

# User-Approved MDM Enrollment and Legacy Kernel Extensions (macOS)

## Current scope

User-approved MDM enrollment was introduced with macOS High Sierra for security-sensitive management. Macs enrolled through Automated Device Enrollment satisfy the approval requirement without a separate user approval step.

For current deployments, identify which extension type the vendor ships before choosing a FileWave payload:

- Use a [System Extensions payload](#) for modern system extensions.
- Use a [Kernel Extension Policy payload](#) only when a vendor still requires a legacy kernel extension.

The detailed High Sierra examples below are retained for administrators supporting older software that still uses kernel extensions.

[Apple: Enterprise management of legacy system extensions](#)

 Check the vendor's current deployment guide. System Extension, Network Extension, Full Disk Access, and legacy Kernel Extension approvals are separate controls. Deploy only the payloads required by the installed product and test them on the macOS versions in your fleet.

## Historical High Sierra kernel-extension behavior

### User Approved MDM Enrolment

Currently, User Approved MDM Enrolment relies on the device being enrolled; the method of enrolment does not matter yet but will do in future releases. At this point, the enrolment must be either:

- DEP enrolment (user approval not required)
- User installing the enrolment profile manually
- User accepts the enrolment profile through System Preferences > Profiles:

# FileWave MDM

## FileWave **Unverified**

⚠️ Functionality may be limited until this profile is approved.

Approve...

You will notice this approval box in 10.13.2, if the method of enrolment was hidden from the user, e.g. scripted. Devices enrolled on earlier versions and then upgraded will automatically be MDM enrolled as User Approved.

## Kernel Extensions

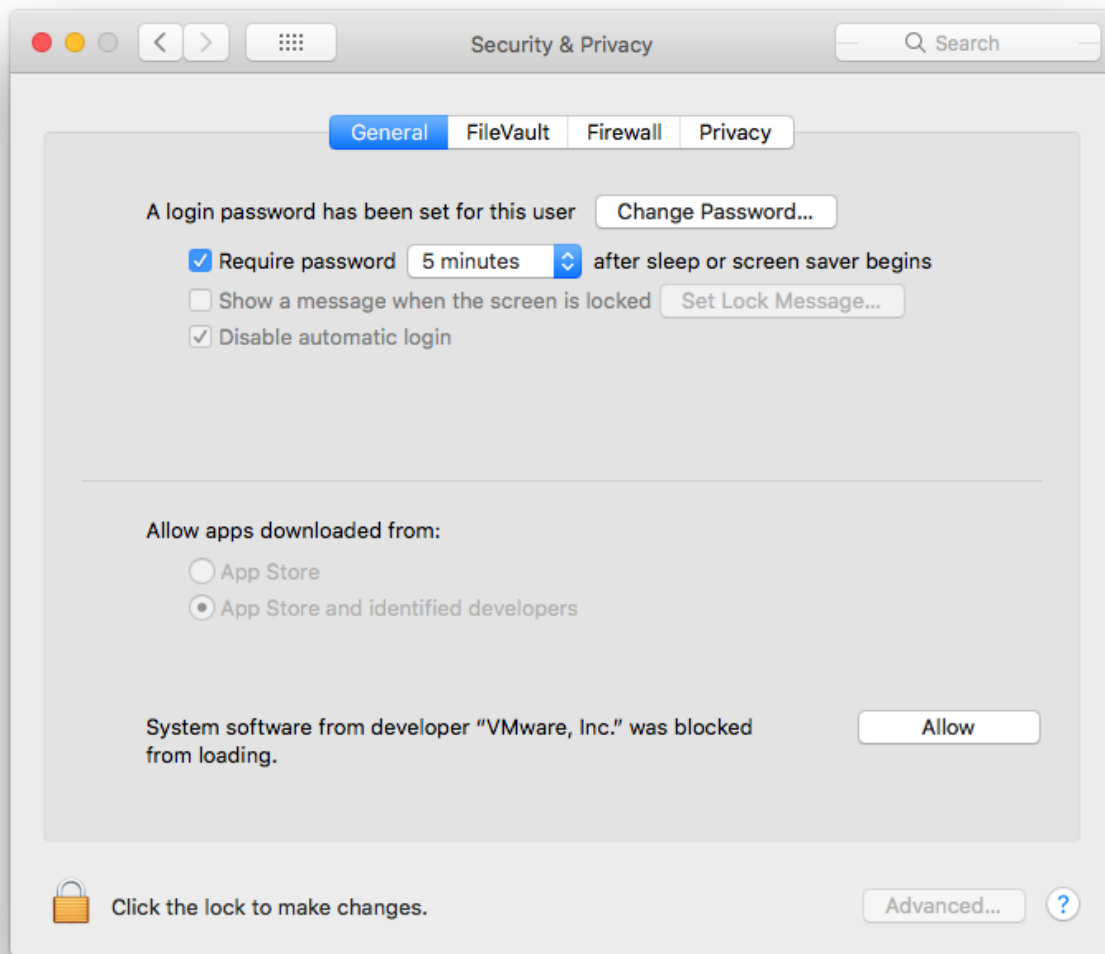
Apple introduced a halfway house with the release of 10.13. Apple has now released version 10.13.4 which has full implementation of this feature.

### How does this affect kernel extensions?

Attempts to install a Kernel Extension with a device that is not enrolled into MDM will be greeted with the following message:



To approve the Kernel Extension will either require MDM enrolment or the user allowing the blocked Extension to run, via System Preferences > Security & Privacy > General:



## What happens if I already have kernel extensions installed?

Any extension installed prior to upgrading to 10.13 High Sierra will continue to work, only newly installed kernel extensions will be affected.

Once a particular kernel extension is approved, subsequent upgrades to that kernel extension will automatically be user-approved.

## Managing Kernel Extensions through MDM

Prior to version 10.13.4, there is no management beyond having the device enrolled into MDM. However, with 10.13.4, management is now available through the Kernel Extension Policy payload, allowing extension loading without user consent when enrolled appropriately; the payload can only be delivered with MDM, to devices that are User Approved MDM Enrolled. This could result in apps relying on kernel extensions to stop functioning properly (e.g. VPN clients, antivirus software).

As of FileWave version 12.7.0, the Kernel Extensions payload was introduced. To allow Kernel Extensions requires either:

1. 'Team Identifier'
2. Individually using the 'Kernel Extension bundle ID'.

These values are stored locally on a device after installation. Therefore, to find these values involves installing them on a device and then reading these values from a file, e.g., for a machine that has VMware Tools installed. One machine could have all Extensions installed prior to running the command to list all necessary Kernel Extensions.

```
$ sqlite3 /var/db/SystemPolicyConfiguration/KextPolicy 'select team_id,bundle_id from kext_policy;'
EG7KH642X6|com.vmware.kext.VMwareGfx
EG7KH642X6|com.vmware.kext.vmhgfs
```

This lists the Team Identifier followed by the Bundle ID for two Kernel Extensions that have been added with the installation of VMware Tools. Both have the same Team Identifier, but have differing Bundle IDs.

1. To just use Team Identifier, add the returned Team Identifier from the command for the Kernel Extensions you wish to approve, to the 'Allowed Team Identifiers' whitelist. All Kernel Extensions with this Team Identifier will be whitelisted.
2. To only allow certain Kernel Extensions, instead use the 'Allowed Kernel Extensions' whitelist and add both Team Identifier and Bundle ID. Note, legacy Extensions may not have a Team Identifier. For those that don't, just supply the Bundle ID and leave the Team Identifier empty.

There is also a community of users that are adding Identifiers and Bundle IDs which could save you having to instal in advance.

## Community Kernel Extensions List

Data in this list is not checked in any way. As this is in place for security reasons and anyone can add information to this file, use with care:

[Community Kernel Extensions List](#)

## Can I use User Approved Kernel Extension loading without MDM?

Yes. This however involves booting the computer into recovery mode and using the following command:

```
“ $ spctl
```

See the man page for required options:

<https://developer.apple.com/legacy/library/documentation/Darwin/Reference/ManPages/man8/spctl.8.html>

N.B. This is stored in NVRAM. If you reset the NVRAM, you will lose the ability to use User Approved Kernel Extension loading with this method until the steps are retraced. A firmware password could be set to prevent unauthorized NVRAM resets.

## Extensions Payload

The Extensions payload should not be confused with the Kernel Extensions payload.

<https://help.apple.com/profilemanager/mac/5.4/#/apd58550e429>

The Extensions payload controls those extensions visible through the Extensions System Preferences and will not affect Kernel Extensions

---

🔄Revision #4

★Created 2023-07-15 00:29:28 UTC by Josh Levitsky

✎Updated 2026-07-31 12:55:50 UTC by Josh Levitsky