How do I create a certificate signing request from EZproxy

Last updated: Tue, 03 Aug 2021 12:25:34 GMT

Applies to

- All versions

Answer

1. From the EZproxy administration page, under the Miscellaneous heading, click on Manage SSL (https) certificates. This page is referred to as the SSL management page throughout the rest of this document.
2. On the SSL management page, click Create New SSL Certificate.
3. In the Create New SSL Certificate form, when creating a new certificate, you must fill in the following required information.
   1. **Country**: your two-letter country code
   2. **State or Province**: your unabbreviated state or province (e.g. Ohio, not OH)
   3. **Organization**: your organization
   4. **Administrator email**: your email address

**Wildcard Certificates and EZproxy**

- **Certificate name**: The name that will appear in the CN field of your certificate.
- **Subject Alternate Name**: The name(s) that will appear in the SAN field of your certificate.

The options you select in these fields will depend upon the requirements of your Certificate Signing Authority (CSA). For details about these fields and other optional fields, refer to your certificate authority's documentation. Some CSA requires you to enter your server's wildcard name in the SAN field.

If you are generating a self-signed certificate, you can select any combination of entries for these fields because all self-signed certificates generate browser warnings.

6. If you have decided to create a **self-signed certificate**, click Self-Signed Certificate. Once you see the Certificate Details page, skip to step 11.
7. If you have decided to **purchase a certificate**, click Certificate Signing Request. You will be taken to a page with Certificate Signing Request (CSR) Details.
8. EZproxy will display a Certificate Signing Request (CSR), which is a block of lines that looks like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBxTCCAS4CAQAwgYQxHjAcBgNVBAMUFSozU2Zyb20xLmNvbnRlbnQuY29t
...
```

https://help.oclc.org/Library_Management/EZproxy/Troubleshooting/How_do_I_create_a_certificate_signing_request...
You will need to submit this text to your certificate authority.

While your certificate request is being processed, do not delete the certificate signing request. When you receive your certificate, it must be applied against the original request. This information will be saved on and accessible from the SSL management page.

9. Visit the web site of your certificate authority and follow their procedure for purchasing a certificate. When purchasing, if you are asked for your web server type, select Apache+ModSSL or just Apache as either is directly compatible with EZproxy.

When you are asked for your certificate signing request, you will need to copy and paste everything from the certificate signing request created in step 7, starting with the BEGIN CERTIFICATE REQUEST line through the and END CERTIFICATE REQUEST line, including all the hyphens. If you have logged out of EZproxy, you can log back in and access your CSR details from SSL management page. From there click on the ID number for the appropriate CSR to view this information.

10. Depending on the policies of your certificate authority, it may take a few minutes or a few days to receive your certificate. The certificate will look similar to:

```
-----BEGIN CERTIFICATE-----
MII5jCCBU+gAwIBAgIDAJAYMA0GCSqGSIb3DQEBAQUAA4IAAgEA
-----END CERTIFICATE-----
```

In addition to the certificate for your server, the certificate authority may also provide intermediate or chained certificates. At this point, you should only be working with the certificate that has been issued for your server.

Once you receive your certificate, return to the SSL management page and click on your certificate signing request. Paste in all of the lines from BEGIN CERTIFICATE through END CERTIFICATE from the Certificate Signing Authority, including all the hyphens, into the certificate box, and click Save. EZproxy should accept the certificate. If it does not accept the certificate, ensure that you are copying the certificate for your server and not an intermediate certificate, then try pasting and saving again.