Option ForceWildcardCertificate

Last updated: Tue, 22 May 2018 18:28:43 GMT

Learn how to use the Open ForceWildcardCertificate config.txt directive to allow EZproxy administrators to treat an installed SSL certificate as a wildcard certificate.

Option ForceWildcardCertificate allows EZproxy administrators to treat the installed SSL certificate as a wildcard certificate. This is necessary in cases where the Certificate Name of the installed SSL certificate does not include a wildcard entry, and the wildcard entry appears instead in the Subject Alternate Name field. This is a rarely used directive, as EZproxy V6.1 and later should read SSL certificates correctly by default.

Option ForceWildcardCertificate is a position-independent directive that interacts with the installed SSL certificate. This directive will cause EZproxy to look in both the Common Name (CN) and the Subject Alternate Name (SAN) fields for a wildcard entry, such as:

* .ezproxy.yourlib.org

This directive is compatible with EZproxy V6.1 and later. EZproxy V6.1 should read the CN and SAN for a wildcard entry by default; however, if you experience any of the problems below, this directive might be necessary:

- Browser warnings when accessing administration https URLs
- Difficulty accessing https hostnames. For example, when you click on the starting point URL http://ezproxy.yourlib.org/login?url=https://www.researchdb.com, you should see it rewritten in your browser as https://www-somedb-com.ezproxy.yourlib.org. If you do not see https URLs rewritten in this way with hyphens you may be experiencing wildcard certificate problems. Adding Option ForceWildcardCertificate should resolve these issues.

Syntax

| Option ForceWildcardCertificate |

Example

When https is enabled, EZproxy checks the Common Name (CN) of its SSL certificate to see if it begins with an asterisk (*). If it does, EZproxy will automatically add "login." to the front of its server name when constructing https URLs that point at its own administrative pages to avoid browser warnings, and it will also change periods to hyphens in the rewritten form of hostnames (e.g., https://ezproxy.yourlib.org/login?url=https://www.researchdb.com will change to https://www-researchdb-com.ezproxy.yourlib.org).

In some instances, the CN of an SSL certificate will not include the asterisk, but instead the wildcard entry will appear as a Subject Alternate Name (SAN). By default, EZProxy V6.1 and later should read both fields; however, if you experience problems with browser warnings or cannot connect to secure URLs, adding this directive to your config.txt could resolve those problems.

Related directives

| Option IgnoreWildcardCertificate |