System extensions in macOS

Archived: 2026-04-05 18:38:12 UTC

A Mac with macOS 10.15 or later enables developers to extend the capabilities of macOS by installing and managing system extensions that run in user space rather than at the kernel level. By running in user space, system extensions increase the stability and security of macOS. Even though kexts inherently have full access to the entire operating system, extensions running in user space are granted only the privileges necessary to perform their specified function.

System extensions support robust management using a device management service, including the ability to allow all extensions from a specific developer or of a specific type (like network extensions) to load without user interaction. Optionally, a device management service can disallow users from approving their own system extensions from loading.

For a Mac with macOS 12.0.1 or later, a dictionary in the System Extensions payload—called `RemovableSystemExtensions` —allows a device management service administrator to specify which apps can remove their own system extensions. No local administrator authentication is required to remove the system extensions. This is especially useful for vendors that may provide automated uninstallers for their apps.

For a Mac with macOS 11.3 through macOS 11.6.4, making changes to a system extension profile directly affects the state of an extension. For example, if an extension is pending approval and a configuration profile is pushed that allows the extension, the extension is allowed to load. Conversely, if an approval is revoked, the system extension is unloaded and marked for removal on the next restart of the Mac. If a system extension tries to unload itself, an interactive authentication dialog appears that requires administrator credentials to authorize the unloading.

Kernel extensions

For a Mac with macOS 11 or later, if third-party kernel extensions (kexts) are enabled, they can’t be loaded into the kernel on demand. They require the user’s approval and restarting of the macOS to load the changes into the kernel, and they also require that the secure boot be configured to Reduced Security on a Mac with Apple silicon.

Developers can use frameworks such as DriverKit and NetworkExtension to write USB and human interface drivers, endpoint security tools (like data loss prevention or other endpoint agents), and VPN and network tools, all without needing to write kexts. Third-party security agents should be used only if they take advantage of these APIs or have a robust road map to transition to them and away from kernel extensions.

Important: Kexts are no longer recommended for macOS. Kexts risk the integrity and reliability of the operating system. Users should prefer solutions that don’t require extending the kernel and use system extensions instead.

Add kexts on an Intel-based or Apple silicon Mac with macOS 11 or later

If you need to use kernel extensions, review the approval methods based on enrollment method.

Enrollment method	**Approval method**
Not enrolled User Enrollment	When a new kext is installed and there's an attempt to load it, a restart needs to be initiated by the user from the warning dialog in: • *macOS 13 or later:* Apple menu > System Settings > Privacy & Security. • *macOS 12.0.1 or earlier:* Apple menu > System Preferences, > Security & Privacy. This restart initiates the rebuild of the AuxKC before to the kernel booting.
Device Enrollment Automated Device Enrollment	Every time a new kext is installed and there's an attempt to load it, a restart needs to be initiated by either: • A local administrator account, from the warning in Privacy & Security in System Settings (macOS 13 or later) or the Security & Privacy pane of System Preferences (macOS 12.0.1 or earlier). A device management service can also allow this for standard users. • The device management service itself, using the `RestartDevice` command with `RebuildCache` flagged. The AuxKC rebuilds the next time the Mac restarts. kexts already discovered by macOS (for example, loaded by their software and blocked) are included, and the device management service can supply ones that haven't yet attempted to load using the `KextPaths` key. *Note:* The device management service first needs to install a kext allow list profile that specifies the kext. A Mac with macOS 11.3 or later optionally allows the service to notify the user to complete the restart at their convenience.

Additional steps to add kexts on a Mac with Apple silicon

If you're adding kernel extensions on a Mac with Apple silicon, you need to take additional steps.

Enrollment method	**Approval method**
Not enrolled	Kext management by the user requires a restart to recoveryOS to downgrade security settings. The user needs to press and hold the power button to restart into recoveryOS and authenticate as an administrator. Only when recoveryOS is entered using the power button press does the Secure Enclave accept the change of policy. The user needs to then select the checkbox Reduced Security and the option “Allow user management of kernel extensions from identified developers” and restart the Mac.
User Enrollment	The user needs to restart into recoveryOS to downgrade security settings. The user needs to press and hold the power button to restart into recoveryOS and authenticate as a local administrator. Only when recoveryOS is entered using the power button press does the Secure Enclave accept the change of policy. The user needs to then select Reduced Security, check “Allow user management of kernel extensions from identified developers,” and restart the Mac.
Device Enrollment	The device management service needs to notify the user to restart into recoveryOS to downgrade security settings. The user needs to press and hold the power button to restart into recoveryOS and authenticate as an administrator. Only when using the power button press does the Secure Enclave accept the change of policy. The user needs to then select Reduced Security, select “Allow remote management of kernel extensions and automatic software updates,” and restart the Mac. To learn if this feature is supported for your devices, consult your developer’s device management service documentation.
Automated Device Enrollment (The serial number of the Mac needs to appear in Apple School Manager or Apple Business Manager, and the Mac needs to enroll in a device management service that links to	Device management services can manage this automatically. To learn if this feature is supported for your devices, consult your developer’s device management service documentation.

Enrollment method	Approval method
Apple School Manager or Apple Business Manager.)	

Kernel extensions with System Integrity Protection

- If System Integrity Protection (SIP) is enabled, the signature of each kext is verified before being included in the AuxKC.
- If SIP is turned off, the kext signature isn’t enforced.

This approach allows Permissive Security flows for developers or users who aren’t part of the Apple Developer Program to test kexts before they’re signed.
