Sample Code

# Monitoring System Events with Endpoint Security

Receive notifications and authorization requests for sensitive operations by creating an Endpoint Security client for your app.

Download

macOS 11.0+ | Xcode 13.0+

## Overview

> **Note**
>
> This sample code project is associated with WWDC 2020 session 10159: Build an Endpoint Security App. For further information, see WWDC 2019 session 702: System Extensions and DriverKit.

`SampleEndpointApp` is a minimal system extension that shows how to use the Endpoint Security library. You can configure the extension to either receive notifications of events after they occur, or to allow or deny in-flight events.

## Configure the Sample Code Project

This sample code project only runs on macOS 11 and later.

You can build the project to receive either `NOTIFY` or `AUTH` events. You control this in the Xcode file inspector.

- For NOTIFY events: Select `notify_demo.c` and, in the file inspector, select the “Extension” target in the “Target Membership” section.
- For AUTH events: Select `auth_demo.c` and, in the file inspector, select the “Extension” target in the “Target Membership” section.

You must set the “Extension” target membership on exactly one of these two files.

To install the system extension:

1. Generate your Developer ID certificate. Refer to Developer ID for instructions.
2. Request the Endpoint Security entitlement; see System Extensions and DriverKit.
3. In Xcode, build and sign both the app and the extension with your Developer provisioning profile.
4. Copy the app to `/Applications`, and launch it from there. You can only install System Extensions for apps launched from the `/Applications` folder.
5. Click “Install Extension” and follow the prompts to allow the extension to launch.
6. In System Preferences, choose Security & Privacy > Privacy. Scroll to “Full Disk Access” and grant permission to use the extension.
7. In Terminal, run `systemextensionsctl list` to verify that the system extension is activated.
8. In Terminal, run `sudo launchctl list <Team-ID>.com.example.apple-samplecode.SampleEndpointApp.Extension` to verify that the system extension is running.

After installing the system extension, you can monitor its activity as follows:

- If you built `notify_demo.c`, open the system log to see log messages every time a process executes, forks, or exits.
- If you built `auth_demo.c`, the extension blocks any operations on an EICAR test file on your system. The extension also prevents writing to any file that starts with the read-only prefix, defined in `auth_demo.c` as `/usr/bin/local`. For process executions, the extension denies new execs that use the signing ID `com.apple.TextEdit`; this means the extension will prevent the default `TextEdit.app` from launching.

To uninstall the system extension:

1. In Terminal, run `systemextensionsctl uninstall <Team-ID> com.example.apple-samplecode.SampleEndpointApp.Extension`.
2. Alternatively, drag the sample app from the `/Applications` folder to the Trash.

# See Also

## Event Monitoring

- Client

  An opaque type that maintains Endpoint Security client state, and functions related to this type.

- Message

  A type used by Endpoint Security to notify your client when a monitored action occurs.

- Event Types

  Types used by messages to deliver details specific to different kinds of Endpoint Security events.