Hardened Runtime Entitlements

Manage security protections and resource access for your macOS apps.

Overview

Enabling the Hardened Runtime capability allows your app to execute with additional security protections and resource access restrictions. Turn on individual protections and restrictions using entitlements.

Important

To upload a macOS app to be notarized, you must enable the Hardened Runtime capability. For more information about notarization, see Notarizing Your App Before Distribution.

Topics

Runtime Exceptions

Allow Execution of JIT-compiled Code Entitlement

A Boolean value that indicates whether the app may create writable and executable memory using the `MAP_JIT` flag.
Key: com.apple.security.cs.allow-jit

Allow Unsigned Executable Memory Entitlement

A Boolean value that indicates whether the app may create writable and executable memory without using the `MAP_JIT` flag.
Key: com.apple.security.cs.allow-unsigned-executable-memory

Allow DYLD Environment Variables Entitlement

A Boolean value that indicates whether the app may be impacted by `dyld` environment variables, which can be used to inject code into the process.
Key: com.apple.security.cs.allow-dyld-environment-variables

Disable Library Validation Entitlement

A Boolean value that indicates whether the app may load plug-ins or frameworks signed by other developers.
Key: com.apple.security.cs.disable-library-validation

Disable Executable Memory Protection Entitlement

A Boolean value that indicates whether to disable code signing protections while launching the app.
Key: com.apple.security.cs.disable-executable-page-protection

Debugging Tool Entitlement

A Boolean value that indicates whether the app is a debugger and may attach to other processes or get task ports.
Key: com.apple.security.cs.debugger

Resource Access

Audio Input Entitlement

A Boolean value that indicates whether the app may record audio using the built-in microphone and access audio input using Core Audio.

Key: com.apple.security.device.audio-input

Camera Entitlement

A Boolean value that indicates whether the app may capture movies and still images using the built-in camera.

Key: com.apple.security.device.camera

Location Entitlement

A Boolean value that indicates whether the app may access location information from Location Services.

Key: com.apple.security.personal-information.location

Address Book Entitlement

A Boolean value that indicates whether the app may have read-write access to contacts in the user's address book.

Key: com.apple.security.personal-information.addressbook

Calendars Entitlement

A Boolean value that indicates whether the app may have read-write access to the user's calendar.

Key: com.apple.security.personal-information.calendars

Photos Library Entitlement

A Boolean value that indicates whether the app may have read-write access to the user's Photos library.

Key: com.apple.security.personal-information.photos-library

Apple Events Entitlement

A Boolean value that indicates whether the app may send Apple Events to other apps.

Key: com.apple.security.automation.apple-events

See Also

Secure Code

Code Signing Services

Examine and validate signed code running on the system.

Notarizing Your App Before Distribution

Give users even more confidence in your software by submitting it to Apple for notarization.

Preparing Your App to Work with Pointer Authentication

Test your app against the arm64e architecture to ensure that it works seamlessly with enhanced security features.

App Sandbox Entitlements

Manage access to system resources and user data in macOS apps to contain damage if an app becomes compromised.