Working with custom domain names on hosted ExLibris environments

- **Product: Primo Classic, Primo VE, Leganto, Esploro Portal, campusM, Rosetta**
- **Custom Domain not supported for: Alma, Esploro Management, Summon**
- **Relevant for Installation Type:** Multi-Tenant Direct, Dedicated-Direct, Total Care

---

Note

Clarivate now uses an automated certificate renewal process based on the ACME protocol for custom domains. This article describes the previous manual CSR and certificate upload method and is relevant only for environments still on the older process.
For the current automated certificate management approach, see *Simplifying Custom Domain Certificate Renewals – Introducing Automated Management with ACME*.

In order to use a private domain name on a hosted server, Ex Libris needs to upload a certificate to the hosted environment. This certificate needs to be issued to the private Domain Name Server (DNS) and signed by a recognized **Certificate Authority** (CA). At the present time, in order to obtain the signed certificate, Ex Libris provides the customer with a **Certificate Signing Request** (CSR) and the customer returns a signed certificate to be uploaded.

The type of certificate that needs to be purchased varies by product, environment setup, and customer preference; if you are not certain what kind of certificate is required, please mention that when creating the case.

The CSR is required for the **initial** setup of custom domains on Ex Libris hosted environments, and could be required when renewing the certificate.
You will be notified by Ex Libris that your certificate is about to expire. Please make sure that the relevant contact in your institution is subscribed to the relevant mailing list.
Please refer to the **RENEWAL** section below for details regarding the renewal process.

What is a CSR?

A CSR or Certificate Signing request is a block of encoded text that is given to a Certificate Authority when applying for an SSL Certificate. It is generated on the server where the certificate will be installed and contains information that will be included in the certificate such as the organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate. A private key is created at the same time, making a key pair.

A certificate authority will use a CSR to create your SSL certificate, but it does not need the private key. The private key must be kept secret and secure. The private key is not moved from the hosted environment and remains protected at all times.

Certificate production process:

0. A request is received by Ex Libris to use a custom domain name on a hosted environment via SSL.
0. Ex Libris staff will request identifying information from the customer to be used in the creation of the CSR.

0. Ex Libris will generate the CSR and provide it to the customer.
0. The customer will pass the CSR to a Certificate Authority such as GoDaddy, GeoTrust, etc., with a request to receive a signed certificate.
   Please verify that the certificate has SHA2 encryption or higher.
0. The Customer will then pass the signed certificate to Ex Libris to be uploaded to the hosted environment.
1. Customer need to add the DNS entry of the new host name as a CNAME.

Note

The "Time to Live" (TTL) should be configured to no more than 5 minutes

---

Details required to generate the CSR

To generate the CSR, Ex Libris will require the following information:

0. **Common Name**: *The fully-qualified domain name (FQDN), host name, or URL to apply to the certificate. (This URL should have a CNAME pointing to the environment's domain name)*
0. **Organization**: *The name under which the customer's organization is legally registered*
0. **Division**: T*o differentiate between divisions within an organization*
0. **Locality**: *Name of the city in which the customer's organization is registered*
0. **State or Province**: *Name of state or province where the customer's organization is registered (Use FULL NAME - For example: Pennsylvania instead of PA)*
0. **Country**: *The two-letter country code for the country in which the customer's organization is registered*
0. **Email Address**: *An email address to contact the organization. Usually the email address of the certificate administrator or IT department.*

Certificate Renewal Process

Ex Libris will notify customers with hosted certificates when their certificate is about to expire.
Please make sure the relevant contact in your institution has a Support Center user account (refer to these instructions if you need to create one) and subscribed to receive email notifications for the relevant product.
For more information about subscribing to product and hosting updates please follow this link.

Note

Failure to renew the certificate will result in a service disruption for your users, and they will not be able to access the system.
We recommend that this will be handled as soon as possible.

Please contact your Certificate Authority and ask them to renew the certificate. Note that there are 2 options -

Option 1 – renew the certificate ***without*** creating a new private key:

1. Contact your Certificate Authority and ask them to renew the certificate without creating a new private key.
2. Open a support case and attach the renewed SSL certificate, the relevant intermediate certificate and the root certificate to this support case.

Option 2 – renew the certificate ***with*** creating a new private key:

The process for this option are the same as creating a new certificate:

1. Open a support case, and provide the relevant information.
2. Ex Libris will generate the Certificate Signing Request (CSR) and send it to you.
3. Contact the CA and ask them to provide a signed certificate. **Please verify that the certificate has SHA2 encryption or higher.**
4. Attach the renewed SSL certificate, the relevant intermediate certificate and the root certificate to the support case.

Please make sure that:

1. All of the certificates are in PEM format.
2. In order to allow us to efficiently identify and handle the case, when opening it please select:
    - Case Type – Security and Privacy
    - Category – Hosted Infrastructure
    - Sub-category – SSL Certificate Renewal

Important: Certain Certificate Authorities upon creation of a new private key will revoke the old certificate within a short period of time, please verify the CA's policy before renewing the private key and make sure to complete the procedure within the revocation timeframe to avoid any service interruptions.

- **Article last edited:** 16-Sep-2020