Why am I getting a browser warning of ERRCERT COMMON NAME INVALID after updating the SSL certificate on EZproxy

Last updated: Thu, 16 Dec 2021 14:49:55 GMT

Symptom

• Users are getting a web browser warning about the EZproxy SSL certificate right after SSL certificate was updated. The warning is ERR_CERT_COMMON_NAME_INVALID

• The EZproxy prefix being used for HTTPS does not start with login. https://cptest.idm.oclc.org/login?url= is an example.

• The SSL certificate being used does not include the exact EZproxy name in either the CN or SAN fields only the wildcard entry is present.

Applies to

• EZproxy all versions

Resolution

Here is what you need to do to fix the issue:

1. Update the SSL certificate to include both the exact EZproxy name and also the wild card of the EZproxy name. Using the example about *.cptest.idm.oclc.org and cptest.idm.oclc.org must be present on the SSL certificate. It does not matter which value is in which field just both must be present or https://cptest.idm.oclc.org/login?url= will generate the ERR_CERT_COMMON_NAME_INVALID browser warning

Additional information

The EZproxy prefix can also be updated to https://login. to resolve this issue as well.