to 'SSL':

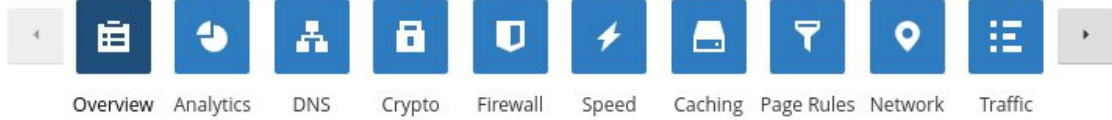
vivioexample.us



[Add Site](#)

[Support](#)

[vivio@vivioexa...](#) ▾



Overview

vivioexample.us



Status: Active

This website is active on CloudFlare.

Quick Actions



[Advanced ▸](#)

Settings Summary



Security Level: Medium

SSL: Flexible




Caching Level: Standard

Development Mode: Disabled

Select Full (Strict) from the drop down

CF Crypto: vivioexample.us x

← → ↻ CloudFlare, Inc. [US] https://www.cloudflare.com/a/crypto/vivioexample.us#ssl

vivioexample.us  Add Site Support vivio@vivioexa... ▾

Overview Analytics DNS **Crypto** Firewall Speed Caching Page Rules Network Traffic

Crypto

Manage cryptography settings for your website.

SSL

Encrypt communication to and from your website using SSL.

This setting was last changed a few seconds ago

Flexible

Off

Flexible

Full

Full (strict)

[Help ▸](#)

HTTP Strict Transport Security (HSTS)

Enforce web security policy for your website.

[Enable HSTS](#)

On the same page, scroll down until you see 'Create Certificate'

CF Crypto: vivioexample. x

CloudFlare, Inc. [US] https://www.cloudflare.com/a/crypto/vivioexample.us#ssl

vivioexample.us Add Site Support vivio@vivioexa... ▾

API ▸ Help ▸

Authenticated Origin Pulls

TLS client certificate presented for authentication on origin pull.

Off

API ▸ Help ▸

TLS 1.2 Only

Only use the latest TLS protocol. Note: This is required for PCI 3.1 compliance, but may restrict traffic to your site from older browsers.

Upgrade to Business plan

API ▸ Help ▸

Origin Certificates

Generate a free TLS certificate signed by CloudFlare to install on your origin server.

Create Certificate

Hosts	Expires On
No Certificates	
◀ 1 ▶ 0 - 0	

CLI ▸ API ▸ Help ▸

Step 3: Generate Your SSL Certificate

Here we generate the SSL. The defaults that CloudFlare gives you should be fine for most purposes.

Origin Certificate Installation

Follow the steps below to generate and install a certificate on your origin server.

The first step in generating a certificate for your origin is creating a private key and a Certificate Signing Request (CSR). You can provide your own CSR or we can generate a key and CSR using your web browser.

- ☒ Let CloudFlare generate a private key and a CSR

Private key type

RSA

- ☐ I have my own private key and CSR

List the hostnames (including wildcards) on your origin that the certificate should protect. By default your origin certificate covers the apex of your zone (**example.com**) and a wildcard (***.example.com**). If there are others you wish to add, e.g., those not covered by the wildcard such as **one.two.example.com**, you can add them below.

× *.vivioexample.us × vivioexample.us

Choose how long before your certificate expires. By default your certificate will be valid for fifteen (15) years. If you'd like to decrease how long your certificate will be valid make a selection below.

Certificate Validity

7 days

Cancel

Next

Hitting the 'Next' button here will generate your new SSL certificate.

IMPORTANT! Keep this window open! We'll need to copy and paste our SSL keys on this screen in the next step.

Step 4: Install your SSL into cPanel

Next you'll want to copy both the 'Origin Certificate' and 'Private Key'.

Origin Certificate Installation

Follow the steps below to generate and install a certificate on your origin server.

Save both the private key and certificate below to your web server. To save, you can either copy the contents of the boxes below and paste them into different files on your web server, e.g., example.com.pem and example.com.key, or you can click the download link above each box and then upload using scp or sftp. After saving, select your web server from the dropdown and click the "Show Instructions" button for an installation guide.

Key format

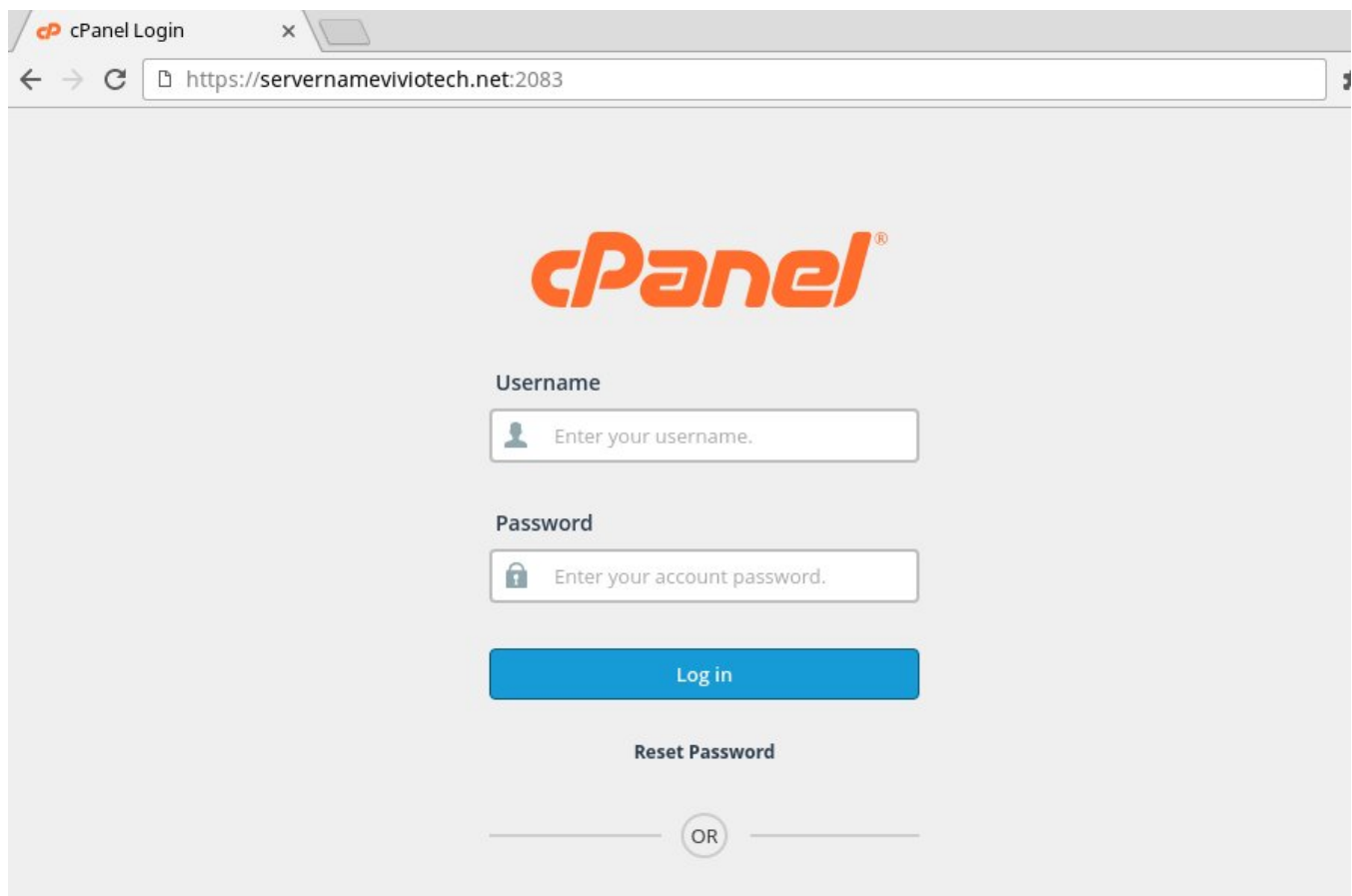
PEM (Default)

Origin Certificate

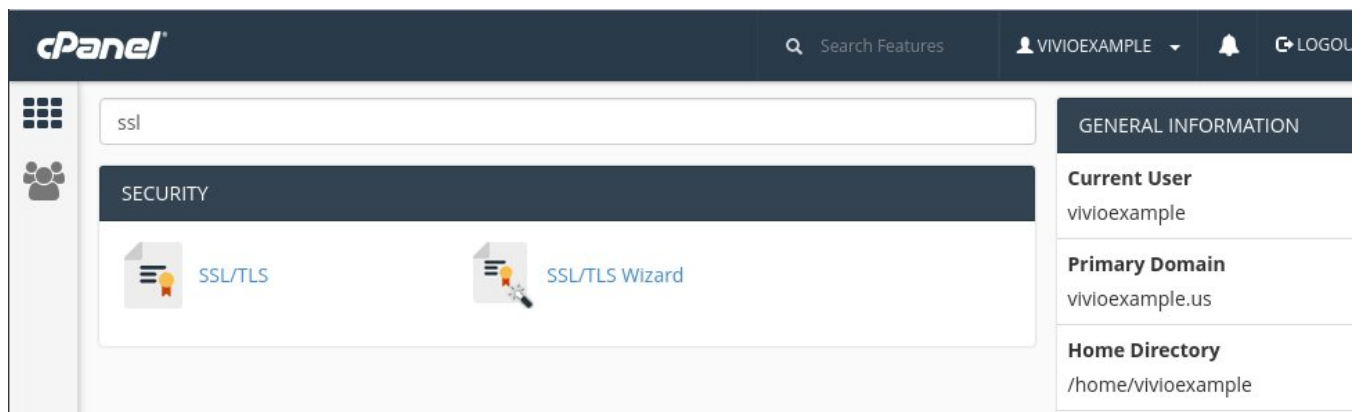
```
-----BEGIN CERTIFICATE-----
MIIEdDCCA4igAwIBAgIUe+8J3moVDj0Z2rqttWzygI36dZswDQYJKoZIhvcNAQEL
BQAwYsxCzAJBgNVBAYTA1VTMRkwFwYDVQQKEwBDbG91ZEZsYXJ1LCBjb210MTQw
MgYDVQQLEytDbG91ZEZsYXJ1IE9yaWdpbiBTU0wgQ2VydG1maWNhdGUgQXV0aG9y
aXR5MRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MB4XDTE2MDgxODIzMTEwMFoXDTE2MDgyNTIzMTEwMFowYjEZMBcGA1UEChMQQ2xv
dWRGbGFyZSwgSw5jLjEdMBsGA1UECzMUMQ2xvdWRGbGFyZSBPcm1naW4gQ0ExJjAk
BgNVBAMTHUNsb3VkrMxhcmUgT3JpZ21uIENlc3R5YXR1MIIBIjANBgkqhkiG
9w0BAQEFAAOCQA8AMIIBCgKCAQEA7dnu+4i9c6SlySuHZ67rU9xDcRCmdKY9BrD/
TgXgT5c1yVXg7YMg2nIawtx854FtC+6JBammv0z3HaZzpB9hZedreBx01EaMBf/6
KGbckMUyn0Zv580QcTArVLEIVu93KBDjS1LDdTnI43oKLCrG8GCEbVKX/E60Q8r
NtQt1KqsXSVRtx4fAiyJxj6CnYNc2V04s15VoXZz78q3LBba30vhE0PBPrGk6gE/
```

In order to copy and paste our keys, we'll login into our Cpanel account at:

<https://servername.viviotech.net:2083> (where 'servername' is the name of our cPanel server)



Click on SSL/TLS under 'Security'



Now we'll need to install a key, certificate and a CA. Click on Install and Manage SSL sites.



SSL/TLS

The SSL/TLS Manager will allow you to generate SSL certificates, certificate signing requests, and private keys. These are used to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card numbers, and other sensitive information is 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.](#)

Paste the CRT in the CRT box from our Original Certificate install above. You'll want to ensure that you also include the '-----BEGIN CERTIFICATE-----' lines as well as '-----END CERTIFICATE-----' lines.

Save both the private key and certificate below to your web server. To save, you can either copy the contents of the boxes below and paste them into different files on your web server, e.g., `example.com.pem` and `example.com.key`, or you can click the download link above each box and then upload using `scp` or `sftp`. After saving, select your web server from the dropdown and click the "Show Instructions" button for an installation guide.

Key format

PEM (Default)	
---------------	---

Origin Certificate -----BEGIN CERTIFICATE-----
MIIEoDCCA4igAwIBAgIUe+8J3moVDj0Z2rqttWzygI36dZswDQYJKoZIhvcNAQEL
BQAwgYsxCzAJBgNVBAYTA1VMTMRkwFwYDVQQKEwBDbG91ZEZsYXJ1LlCBJmMuMTQw
MgYDVQQLEytDbG91ZEZsYXJ1IE9yaWdpbiBTU0wgQ2VydG1maWNhDGUGXV0aG9y
aXR5MR9wFAYDVQQHEw1TYW4gRnJhbmcNpc2NvMRMwEQYDVQQIEw1DYWxpZm9ybmlh
MB4XDTE2MDgxODIzMTIwMFoXDTE2MDgyNTIzMTIwMFowYjEzMBCGA1UEChMQQ2xv
dWRGbGFyZSwgSW5jLjE2MDMsGA1UECwMUQ2xvdWRGbGFyZSBPcm1naW4gQ0ExJjAk
BgNVBAMTHUNsb3VkrMxhcmlUgT3JpZ21uIEN1cnRpbWljYXR1MIIIBjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEa7dnu+4i9c6S1ySuH267rU9xDCRCmdKY9BrD/
TgXgT5c1yVXg7YmG2nIawtx854Ftc+6JBAmmv0z3HaZzpB9hZedreBx01EaMBf/6
KGbckMUyn0Zv580QcTarVLEIVu93KBDjS1LDdTnI43oKLCrG8GCUeBVkX/E60Q8r
NtQt1KqsXSVRtx4fAiYJxj6CnYNc2V04s15VoXZz78q3LBba30vhEOPBPPrGk6gE/
Ldr6K600Howada0s88C2DG9c9sdyHBp4oBP2qE071mZStfIT/I+thJ61G3f4TsgN
gTiaQ5P2ae0CwwGgRePfe6gZ4DbwsY21mgxB1MmxwMo5WfLegwIDAQABo4IBIjCC
AR4wDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAwGA1UdEwEB
/wQCAAwwHQYDVR00BBYEFntslwmkdBDBVpEn9mZ42TqmEdS0wMB8GA1UdIwQYMBAA
FCToU1ddfDRAh6nr1Nu64RZ4/CmkMEAGCCsGAQUFBwEBBDQwMjAwBggrBgEFBQcw
AYYkaHR0cDovL29jc3AuY2xvdWRmbGFyZS5jb20vb3JpZ21uX2NhMC0GA1UdEQQM-----

You'll want to do the same for the Private key. Remembering again to include the '-----BEGIN PRIVATE KEY-----' and '-----END PRIVATE KEY-----'

Private key

Copy the contents of your private key below to your web server and set file permissions such that only your http server access it. Additionally, you can optionally encrypt this file and provide a password to decrypt it during your origin web startup.

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQCvpea3lUsVF1BB
zH1gW1T7wjmSzduPUJhKC2IfSkVseyvif0rhdggOnRiSAFoN1r2aVYEAMSpucqa
PsRETrg5JMLBu0nfbr6fet3wIcpt9ieb/q0bEgVgFqW4kzszpd6wb0atdXWR5j3F
4QeNT81H/OmccSPEDFgtLqxKAlgQP01xsh28X1mFtbfG1BFyIHBIN4R0ZIOFTmbk
R7sxC9Ho/LYiNsFLiTo0ia5the7UVuU+T2ZvQoi7UCxI4M1fxEX8dpqf9z8Mwnz1
MWuRs530VFNioMF3mwAlPY32BPbSDp3wrA7lsha0XNqbKviUixHXcHbPYZtQ1CvJ
A5hUyuiHAgMBAAECggEBAKowSRhgI1vPEHowtNqEJBe73SUNKUv3f1de9UNmYkSP
HRII1bEyAnNXsCT6N8L0v+g5sAo45FS/nDtPzc0RspZLtBkaaz1+hFzqI9jkYs6g
z0gqv3eXQnYT+4aXwakNcnPpncw8JaQ0N+5fV33ocLLrrz7RsSHoBBfjPTSIi0NR
SWRAI+k5BFd12okrtotUnuBM+FhsASNyXoN9IGbFKhMy9wnX9BfwAiekdMYXUBUX
ozXK6Q+oE0Jn+8q+RZCSwieKLwsKrASJ4LOu6iQF09cAa0tsB90gpAZTCeG0sAhy
0hfVfGpty9oaf/UxIocCZ3mSrUhyRJoViDF30r13KKECgYEA5TMkdrP50/X50STH
iUQo13e5ztjw4GL3veCSH3oI499/ZQaTVICa40T6X9Ide4kmJ/1MB6r3SAosIhED
Fxf5II4fpIwCn/E5pxoh50aKksicdQWtuxGD2NstbX68u2Zt67+qeGwbe8Sqd7ap
txXc+is60UFD04bE0hFzm0pq0/0CgYEAC++Vg8JZ18nVx1dAXuqoHdtiCfBW7K+
CisGqGwu0YV2Pp/Txaonj8tKdqt80mptc9N6Sa4E9sKs0ypsu466/jxQxkquI3zD
cc5Jkn5EBbrLvga81B6NvtAvw+I4JcI2dsXJRlyFN10i3WMGZKH+ALm7B4IGPgW+
jX/r0zh9g9MCgYAsb6foI6iSAaR3eev9nutHwnyRr9mzhzyE4Z8y3xQ0KeynB41U
-----
```

Your domain should auto fill in when you paste the certificate.

To install the Certificate Authority Bundle, we'll need to grab that from Cloudflare, [here](#).

You'll want the CloudFlare Origin CA — RSA Root.

What are the root certificate authorities (CAs) used with CloudFlare Origin CA?



Patrick Donahue

Sunday at 15:40

If you are using cPanel, or another application that attempts to validate the chain of your Origin CA certificate, you will need to append the appropriate root below to your .pem file.

Note that cPanel in particular does not support ECC certificates, so make sure you generate an RSA certificate.

CloudFlare Origin CA — RSA Root

```
-----BEGIN CERTIFICATE-----
MIID/DCCAuagAwIBAgIID+r0SdTGfGcwCwYJKoZIhvcNAQELMIGLMQswCQYDVQQG
EwJVUzEZMBcGA1UEChMQQ2xvdWRGbGFyZSwgSW5jLjE0MDIGA1UECxMrQ2xvdWRG
bGFyZSBPcmInaW4gU1NMIENlcnRpZmljYXRlIEF1dGhvcmI0eTEWMBQGA1UEBxMN
U2FuIEZyYW5jaXNjbzETMBEGA1UECBMKQ2FsaWZvcn5pYTAeFw0xNDExMTMyMDM4
NTBaFw0xOTExMTQwMTQzNTBaMIGLMQswCQYDVQQGEwJVUzEZMBcGA1UEChMQQ2xv
dWRGbGFyZSwgSW5jLjE0MDIGA1UECxMrQ2xvdWRGbGFyZSBPcmInaW4gU1NMIENl
cnRpZmljYXRlIEF1dGhvcmI0eTEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzETMBEG
-----END CERTIFICATE-----
```

Ensure that the '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' are also copied for the Certificate Authority bundle or CA. Pasting in all 3 certificates should look something like this

Certificate: (CRT)

MIIEoDCCAigAwIbnjEwE+8j3mVdJ0ZrtttWzYgI36dZswQ0j3KozThvNCaQEL
BQAAVwQsYcZAJBgmVBAYATLXtRrXmFgYDVQDQExBDB6B9ZDZESYXJ1LCBjbGluM0A=

(More information)

Private Key (KEY)

H1EwIBADANBakukikG9w9BAQEFAAScKwwgSlaGAeAeIPA0Q1ze7ZiLzpkXJ
 K4dnrtZ3tAEKFKZ0l9w6f9BpLz3V2e0vQachrc3H2nWd0L7ekEAc/TP
 00kHt2FkR2t1XfE1R0GfP//o0ztyXkTfRm/nw5BM8wLjWbW37C0eONUK5Nl0c1i
 eqn0skbwJ0RTU1tRfTRdys2L1C3qaxqJ4V3GH8cLlCnYmKblz2XZTixYlWhdnPv
 yrcsFtrFs+Q0F8E+saAT0R21vorrQ4eIb0LrSzzWYp6L2x3iC6nieAe/PTUW
 ZL1R8P186icnabUd/hQvAZ8MhnpD/Zp44L84Z49974n8nqNwCkwnMaEaHlYvHhA
 vLZ8t6D0ABMAAEqGAEAOXZT1jGkscZx5Wm2Ykxbl1Gul1kHwYek0k3Z5WmY
 xKh1Fol7Dd6GfKcKHd8KAvfc1Ym2AKLBUctvix2n071321axWU9VQ0VhAtPyq
 ph6AL0Q25SSfVhYlawZ13xx1mDm0q6Y9C79LDiHczUpBexZGohZ8E8tuVdCQ

The private key may already be on your server. You can either paste the private key here or try to retrieve the matching key for your certificate.

Certificate Authority Bundle: (CABUNDLE)

MIID,DCBAAAwIeITID+R0sdGTFGvc+YJKoZhtvNCAQELM1GLM0ScmYQYDVQgE
EwJUVZEEUaG1UECNMQ0wZWRGbgGyFZW5wS5JlIE0MDJGE1UECmR0ZWRG
bG9yFZSPcmIuZm91LW1NMTIENmR0ZmZml0eTEWMBQGA1UEBjNl
DUFuZEluZm9yYXNjZjE2TEBEGAIUECBMKQZSfawZwcm5pTAAwF0NDExMTY4MDM4
NTBhFm90ZExtMTQzNTBhM1GLMQ0wYQYDVQGEW5wZm9yYXNjZm9yFZEEUaG1UECNMQ0w
ZWRGbgGyFZW5wS5JlIE0MDJGE1UECmR0ZWRGbgGyFZSPcmIuZm91LW1NMTIENmR0ZmZml0e
TmR0ZmZml0eTEWMBQGA1UEBjNlDUFuZEluZm9yYXNjZjE2TEBEG

Finally, click on 'Install Certificate' at the bottom of the page. You can now browse to your domain to confirm that SSL is working.



If you have any questions, please feel free to reach out to our Support staff via [email](#), [phone](#), or [web chat](#).

Related articles

- [How to add or manage a credit card on file](#)
- [How to add two-factor authentication to your Vivio Portal account](#)
- [How to Reduce Your Backup Usage in R1Soft](#)
- [How to access your Vivio Portal client account](#)
- [Managing Security Codes](#)