Learn how to use the Option DisableSSLv2 config.txt directive to specify that SSL version 2 handshakes should not be permitted in EZproxy.

Option DisableSSLv2 specifies that SSL version 2 (SSLv2) handshakes should not be permitted.

SSLv2 remains enabled in EZproxy by default for backward compatibility, but is generally regarded as a weak protocol that is best disabled using this option.

This directive is a non-repeatable position-independent that must appear before any LoginPortSSL directives.

Syntax

```
Option DisableSSLv2
```

Examples

Disable 56-bit (and also 40-bit) algorithms plus SSLv2. Unlike OptionDisableSSL40bit, Option DisableSSLv2 must appear explicitly to disable SSLv2 processing. Note how both of these options appear before the first LoginPortSSL directive.

```
Option DisableSSL56bit
Option DisableSSLv2
LoginPortSSL 443
```

Related directives

Option DisableSSL40bit, Option DisableSSL56bit