HOW TO GENERATE A PFX SSL CERTIFICATE FOR YOUR CUSTOM DOMAIN

To enable your custom domain in your Engage account with an SSL protected site, the SSL certificate is required.

You can submit the below types of files:

- .CER
- .PFX FILES

CER files can be obtained from your SSL provider.

Follow the steps below to create a PFX Certificate.

1. GENERATE A CSR ON A COMPUTER/SERVER

CSR stands for Certificate Signing Request and it is one of the first steps toward getting your own SSL/TLS certificate. It is generated on the same server where you plan to install the certificate. CSR contains information (e.g., common name, organization, country, etc.) that the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key. Below are the steps to create a CSR. **In case you already have a CSR generated, you can jump to step 2.**

APACHE

```
openssl req -new -newkey rsa:2048 -nodes -keyout yourdomain.key -out yourdomain.csr
```

Replace ‘yourdomain’ with the domain name you're securing. For example, if your domain name is mycompany.com, you would type mycompany.key.

It will then have a series of prompts asking you for the following:

- *Common Name*: The fully-qualified domain name, or URL, you're securing. If you are requesting a Wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard, for example, *.myexample.com.
- *Organization*: The legally-registered name for your business. If you are enrolling as an individual, enter the certificate requestor's name.

- *Organization Unit*: If applicable, enter the DBA (doing business as) name.
- *City or Locality*: Name of the city where your organization is registered/located. Do not abbreviate.
- *State or Province*: Name of the state or province where your organization is located. Do not abbreviate.
- *Country*: The two-letter International Organization for Standardization (ISO) format country code for where your organization is legally registered.

WINDOWS/IIS

1. Launch Internet Information Services (IIS) Manager.

2. In the Connections panel on the left, click the server’s name for which you want to generate the CSR. In the middle panel, double-click Server Certificates. In the Actions panel on the right, click Create Certificate Request.

3. Enter the following Distinguished Name Properties, and then click Next:

Characters not accepted when entering information: < > ~ ! @ # $ % ^ * / \ ( ) ? &

- *Common Name*: The fully-qualified domain name (FQDN) — or URL — for which you plan to use your certificate (the area of your site you want customers to connect to using SSL). An SSL certificate issued for www.myexample.com is not valid for secure.myexample.com. If you want your SSL to cover secure.myexample.com, make sure the common name submitted in the CSR is secure.myexample.com. If you are requesting a wildcard certificate, add an asterisk (*) on the left side of the Common Name (e.g., *.myexample.com or *.secure.myexample.com).
- *Organization*: The name in which your business is legally registered. The organization must be the legal registrant of the domain name in the certificate request. If you are enrolling as an individual, enter the certificate requester's name in the Organization field, and the Doing Business As (DBA) name in the Organizational Unit field.

- *Organizational Unit*: Use this field to differentiate between divisions within an organization (such as "Engineering" or "Human Resources").
- *City/Locality*: The full name of the city in which your organization is registered/located. Do not abbreviate.
- *State/Province*: The full name of the state or province where your organization is located. Do not abbreviate.
- *Country*: The two-letter International Organization for Standardization- (ISO-) format country code for the country in which your organization is legally registered.
- *Cryptographic service provider* - Microsoft RSA SChannel Cryptographic Provider.
- *Bit length* - 2048 or higher, and then click Next.

4. Click ..., enter the location and file name for your CSR, and then click Finish.

2. SEND CSR TO SSL PROVIDER

Once they receive the CSR they will generate 2 files for you to download:

1. The crt file contains your public certificate. But you can't (yet) upload it to your web hosting provider because it doesn't include the associated private key. The web host needs the private key as well as the public key because it will be doing end-to-end encryption on your behalf.
2. The p7b file contains the certificates that comprise the "certificate chain" that allows your certificate to be verified up to your CA. In other words, when someone comes to your website and gets your certificate that claims that your website is run by Acme.com, this certificate chain lets that person's browser verify that your CA vouches for your identity.

Now you need to combine your public certificate with your private key and store the result in a password-protected pfx file.

3. GENERATE PFX

WINDOWS

- Get back into IIS Manager on the same machine that created the CSR (Step 1), navigate back to the Server Certificates page, and click on Complete Certificate Request (in the Actions pane on the right side of the screen).
- Tell the wizard to use the certificate crt file (but it might be a different file type if your CA used a different encoding method).
- Friendly Name is your domain name (for example yourdomainSSL).
- Tell the wizard to store the key in your Personal store.
- You should now see your new certificate listed on the Server Certificates page in IIS Manager.
- Select that certificate and export it as a pfx file (via the Actions pane on the right side of the screen).

UBUNTU

Command line:

-
  ```
  openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer
  ```

-
  ```
  openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out certificate.pfx -certfile CACert.cer
  ```

Once the PFX certificate is generated, please share it with us at cs@k12insight.com along with the associated password.