

Profiles in macOS 11 Big Sur and beyond must be installed via MDM

Prior to Big Sur, profiles could be installed on macOS devices in multiple ways, including:

- Opening a profile locally in System Preferences
- Command line tools
- Via MDM to devices that are MDM enrolled


FileWave had the ability to use either of the latter two options, defaulting to MDM if the device were MDM enrolled at the time of receiving the association.

As of Big Sur, Apple made a fundamental change, denying the ability to add profiles using command line tools; they may still be removed though. This leaves MDM as the only manageable option in Big Sur onwards.

FileWave was required to remember the method of profile installation: via FileWave Client app or via MDM. Each of these methods uses a different channel to install the profile; to change channel requires removing the profile and re-installing it. Note though, that updating profiles alone could still be achieved and will use the same method of delivery without consequence where allowed.


Example:

- Associate a Dock profile to a non-MDM enrolled device and Update Model
- Profile will install using the FileWave Client App
- Subsequently MDM enrol the device
- Update the dock profile and Update Model
- The update of the profile will continue to be handled using the FileWave Client App
- Newly associated profiles would though be handled by MDM.
- Remove the association of the Dock profile, Update Model
- Once removed, re-associate the Dock profile and Update Model
- Since the device is now MDM enrolled, the profile will be delivered using MDM, as will any updates to this profile

 Note that not every type of change that a profile makes can be cleanly undone simply by removing the profile. One example would be if you add a printer via profile and then remove the profile the printer will remain. Always test adding and take a look at what happens when removing a setting.

Impact

Consequences can therefore occur when devices are upgraded to macOS Big Sur or higher.

 If devices rely upon profiles, for example providing network connectivity, and the profile is removed to be re-installed, the network will be lost and the new profile will never become installed until the device is back online. As such, FileWave will not attempt to change the channel of delivery of these profiles, but careful consideration should be contemplated when manually attempting to use this process. Other examples could include profiles containing certificates, VPN, etc.

Devices not MDM enrolled

Where devices are not MDM enrolled:

- Any associated profile would have been installed using the FileWave Client App prior to Big Sur
- After upgrading to Big Sur, profiles would remain installed
- Once on Big Sur any attempt to make changes to the profile will result in a failure to deliver the update
- Once on Big Sur any new profile associations will also fail
- Disassociation of a profile will remove the profile

Device MDM enrolled after profile installation

When not MDM enrolled, the above would still be of consideration. However after MDM enrolled:

- Any new association will install via MDM
- Removing an association, allowing the device to remove the profile and then re-associating the profile will then install the profile using MDM

This is the same impact even if not upgraded to Big Sur

Resolution

Management of profiles on Big Sur relies upon devices being MDM enrolled. If not they may not be installed or updated. As such devices must be MDM enrolled

Where profiles were installed not using MDM, the only way for these profiles to become managed is by removing the association,

allowing the device to remove the profile and then creating a new association.

As highlighted above, take great care in the choice of profile removal if you have network reliance on installed profiles. This will require some manual method of transition where this is the case.

Additional Information

If the Client Info of a Device does not have a 'Command History' tab, it should imply that the device is not MDM enrolled. In this instance, only the FileWave Client App may instal Filesets of any type. Note Apple's VPP also requires MDM.

🕒Revision #3
★Created 15 July 2023 00:47:51 by Josh Levitsky
✍Updated 29 August 2023 21:29:31 by Josh Levitsky