Learn how to use the `ForceHTTPSLogin` config.txt directive to redirect users to a secure login page in EZproxy. To increase the security of logins, we have enabled the `ForceHTTPSLogin` option by default for all libraries, starting with EZproxy v7.0.

By including `ForceHTTPSLogin` in your config.txt, your users will be redirected to a secure login page whenever they try to access EZproxy resources. This security configuration will keep your server and users’ credentials secure.

`ForceHTTPSLogin` is a position-independent config.txt that presents the login page with a secure https protocol at the beginning of the URL. To use this directive, you must configure your EZproxy to use a secure certificate encrypted with SSL (Secure Socket Layer) technology. For details about SSL Configuration, see [SSL Configuration](#).

### Syntax

```
Option ForceHTTPSLogin
```

This will cause EZproxy to redirect any requests for the login page to the secure, https URL.

### Example

To use `Option ForceHTTPSLogin`, you need to configure EZproxy to listen on a secure port and configure EZproxy to use an SSL certificate. Once you have completed the steps in [SSL Configuration](#), you can enter the following lines in your config.txt to cause EZproxy to redirect to a secure login page whenever a login page is requested:

```
LoginPortSSL 443
Option ForceHTTPSLogin
```

These lines can be entered anywhere in your config.txt; however, most institutions enter these statements towards the top along with other EZproxy configuration information to keep these details separate from the database stanzas.

### Related directives

- [LoginPortSSL](#)