
[Bundle Resources](#) / [Information Property List](#) / `NSEExceptionRequiresForwardSecrecy`

Property List Key

NSEExceptionRequiresForwardSecrecy

A Boolean value indicating whether to override the perfect forward secrecy requirement.

iOS 9.0+ | iPadOS 9.0+ | macOS 10.11+ | visionOS 1.0+

Details

Type

Boolean

Attributes

Default: YES

Discussion

Set the value for this key to NO to override the requirement that a server support perfect forward secrecy (PFS) for the given domain. Disabling this requirement also removes the key length check described in [Ensure the Network Server Meets Minimum Requirements](#). However, it doesn't impact the TLS version requirement. To control that, use [NSEExceptionMinimumTLSVersion](#).

This key is optional. The default value is YES, which limits the accepted ciphers to those that support PFS through Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange.

See Also

Exceptions

`NSEExceptionAllowsInsecureHTTPLoads`

A Boolean value indicating whether to allow insecure HTTP loads.

`NSEExceptionMinimumTLSVersion`

The minimum Transport Layer Security (TLS) version for network connections.

`NSRequiresCertificateTransparency`

An obsolete Boolean value indicating whether to require Certificate Transparency.