Option DisableSSL40bit

Learn how to use the Option DisableSSL40bit config.txt directive to specify SSL encryption algorithms that use only 40-bits to be disabled in EZproxy.

Option DisableSSL40bit specifies that SSL encryption algorithms that use only 40-bits should be disabled, and for historic reasons, also disables SSLv2.

40-bit and 56-bit algorithms remain enabled in EZproxy by default for backward compatibility, but are generally regarded as weak protocols that are best disabled using Option DisableSSL56bit.

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

Syntax

Option DisableSSL40bit

Examples

Disable 40-bit algorithms and SSLv2. For historic reasons, the behavior of Option DisableSSLv2 is implied by the presence of Option DisableSSL40bit, but Option DisableSSLv2 is included to avoid confusion. Note how both of these options appear before the first LoginPortSSL directive.

Option DisableSSL40bit
Option DisableSSLv2
LoginPortSSL 443