Allow System Extensions with Addigy MDM

https://support.addigy.com/hc/en-us/articles/4403549605267-Allow-System-Extensions-with-Addigy-MDM

What are System Extensions?

Addigy Mobile Device Management (MDM) capabilities offer functionality to allow System Extensions. As Kexts, also known as legacy system extensions, are being deprecated for newer macOS systems (Catalina and above) System Extensions allow software (network extensions and endpoint security) to extend functionality without requesting kernel-level access.

Prerequisites

In order to use this functionality, the device must be managed by Addigy MDM and have checked into the Addigy MDM Server properly. For help setting up Addigy MDM, see our article Addigy Mobile Device Management (MDM) Integration. Also, System Extensions payloads will fail to deploy unless the Addigy MDM Profile has been Approved on the device.

Configuring the System Extensions Policy

For building a System Extensions payload, first, let's navigate to **Catalog > MDM Profiles > New.** Then, in the selection window, search for **System Extensions**.

Image not found or type unknown

Image not found or type unknown

Load the appropriate **Team ID** or **Identifiers** for the corresponding software. To note, we recommend having each unique software separated into its own System Extension profile.

Obtaining System Extensions Identifiers

If you already have the Team ID or Identifiers, skip the next step and go to Deploying the Payload

If you still need to obtain this information, please follow our separate guide on How To Get The Team ID, Bundle ID, and Code Requirement.
Through the steps above you will be able to obtain the Identifiers as well as Code Requirement for the specified application.

Deploying the Payload

You can allow **Allowed System Extensions**, **Allowed System Extensions Types**, or **Allowed Team Identifiers** (Only fill out one of them).

Image not found or type unknown

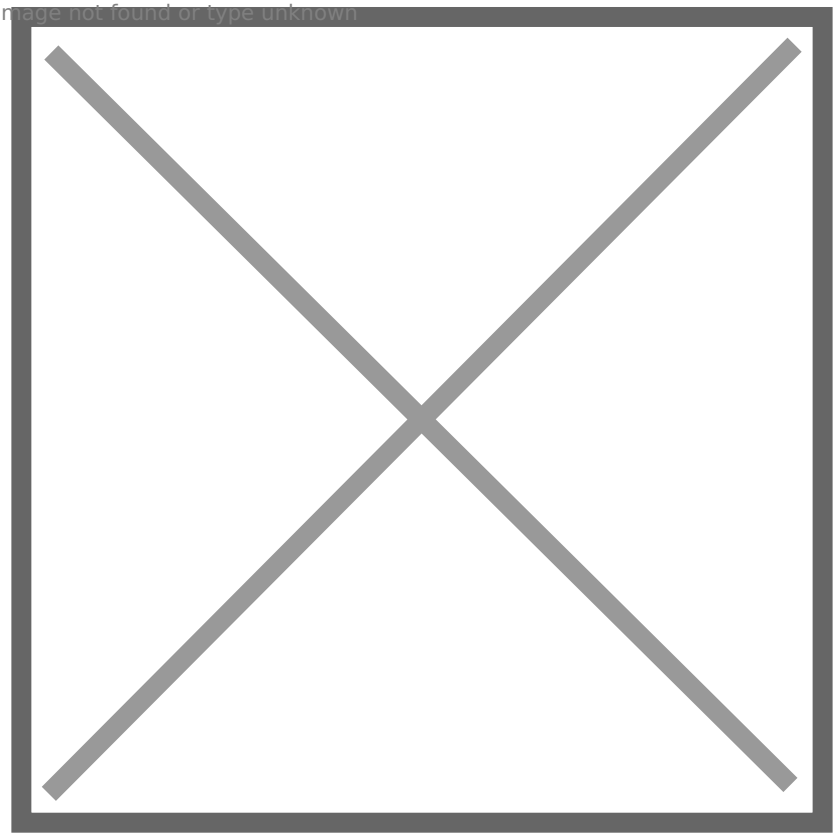


Image not found or type unknown

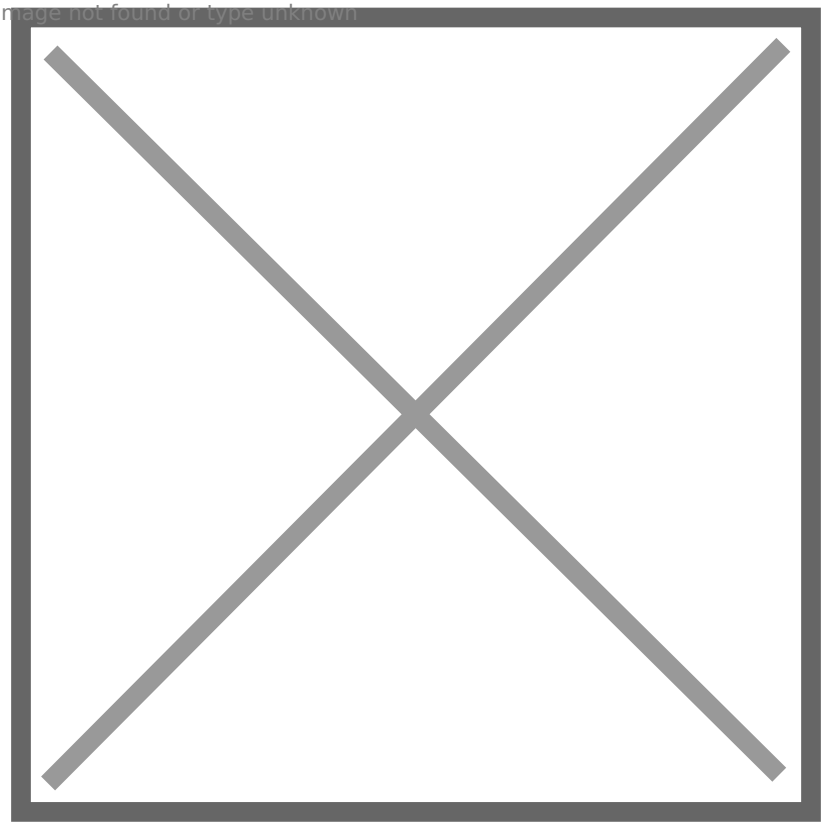
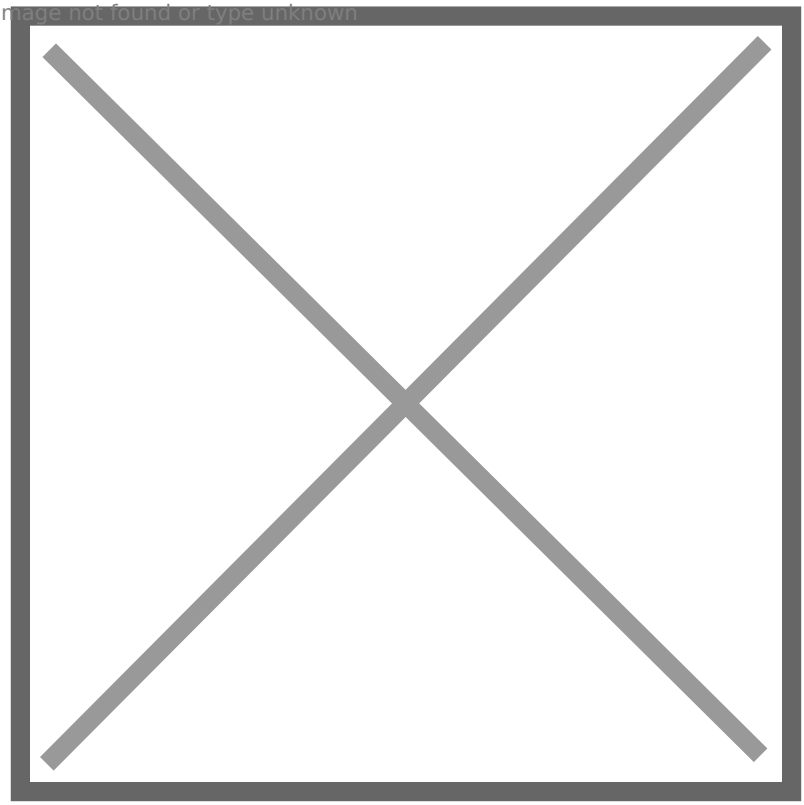


Image not found or type unknown



Note: Whitelisting an app based on the Team ID alone will approve any Bundle Identifiers tied to that Team ID. For example, if an app has 6 Bundle IDs all tied to the Team ID "AADH234", I can whitelist just that and all 6 Bundle IDs will be allowed.

Once the identifiers are set, select Create Configuration to complete the process.
Additionally, if your software has multiple Bundle Identifiers, you can add multiple by using a comma (,) to separate them, see the example below:

com.bitdefender.FileProtect, com.bitdefender.SelfProtect, com.bitdefender.TMProtection, com.bitdefender.atc, com.bitdefender.mdredr, com.bitdefender.mdrnet, com.bitdefender.mdrfp, com.bitdefender.devmac, com.bitdefender.EndpointSecurityforMac, BDLDaemon

After this has been configured you can begin assigning it to your policies.

You're all set! If you experience any issues with allow-listing/whitelisting the app, please refer to our troubleshooting article here:

FAQ: App(s) not Whitelisting via MDM Profile (PPPC, System Extensions, etc..)

Revision #1
Created 31 July 2024 19:31:30 by ColtM
Updated 7 August 2024 23:24:40 by ColtM