

Apple MDM

- [Profile Payload Planning](#)
- [Inventory Items in Profiles](#)

Profile Payload Planning

What

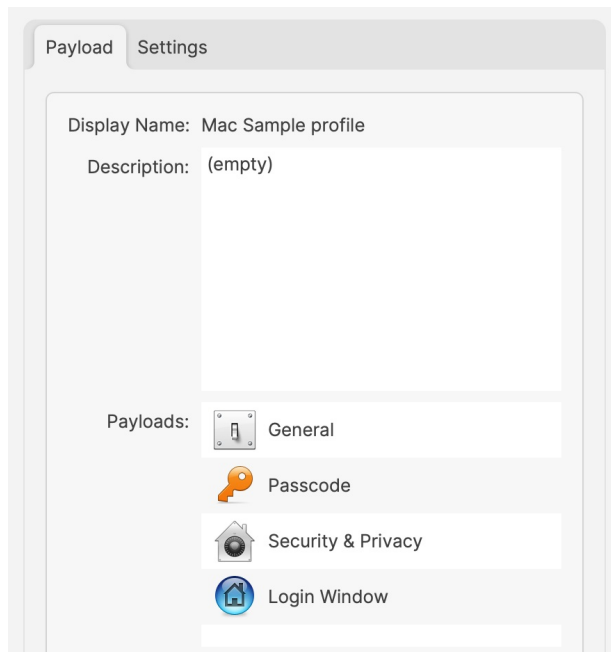
- Apple Profiles contain Payloads
- Payloads provide configuration options
- As of macOS 11, Profiles may only be delivered to devices which are also MDM enrolled. (MDM is the only enrolment option for iOS and similar OS types).

That's the fundamentals of Profiles in a nutshell, but there is more consideration.

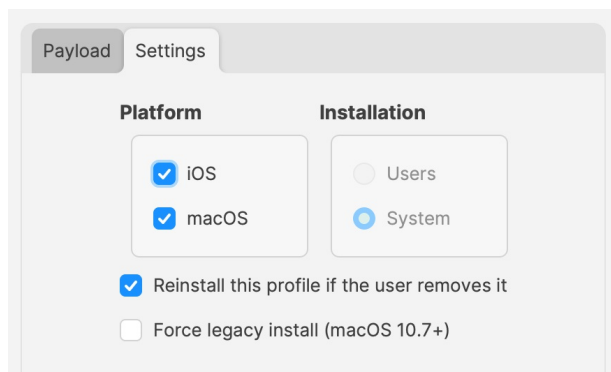
Key aspects:

- A Profile may contain multiple Payload types
- Multiple Profiles may be pushed to each device
- macOS devices have an additional option: should the Profile be set against the User or the System?

Example Profile with multiple Payloads:



For the same above Payload, the Settings show:



Apple's implementation is such, that only one local user can be managed (the first user after enrolment). However, any amount of directory users can be managed. This restriction applies to User set Profiles only.

Not all Payload types can be User or System. Some may only be User or only System, rather than the choice. From the screenshot above, the Settings show System is the only choice and is therefore greyed out.

Possibly, one of the most important consideration:

Where multiple Profiles are assigned which contain the same Payload type (but differing settings), Apple do not guarantee the experience. There used to be a suggestion for restrictive Payload settings, the most restrictive wins, but other Payload types

How

Firstly, overlapping Payloads should be avoided, to ensure experience is by design, not luck.

Next, from the above, Profiles can contain many Payloads, but should they? Consider:

- Having an experience that is undesired in the Profile
- Needing to 'Force Reinstall' a Profile

Undesired Experience:

More items in the Profile makes it harder to identify anything occurring that is undesired.

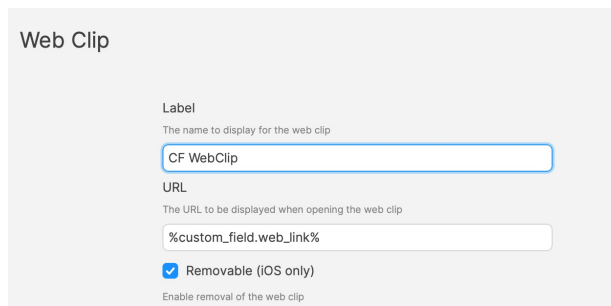
Removing the undesired experience temporarily, whilst identifying, involves removing the entire Profile, which could easily be undesirable in its own right. By creating multiple Profiles with different Payloads, instead of one massive Profile with lots of Payloads, makes identifying and resolving unexpected experiences, much more easily with less impact.

Force Reinstall

This option can be desirable for a few reasons, but consider this example:

- Profile contains a Payload with a value that is set by way of a Custom Field or Inventory item.
- Custom Field or Inventory Item is altered and devices need that new value to be applied within the Profile Payload

An example Web Clip Payload, using a Custom Field to populate the value:



The screenshot shows a 'Web Clip' configuration interface. It has a 'Label' field with the value 'CF WebClip' and a description 'The name to display for the web clip'. Below it is a 'URL' field with the value '%custom_field.web_link%' and a description 'The URL to be displayed when opening the web clip'. At the bottom, there is a checkbox labeled 'Removable (iOS only)' which is checked, with a sub-label 'Enable removal of the web clip'.

When a Profile is altered, FileWave will note the Profile as Modified and the Profile will be redelivered with the new settings. However, when changing Custom Field or Inventory values, there is no change to the Profile. The Payload referencing the Custom Field or Inventory item is still referencing this, it is only during delivery that the value is noted and entered in the Profile. As such, if the referenced Custom Field or Inventory values are altered for devices, the current Profile will need to be reinstalled. A 'Force Reinstall' will ensure this occurs, but two things occur from this action. The current Profile is removed and the updated Profile is installed. Consider, what is the consequence of Profile removal?

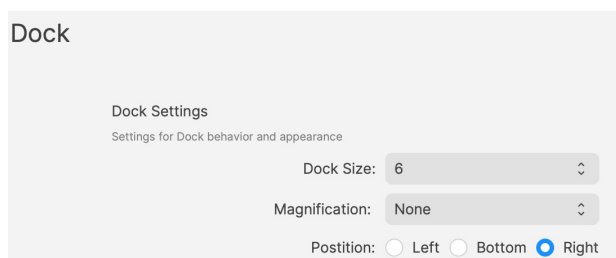
With the above in mind, always consider what is being included in a Profile and therefore keep each Profile lean in content; try not to overload too many Payloads into one Profile.

Overlapping Payloads

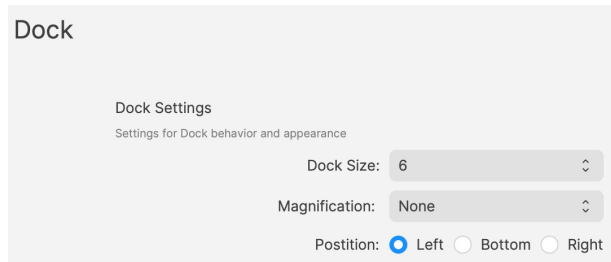
What is an overlapping Payload. This is when two or more Profiles are trying to manage the same thing, but with different settings. This shouldn't be confused with multiple allowed Payloads.

For example:

Profiles to manage the Dock. One Profile sets the dock on the right and the other on the left. This is overlapping and should be avoided:



The screenshot shows a 'Dock Settings' configuration interface. It has a title 'Dock Settings' and a subtitle 'Settings for Dock behavior and appearance'. There are three settings: 'Dock Size' set to '6', 'Magnification' set to 'None', and 'Position' with radio buttons for 'Left', 'Bottom', and 'Right'. The 'Right' radio button is selected.



If both of the above were assigned to a device, how could the device possibly determine which should be obeyed?

Profile to provide certificates. One Profile provides one certificate and another Profile provides a different certificate. This isn't overlapping. Providing multiple certificates is desirable and need not be from one single Profile.

User vs System

Within the settings of Profiles is an option to define whether the Profile should apply to users or system. Some Payloads may be set as User or System only, but not either, whilst others may be either. A Profile must have a setting, so a default will be used when a Profile Payload is first added. Always check to confirm it is set as desired.

A Profile may only have one setting applied. FileWave will therefore prevent the addition of a User only Payload to a Profile already containing another Payload set as System. However, where Payloads may be either, if a Profile already contains a Payload, any additional Payloads that can be added will all be set with the same setting.

For example:

- Create a new Profile and add the Login Window Payload
- Save the Profile and re-open to observe the Settings (should be shown as System and greyed out)
- Create another new Profile and add a Dock Payload
- Save the Profile and re-open to observe the Settings (should show as either System or User, but defaulted to System).
- Change to User, save and re-observe the change

It can be seen that the Login Window is System only, yet the Dock Payload could be either

- Re-open the Login Window Profile created above and add the Dock Payload to this Profile
- Save and re-open to observe the Settings

The Settings remain as System and the applied Dock Payload will therefore be set for the System and not User. If a Dock Profile of User were required, it should not be included in a Profile that already contains a Payload that is set as System.

Why

Should all of the above be of consideration? Why would User be chosen over System? If System will work for all users, why not just set all Profiles as System where possible. However, what if the settings included were only for users, but not for a hidden Admin account. This local admin account is not managed by MDM. By setting System level, any Profiles built this way will impact this user, along with the managed local user and any directory users. This may be undesirable. Passcode policy could be an example.

Some Payload types require certain types of enrolment. Many Payload settings require Supervision, for example. macOS devices managed via User Enrolment, do not qualify as Supervised.

- ☒ Allow use of iMessage (Supervised devices only)
- ☒ Allow Apple Music (Supervised devices only)
- ☒ Allow Radio (Supervised devices only)
- ☒ Allow installing apps using Apple Configurator and iTunes
 - ☒ Allow installing apps using App Store (Supervised devices only)
 - ☒ Allow automatic app downloads (Supervised devices only)
- ☒ Allow removing apps (Supervised devices only)
- ☒ Allow removing system apps (Supervised devices only)
- ☒ Allow App Clips (Supervised devices only)
- ☒ Allow In-App Purchase

Planning

The above comes down to planning.

Profiles could contain multiple Payloads based upon functionality and for User or System determined targeting. Who needs to be managed? Local user (all or just managed) and/or directory users.

Consider the impact if a Profile were 'Force Reinstalled' or if it was deemed necessary to temporarily remove the association to one or more devices, for whatever reason.

Also give thought to how devices will be purchased and enrolled depending upon what needs to be managed. Using a BYOD scheme and only using User Enrolment will greatly reduce what can be managed, whilst ADE(DEP) gives the maximum amount of control through Profiles.

Will the choice made, incur additional concerns over security, if desired management cannot be achieved?

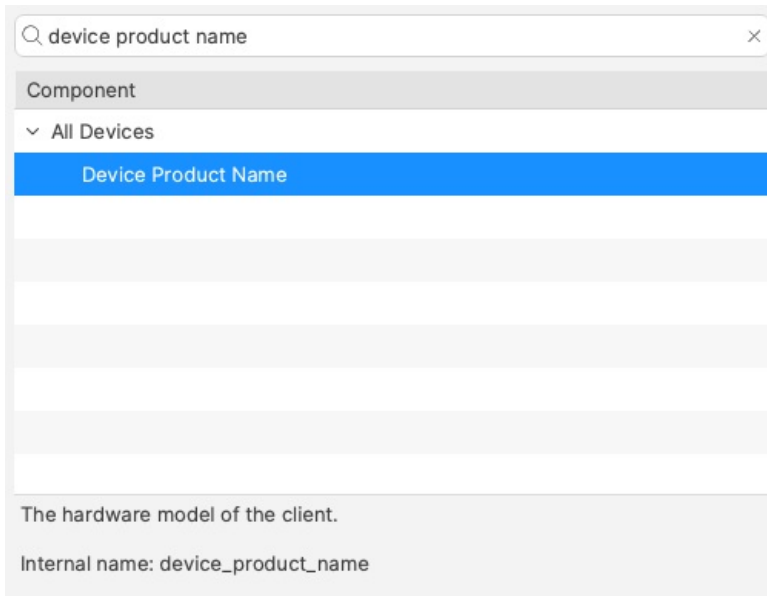
Inventory Items in Profiles

What

- Each Inventory Item has an Internal Name, including Custom Fields which provide extended inventory
- The Internal Name can be used to reference any Inventory Items in Profiles

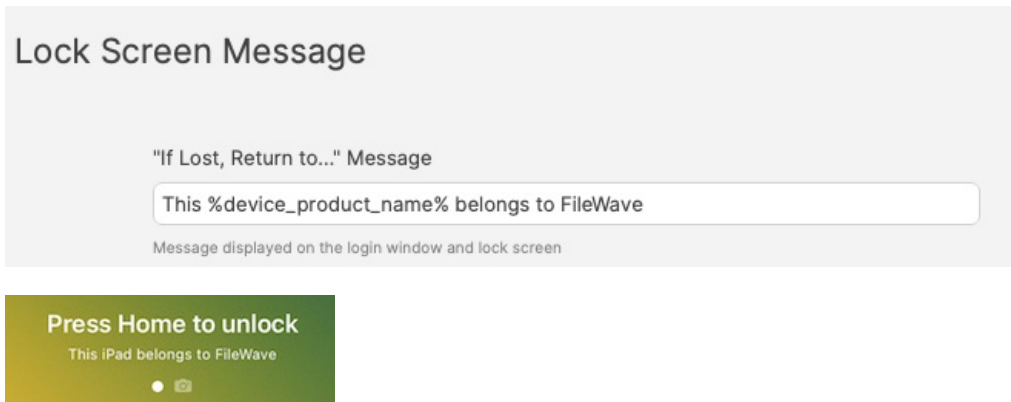
When

Internal Name of an Inventory Item may be located from the Inventory Query Editor. Example shows the Internal Name: 'device_product_name'



The screenshot shows a search interface with a search bar containing 'device product name'. Below the search bar is a table with a header 'Component' and a sub-header 'All Devices'. The table contains one row with the text 'Device Product Name'. Below the table, there is a description: 'The hardware model of the client.' and the internal name: 'device_product_name'.

This may be added into a Profile, effectively customising the Profile per device or user:

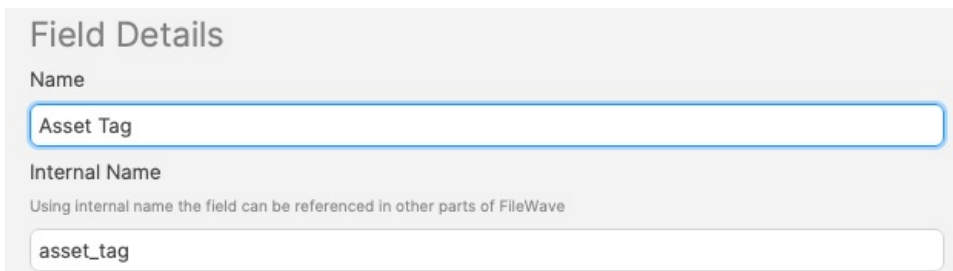


The screenshot shows the 'Lock Screen Message' configuration interface. It includes a section for 'If Lost, Return to...' Message with a text input field containing 'This %device_product_name% belongs to FileWave'. Below this, it states 'Message displayed on the login window and lock screen'. Below the configuration, there is a visual representation of the lock screen message: 'Press Home to unlock' followed by 'This iPad belongs to FileWave' and a home button icon.

Custom Fields

Associated Custom Fields may also be used with Payloads settings of Profiles. Extending the above example, consider a Custom Field for Asset Tag:

Custom Field Definition



The screenshot shows the 'Field Details' form for a custom field. It includes a 'Name' field with the value 'Asset Tag' and an 'Internal Name' field with the value 'asset_tag'. Below the internal name field, it states 'Using internal name the field can be referenced in other parts of FileWave'.

Profile Payload

Lock Screen Message

"If Lost, Return to..." Message

This %device_product_name% belongs to FileWave.

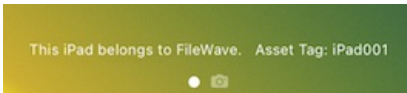
Message displayed on the login window and lock screen

Asset Tag Information

Asset Tag: %asset_tag%

Message displayed at the bottom of the login window and lock screen.

Lock Screen



Improvement

When referencing a Custom Field in a Profile Payload, it could be referenced in one of two ways. From the above example, it could be either:

- %asset_tag%
- %custom_field.asset_tag%

The additional prefix indicates more clearly that this is a Custom Field Inventory Item. If there was an Inventory Item with a matching name provided by FileWave, the first item in the list would report the provided Inventory Item value for the device and not the Custom Field.

For demonstration, imagine creating a Custom Field called 'My Device Product Name' with Internal Name: device_product_name.

Field Details

Name

My Device Product Name

Internal Name

Using internal name the field can be referenced in other parts of FileWave

device_product_name

Warning: custom field used in filesets. [\[details\]](#)

Description

Custom Field

There are now two Inventory Items with the Internal Name: device_product_name:

The hardware model of the client.
Internal name: device_product_name

and

Custom Field
Internal name: device_product_name

With the values:

Criteria	Fields	Dashboard
Drop here the fields you want to see in the query report ; change column order by moving column header.		
My Device Product Name	Device Product Name	
iPad 32GB	iPad	

Altering the above example Lock Message to use both of these:

Lock Screen Message

"If Lost, Return to..." Message

FileWave Inventory: %device_product_name%

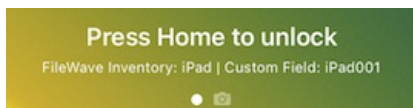
Message displayed on the login window and lock screen

Asset Tag Information

Custom Field: %custom_field.asset_tag%

Message displayed at the bottom of the login window and lock screen.

The device clearly demonstrates how the value without a prefix uses the FileWave provided Custom Field value:



To prevent confusion with overlapping Inventory Items between Custom Field and built-in Inventory, always consider using the prefix for Custom Fields

User Customisation

Although FileWave doesn't manage users, if users are associated with devices, this extends the ability to customise Profiles for users.

User details from enrolment may be used, but to extend beyond this, LDAP servers set for extraction can greatly increase the Inventory Items available for Parameters via LDAP Custom Fields.

An example of Profile customisation for users:

Email

Account Description

The display name of the account (e.g. "Company Mail Account")

My Mail Account

Account Type

The protocol for accessing the account

IMAP Path Prefix: [optional]

User Display Name

The display name of the user (e.g. "John Appleseed")

%full_name%

Email Address

The address of the account (e.g. "john@company.com")

%email%



One Profile can therefore be used for multiple devices, tailoring the Payload to the users of those devices.

