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 thes e 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



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 Analytics	DNS Crypto Fi	rewall Speed	Caching Page Rules Netw	vork Traffic
Overview				
vivioexample.	us			•
Status: Active This website is active	on CloudFlare.		Quick Actio	ins 🚖
				Advanced •
Settings Sumn	nary			
Security Leve SSL: Flexible	: Medium	Cach Deve	ning Level: Standard elopment Mode: Disa	abled

Select Full (Strict) from the drop down



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

/ 🏹 Crypto: vivioexar	mple. ×			Jaco
\leftarrow \rightarrow C \square Cloud	Flare, Inc. [US] https://www.cloudflare.	com/a/crypto/vivioexample.u	us#ssl	무 ☆ 윩
	vivioexample.us		Add Site Support vivio@vivioexa •	
			API + Help +	
	Authenticated Origin TLS client certificate presented origin pull.	Pulls for authentication on	Off	
			API + Help +	
	TLS 1.2 Only Only use the latest TLS protoco for PCI 3.1 compliance, but may site from older browsers.	l. Note: This is required / restrict traffic to your	Upgrade to Business plan	
			API + Help +	
	Origin Certificates Generate a free TLS certificates install on your origin server.	signed by CloudFlare to	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 ke	y 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.

÷

Cancel

× *.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	d	avs

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-----

MIIEoDCCA4igAwIBAgIUe+8J3moVDj0Z2rqttWzygI36dZswDQYJKoZIhvcNAQEL BQAwgYsxCzAJBgNVBAYTALVTMRkwFwYDVQQKExBDbG91ZEZsYXJ1LCBJbmMuMTQw MgYDVQQLEytDbG91ZEZsYXJ1IE9yaWdpbiBTU0wgQ2VydG1maWNhdGUgQXV0aG9y aXR5MRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRMwEQYDVQQIEwpDYWxpZm9ybm1h MB4XDTE2MDgxODIzMTIwMFoXDTE2MDgyNTIzMTIwMFowYjEZMBcGA1UEChMQQ2xv dWRGbGFyZSwgSW5jLjEdMBsGA1UECxMUQ2xvdWRGbGFyZSBPcmlnaW4gQ0ExJjAk BgNVBAMTHUNsb3VkRmxhcmUgT3JpZ21uIEN1cnRpZmljYXR1MIIBIjANBgkqhkiG 9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7dnu+4i9c6S1ySuHZ67rU9xDcRCmdKY9BrD/ TgXgT5c1yVXg7YMg2nIawtx854FtC+6JBAmmv0z3HaZzpB9hZEdreBx01EaMBf/6 KGbckMUyn0Zv580QcTArVLEIVu93KBDjS1LDdTnI43oKLCr68GCUEbVKX/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)

- > C D https://serverr	nameviviotech.net:2083	
	<i>cPanel</i>	
	Username L Enter your username.	
	Password Enter your account password.	
	Log in	
	Reset Password	

Click on SSL/TLS under 'Security'

cP	anel		Q Search Features	⊥ v	IVIOEXAMPLE 👻	٠	🕒 LOGOL
	ssl				GENERAL INF	ORMA	TION
	SECURITY				Current User vivioexample		
	SSL/TLS	SSL/TLS Wizard			Primary Dom vivioexample.u	ain JS	
					Home Director	o ry ample	

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

C https://waterlily.viviotech.net:2083/cpsess4379519407/frontend/paper_lantern/ssl/index.html



The SSL/TLS Manager will allow you to generate SSL certificates, certificate signing requests, and private keys. These ar to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card num encrypted instead of plain text. It is important to secure your site's login areas, shopping areas, and other pages where 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.

4

502

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+8J3moVDj0Z2rqttWzygI36dZswDQYJKoZIhvcNAQE	EL
BQAwgYsxCzAJBgNVBAYTA1VTMRkwFwYDVQQKExBDbG91ZEZsYXJ1LCBJbmMuMTQ	QW
MgYDVQQLEytDbG91ZEZsYXJ1IE9yaWdpbiBTU0wgQ2VydG1maWNhdGUgQXV0aG9)y
aXR5MRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRMwEQYDVQQIEwpDYWxpZm9ybm1	Lh
MB4XDTE2MDgx0DIzMTIwMFoXDTE2MDgyNTIzMTIwMFowYjEZMBcGA1UEChMQQ2x	<v td="" <=""></v>
dWRGbGFyZSwgSW5jLjEdMBsGA1UECxMUQ2xvdWRGbGFyZSBPcm1naW4gQ0ExJjA	Ak
BgNVBAMTHUNsb3VkRmxhcmUgT3JpZ21uIEN1cnRpZmljYXR1MIIBIjANBgkqhki	LG
9w0BAQEFAA0CAQ8AMIIBCgKCAQEA7dnu+4i9c6SlySuHZ67rU9xDcRCmdKY9BrD)/
TgXgT5c1yVXg7YMg2nIawtx854FtC+6JBAmmv0z3HaZzpB9hZEdreBx01EaMBf/	6
KGbckMUyn0Zv580QcTArVLEIVu93KBDjS1LDdTnI43oKLCrG8GCUEbVKX/E60Q8	3r
NtQt1KqsXSVRtx4fAiyJxj6CnYNc2V04s15VoXZz78q3LBba30vhE0PBPrGk6gE	Ξ/
Ldr6K600Howada0s88C2DG9c9sdyHBp4oBP2qE071mZStfIT/I+tHJ61G3f4Tsg	γN
gTIaQ5P2ae0CwWgGRePfe6gZ4DbwsYZ1mgxB1MmxwMo5WfLegwIDAQABo4IBIjC	CC
AR4wDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAwGA1UdEwE	EB
/wQCMAAwHQYDVR00BBYEFNtsWmkdBDBVpEn9mZ42TqmEdS0wMB8GA1UdIwQYMBa	AA
FCToU1ddfDRAh6nr1Nu64RZ4/CmkMEAGCCsGAQUFBwEBBDQwMjAwBggrBgEFBQc	CW
AYYkaHR0cDovL29jc3AuY2xvdWRmbGFyZS5jb20vb3JpZ21uX2NhMC0GA1UdEQQ	Qm

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 serve access it. Additionally, you can optionally encrypt this file and provide a password to decrypt it during your origin web startup.

----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCvpea31UsVFiBB zH1qW1T7wjmSzduPUJhKCy2IfSkVseyvif0rhdqqOnRiSAFoN1r2aVYEAMSpucqa PsRETrg5JMLBu0nfbr6fet3wIgpt9ieb/q0bEgVgFqW4kzszpd6wb0atdXWR5j3F 40eNT81H/OmccSPEDFqtLqxKAlq0P01xsh28X1mFtbfG1BFyIHBIN4R0ZI0FTMbk R7sxC9Ho/LYiNsfLiTo0ia5the7UVuU+T2ZvQoi7UCxI4MlfxEX8dpqf9z8MWnz1 MWuRs530VFNIoMF3mwAlPY32BPbSDp3wrA71sha0XNqbKviUixHXcHbPYZtQ1CvJ A5hUyuiHAgMBAAECggEBAKowSRhgI1vPEHowtNqEJBe73SUNKUv3f1de9UNmYkSP HRII1bEyAnNXsCT6N8L0v+g5sAo45FS/nDtPzc0RspZLtBkaaz1+hFzqI9jkYs6g z0qqv3eX0nYT+4aXwakNcnPpncW8Jaq0N+5fV33ocLLrrz7RsSHoBBfjPTSIiONR SWRAI+k5BFd12okrtotUnuBM+FhsASNyXoN9IGbFKhMy9wnX9BfwAiekdMYXUBUX ozXK60+oE0Jn+8q+RZCSwieKLwsKrASJ4L0u6i0F09cAa0tsB90qpAZTCeG0sAhy 0hfVfGpty9oaf/UxIocCZ3mSrUhyRJoVIdF30r13KKECgYEA5TMkdrP50/X50STH iUQol3e5ztjw4GL3veCSH3oI499/ZQaTVICa40T6X9Ide4kmJ/1MB6r3SAosIhED Fxf5II4fpIwCn/E5pxoh50aKksicd0WtuxGD2NstbX68u2Zt67+geGwbe8Sgd7ap txXc+is60UFDo4bE0hFzm0pq0/0CgYEAxC++Vg8JZ18nVx1dAXuqoHdtiCfBW7K+ CisGqGwuOYV2Pp/Txaonj8tKdqt80mptc9N6Sa4E9sKs0ypsu466/jx0xkquI3zD cc5Jkn5EBbrLvga81B6NvtAvw+I4JcI2dsXJR1yFN10i3WMGZKH+ALm7B4IGPgw+ jX/r0zh9g9MCgYAsb6foI6iSAaR3eev9nutHwnyRr9mzhzyE4Z8y3xQ0KeynB41U 0A7VME0miuCoDDEL 1o /2L /Eo ATMEnVUME02vCOt7ot

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

To install the Certficate Authority Bundle, we'll need to grab that from Cloudflare, here.

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



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

cPa	anel	Q Search Features	L VIVIOEXAMPLE -	A G	LOG
	205.210.190.210				
	Certificate: (CRT)				
	BEGIN CERTIFICATE MIIEODCCA4igAwIBAgIUe+8J3moVDj0Z2rqttWzygI36dZswDQYJKoZIhvcNAQEL BQAwgYsxCzAJBgNVBAYTALVTMRkwFwVDVQQKExBbbG912EZsYXJLCBJbmMuMTQw Mg7DVQQLEytDbG91ZEZsYXJIE9yaWdpbiBTU0wgQ2VydGmaWNhdGUgQXV0aG9y aXSMSWFwFAYDVQQHEwJTYW4gRnJhbmNpcZWMRMcEQ7DVQ0IEwpDVWxpZm9ybmlh MB4XDTE2MDgxODIzMTIwMFoxDTE2MDgyNTIzMTIwMFowYjEZMBcGA1UEChMQQ2xv dWRGbGFyZSwgSW5jLjEdMBsGA1UECxMUQ2xvdWRGbGFyZSBPcmlnaW4gQ0ExjJAk BgNVBAMTHUNsb3VkRmxhcmUgT3JpZ2LuIENLcnRpZmljYXRIMIIBJjANBgkqhki6 9wBAQEFAAOCAQ8AMIIBCgKCAQEA7dnu+419c651ySuH267rU9xDCRCmdKYBPFD/ TgXqT5c1yVXg7VMg2nTawtx854FtC+6JBAmmv0z3HaZzpB9hZEdreBx0IEaMBf/6 KCbbdMum92x6DocLAbM Effunde2XB91LD4TarAJacKLccSCCUEbVXX/EGA0pe Domains: CloudFlare Origin Certificate *.vivioexample.us vivioexample.us Issuer: CloudFlare, Inc. Key Size: 2,048 blts (edd9eefb)				
	Expiration:Aug 25, 2016 11:12:01 PM This certificate will expire in 5 days. (More information) The certificate may already be on your server. You can either paste the certificate here or try to retrieve it for your domain.				
	Private Key (KEY) MIJEwylBADANBakahkiG9w0BAOEFAASCBKkwagSlAgEAAoIBAOD12e77illzpKXJ K4dnrutJENxEKZ00106sP90BeBPlzXJVeDtayDachrC3HzngW0L7okECaa/TPcd ng0kH2EK82t4HE7UBowF//oo2tvQxTKfBm/nw5BxMftUsOhM73caEONKUsN10cil egosKsbwYJORtUpf8TrRDvs2LC3UgaxdJVG3Hh8CLIngPokdglzZXTivX1WhdnPx vrcsEtrI5+E048E+saTgaT8t2varrQ4eiBaJc5zzwiyTWblz2x3Lc6nigFaoTIUW Z1K18hP8160cngUbd/h0vA2BMhDbk/Zp44LBaZEf4997gBngNvCxhmWaDEHUvbHA v1Z8165AgMBAAECggEAOXzTJJ1GkczZxSMgUB2vBJL6g1LkgYDMekt0k3ZSNMi vKb1EoL7DdFGZpKKHdBKavfcZf1vMA2KLMBuctvizX01n7I32laxwUF9VQaHiPya gbbALa02555fVh11aw213xk11m0gnqGsYBC79LD11Hc2UBRexZ6bh28EBtuVuDCQ				
	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 AUTNOFITY BUNGIE: (CABUNDLE)				

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

$\leftrightarrow \rightarrow$	C	https://www.vivioexample.us
-------------------------------	---	-----------------------------

Welcome to Vivio!

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 Restart Lucee on Windows and Linux
 How to View Your Services in Portal
 How to check your Support time used in Portal
 How to Find the Passwords for Your Vivio Services
 How to View Your Invoices in Portal

☆