Telepod

Integration Guide

Agnosys
57 rue Bourguignette
91530 Saint-Maurice-Montcouronne
France
https://www.agnosys.com

Introduction

Telepod is an innovative automaton designed to streamline the lifecycle of iOS devices. Telepod helps IT teams meet all their device configuration and sorting needs, and can be implemented to facilitate MDM switching projects. Telepod operates through highly customizable workflows which are remotely built and monitored. If necessary, users' data transfers take place over a wired connection, without recourse to iCloud.

Telepod provides 8 workflows designed to address common use cases :

• Backup — A device is backed up, and the resulting backup is used as a template for other devices.

• Migration — A device is migrated directly from one MDM to another. The migrated device is re-enrolled using Device Enrollment and retains its Supervised status.

• Migration Back to My Device — A device is migrated from one MDM to another via a pivot device. The migrated device is re-enrolled using Automated Device Enrollment and is Supervised.

• Replacement — A current device is replaced by a new one, enrolled in the same or a different MDM. The new device is enrolled using either Automated Device Enrollment or Device Enrollment, and is Supervised.

• Replacement en masse — Current devices are replaced in batches by new ones enrolled in the same or a different MDM. The new devices are enrolled using either Automated Device Enrollment or Device Enrollment, and are Supervised.

• Setup — A device is configured, optionally using the backup of another device. It is enrolled in an MDM using either Automated Device Enrollment or Device Enrollment, and is Supervised.

• Setup en masse — Devices are configured in batches, optionally using a backup from another device. They are enrolled in an MDM using either Automated Device Enrollment or Device Enrollment, and are Supervised.

• Sorting — Devices are inspected in batches, primarily for inventory and battery diagnostics.

To facilitate the transition between two MDMs, three methods are proposed, each with its own characteristics. All three methods ensure that the device returned to the user is Supervised, but only the one involving the use of a pivot device allows the user to regain their device, enrolled in the new MDM using Automated Device Enrolment, in order to prevent the removal of the remote management profile.

Backups can be stored centrally in a distribution point so that they are available worldwide. When preparing a device, battery cycle count and health are collected, and alerts are triggered when chosen levels are reached. As part of the Replacement en masse, Setup en masse, and Sorting workflows, device details stored in Telepod's cumulative database can be exported as CSV files.

During workflows, the user may be prompted to define inventory values. In the context of MDM Switching, these values are copied from the inventory of the device in the current MDM to the inventory of the same device in the new MDM. In the context of a Replacement, the values are copied from the inventory of the current device in its MDM to the inventory of the new device in the same MDM.

Telepod is multilingual and currently localized in English and French, but translations can be built from a template to match the preferred languages of the users. Telepod is a turnkey software that requires no scripting knowledge for implementation.

References

Before reading this documentation, please consult the following references.

• Introduction

`https://www.agnosys.com/logiciels/telepod-en/`

• Management solutions support

`https://www.agnosys.com/logiciels/telepod-management-solutions-support-en/`

• Hubs support

`https://www.agnosys.com/logiciels/telepod-hubs-support-en/`

• Capabilities

`https://www.agnosys.com/logiciels/telepod-capabilities-en/`

• Offers and pricing

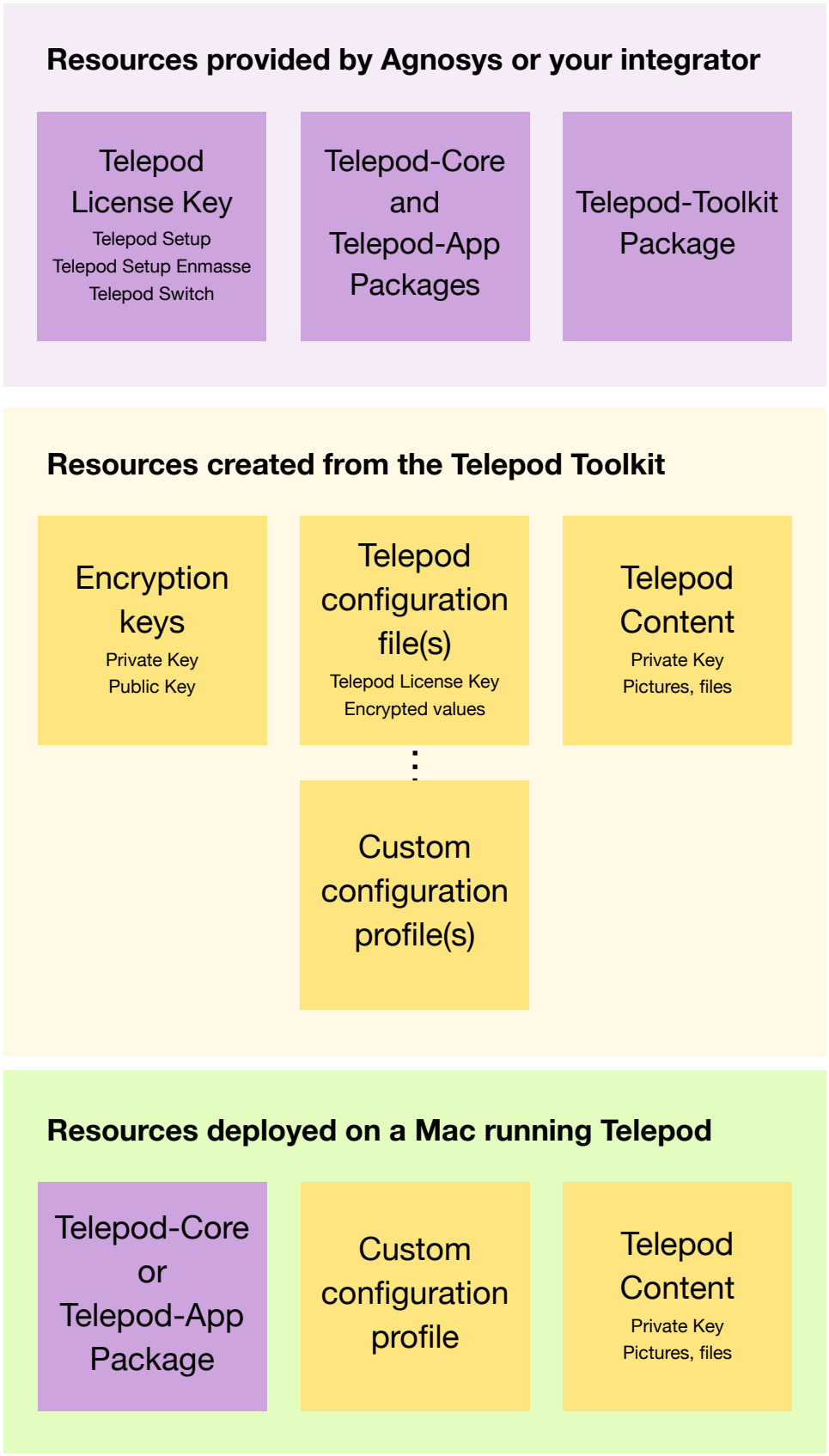
`https://www.agnosys.com/logiciels/telepod-offers-en/`

Terminology

In this guide, the word "AxM" refers both to Apple Business Manager or Apple School Manager.

Synopsis

Resources overview



The Telepod-App package contains only an app titled "Telepod.app" installed in the Applications Folder. This app embeds the Telepod-Core package. Its purpose is to execute Telepod after entering the credentials of a user with administrative privileges. The app is aimed to be used when the MDM does not offer to execute easily, reliably and without delay the installation of a package on-demand, with an execution frequency of type ongoing. Refer to the chapter "Known issues and limitations" for the list of the involved MDMs.

However, the app can be used with any supported MDM. So deploying the Telepod-App package instead of the Telepod-Core package is always an option when the users of Telepod have administrative privileges on their computer.

Implementation workflow

Step	Chapter in this document
Get a Telepod License Key	Software requirements
Download the Telepod-Core Package	
Download the Telepod-App Package	
Download the Telepod-Toolkit Package	
Install the Packages app	
Install a Property List editor	
Install the Telepod-Toolkit	Telepod Toolkit installation
Create the encryption keys	Encryption keys creation
Customize the Telepod configuration file	Telepod configuration file edition
Create other Telepod configuration files if necessary	
Convert Telepod configuration files to Custom configuration profiles	
Build (and sign) the Telepod-Content package	Telepod Content building
Provision the MDM with required configuration profiles	Configuration profiles requirements
Provision the MDM for Telepod	Provisioning *MDM*
Execute Telepod	
Enable logging and display logs	Troubleshooting

Known issues and limitations

This page is the source of truth for the known issues and limitations of Telepod.

The informations below **surpass** the informations found in the software and its documentation, including this Integration Guide, the Telepod Dictionary and the release notes.

FileWave

FileWave does not offer a way to execute Telepod on demand.

Two alternatives are offered.

If the user has administrative privileges on the computer, Telepod can be executed as an application embedded in the Telepod-App package and distributed from the MDM, alongside the Telepod-Content package and the Custom configuration profile. This guide outlines this integration.

If you run a Munki instance alongside FileWave, an alternative is to distribute the Telepod-Content and the Telepod-Core packages from this solution, while the Custom configuration profile is distributed from the MDM.

Jamf School

Jamf School Self Service does not offer a way to execute Telepod on demand.

A support request has been submitted (121823). A package can be installed or uninstalled but cannot be installed with an execution frequency of type ongoing. To help solve this issue, please vote for this Jamf Nation feature request : https://ideas.jamf.com/ideas/JN-I-26394

Two alternatives are offered.

If the user has administrative privileges on the computer, Telepod can be executed as an application embedded in the Telepod-App package and distributed from the MDM, alongside the Telepod-Content package and the Custom configuration profile. This guide outlines this integration.

If you run a Munki instance alongside Jamf School, the other alternative is to distribute the Telepod-Content and the Telepod-Core packages from this solution, while the Custom configuration profile is distributed from the MDM.

JumpCloud

JumpCloud does not offer a way to execute Telepod on demand.

Two alternatives are offered.

If the user has administrative privileges on the computer, Telepod can be executed as an application embedded in the Telepod-App package and distributed from the MDM, alongside the Telepod-Content package and the Custom configuration profile. This guide outlines this integration.

If you run a Munki instance alongside JumpCloud, an alternative is to distribute the Telepod-Content and the Telepod-Core packages from this solution, while the Custom configuration profile is distributed from the MDM.

Kandji

Kandji does not offer to upload an existing Supervision identity, nor to download the Supervision identity it manages to supervise devices enrolled using Automated Device Enrollment.

Therefore, on devices enrolled using Automated Device Enrollment, Telepod cannot override the restriction to "Pair with non-Apple Configurator hosts" set by a configuration profile. Also Telepod cannot install configuration profiles without a user interaction, cannot install wallpapers and cannot trigger locally shutdown commands.

Kandji does not offer to enroll devices using an Enrollment profile, nor an Apple Configurator Enrollment URL. Telepod can only display the URL to be used to enroll devices manually. Consequently, using Kandji with Telepod is in practice reserved for countries where an AxM can be opened.

Microsoft Intune

Microsoft Company Portal does not offer a reliable way to execute Telepod on demand.

A support request has been submitted (33233176) but the delay observed between two possible executions is considered as the expected behaviour. To help solve this issue, please vote for this feature request : https://feedbackportal.microsoft.com/feedback/idea/f6f50e22-dd62-ed11-a81b-000d3a045ff7

Two alternatives are offered.

If the user has administrative privileges on the computer, Telepod can be executed as an application embedded in the Telepod-App package and distributed from the MDM, alongside the Telepod-Content package and the Custom configuration profile. This guide outlines this integration.

If you run a Munki instance alongside Microsoft Intune, the other alternative is to distribute the Telepod-Content and the Telepod-Core packages from this solution, while the Custom configuration profile is distributed from the MDM.

Miradore

Miradore does not offer a way to execute Telepod on demand.

Two alternatives are offered.

If the user has administrative privileges on the computer, Telepod can be executed as an application embedded in the Telepod-App package and distributed from the MDM, alongside the Telepod-Content package and the Custom configuration profile. This guide outlines this integration.

If you run a Munki instance alongside Miradore, an alternative is to distribute the Telepod-Content and the Telepod-Core packages from this solution, while the Custom configuration profile is distributed from the MDM.

Mosyle Business and Mosyle Manager

Mosyle Business and Mosyle Manager do not offer to enroll devices seamlessly using an Enrollment profile. This limitation only impacts devices that are not eligible for Automated Device Enrollment.

The Enrollment profile that can be downloaded from the "Manual enroll via Safari (URL)" pane is not designed for mass enrollment and can therefore only be used by the first device to install it.

The plan is to enroll the devices using an Enrollment URL provided in the "Apple Configurator" pane. The counterpart of this method is that once the device is erased and supervised, the enrollment must be triggered manually from a dedicated pane. Until the device is enrolled, the other tasks planned by the workflow cannot be performed.

In the context of a workflow of type Replacement en masse or Setup en masse, the recommendation is to move away from the cart only after ensuring that all devices are properly enrolled.

Software requirements

macOS and Apple Configurator

Telepod requires macOS 12 and later.

Apple Configurator 2 must be deployed on the Mac prior the execution of Telepod as it embeds the `cfgutil` command line tool. No user interaction with Apple Configurator 2 is required.

Telepod packages

Download (only) the following packages from this URL :

https://www.dropbox.com/sh/c4n186xdarw4ek8/AABbqmk2YFTFGbI2qsBEF3s-a?dl=0

- Telepod-App-*version*.pkg

- Telepod-Core-*version*.pkg

- Telepod-Toolkit-*version*.pkg

Warning : Do not install Telepod-App and Telepod-Core on your computer.

The installation of Telepod-Toolkit is described in the "Telepod Toolkit installation" chapter.

Telepod requires a license key provided by Agnosys or your integrator.

Packaging editor

Download and install the "Packages" app (free) from this URL :

http://s.sudre.free.fr/Software/Packages/about.html

Property List editor

This documentation refers to the "PLIST Editor" app available on the Mac App Store :

https://apps.apple.com/app/plist-editor/id1157491961

You can use the Property List editor of your choice (e.g. Xcode).

Text Editor

For Digital signage and if the MDM solution is VMware Workspace ONE, this documentation refers to "Sublime Text" available at this address :

https://www.sublimetext.com/download_thanks?target=mac

VMware Workspace ONE Admin Assistant

If the MDM solution is VMware Workspace ONE and the Telepod-Content package cannot eventually be signed, download and install this tool :

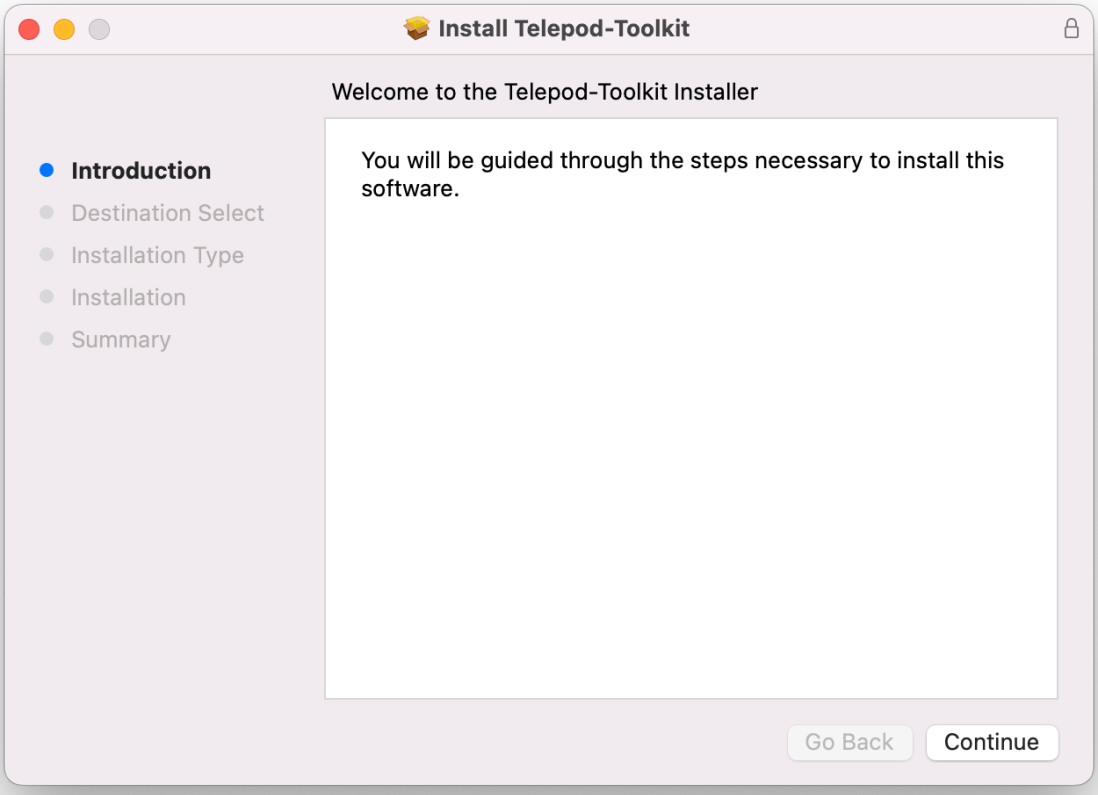
Workspace ONE Admin Assistant
https://getwsone.com/AdminAssistant/VMwareWorkspaceONEAdminAssistant.dmg

Automated Device Enrollment

If the device must be enrolled in an MDM using Automated Device Enrollment, it must be provisioned for this enrollment method in AxM and the MDM. Using Telepod does not replace nor interfere with that process.

Telepod Toolkit installation

Double-click on Telepod-Toolkit-*version*.pkg



Enter your administrator password when prompted.

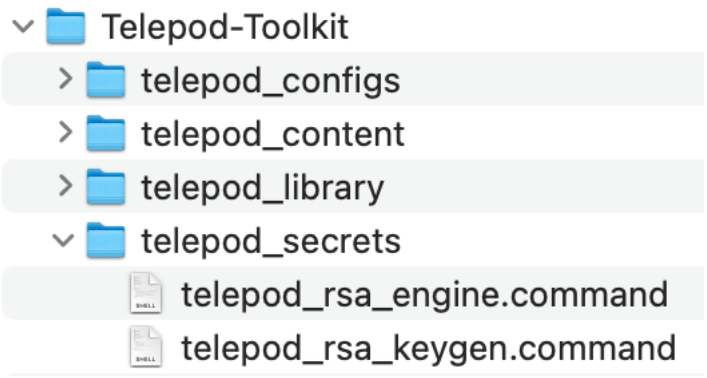
The "Telepod-Toolkit" folder is created in /Users/Shared. It contains the following subfolders :
- telepod_configs
- telepod_content
- telepod_library
- telepod_secrets

Move the "Telepod-Toolkit" folder in a location in your home folder that only you can access.

Do not modify the content of the "Telepod-Toolkit" folder unless instructed to do so for specific items.

Encryption keys creation

Sensitive informations in a Telepod Property List are protected from direct observation using a RSA encryption method :
- a private / public key pair is created with the "telepod_rsa_keygen" script
- the private key is automatically embedded in the Telepod-Content package
- the public key is used when encrypting a string with the "telepod_rsa_engine" script.

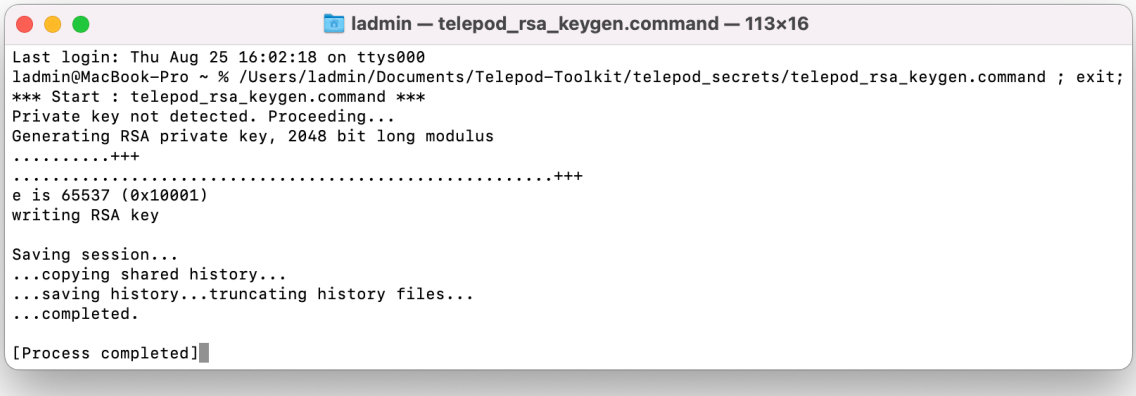


Open the "Telepod-Toolkit" folder.

Open the "telepod_secrets" subfolder.

Execute the "telepod_rsa_keygen" script (double-click on the .command file).

The script is aimed to be executed only once because the private / public key pair must be static for the whole Telepod integration lifetime.



The private / public key pair is created at the following path :
Telepod-Toolkit > telepod_secrets > telepod_rsa_key.pri and telepod_rsa_key.pub

If you delete the private key at this path, execute the script again. It will generate another private / public key pair with the consequence that you will have to :
- re-encrypt all the sensitive strings
- generate a new Telepod-Content package.

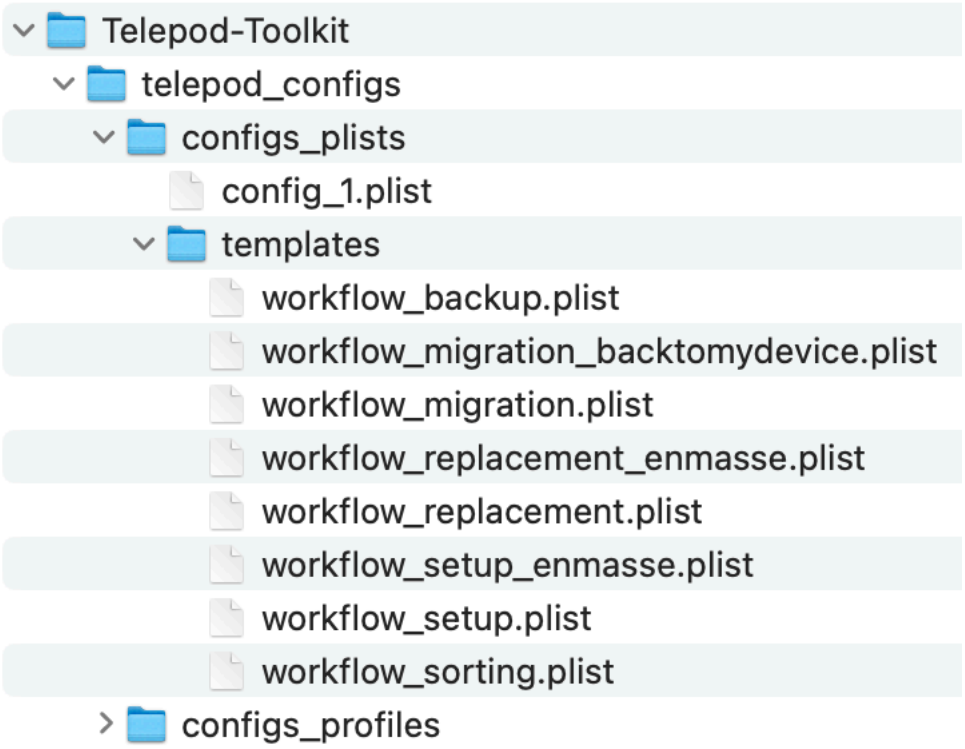
The private key is automatically copied at the following path :
Telepod-Toolkit > telepod_content > Content > telepod_rsa_key.pri

If you delete the private key at this path, execute the script again. It will copy again the existing private key.

Telepod configuration file edition

The Telepod configuration file contains a set of mandatory and optional keys that dictates the functioning of Telepod.

Access to the configuration file templates



Open the "Telepod-Toolkit" folder.

Open the "telepod_configs" subfolder.

Open the "configs_plists" subfolder.

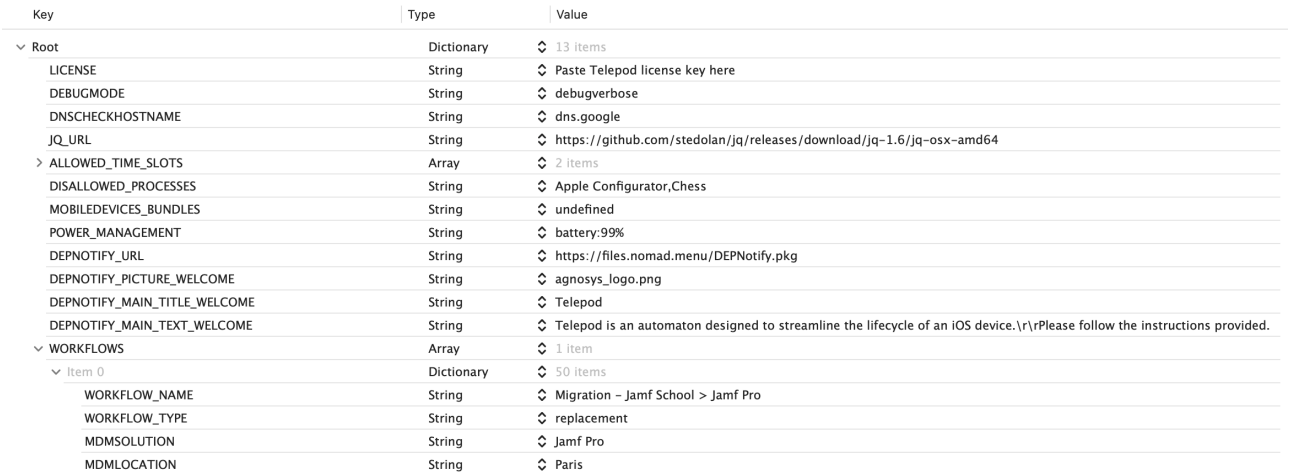
The "config_1.plist" property list is the main configuration file. It contains the keys that are common to all the workflows it embeds, and which constitute the "main settings".

Open the "templates" subfolder.

Each template contains the keys expected for a Backup, Migration, Migration Back to my device, Replacement, Replacement en masse, Setup, Setup en masse, or Sorting workflow.

To define which workflow you should implement for an MDM Switching, please consult in the chapter titled "Workflows configuration" the subchapter titled "Choosing the best workflow for an MDM Switching".

To build a functional configuration file :
- open your favorite Property List editor
- open one of the template
- open the WORKFLOWS array
- select the Dictionary **only** and copy it
- open the "config_1.plist" file
- open the WORKFLOWS array
- paste the Dictionary **inside** the WORKFLOWS array.



Key	Type	Value
Root	Dictionary	13 items
LICENSE	String	Paste Telepod license key here
DEBUGMODE	String	debugverbose
DNSCHECKHOSTNAME	String	dns.google
JQ_URL	String	https://github.com/stedolan/jq/releases/download/jq-1.6/jq-osx-amd64
ALLOWED_TIME_SLOTS	Array	2 items
DISALLOWED_PROCESSES	String	Apple Configurator,Chess
MOBILEDEVICES_BUNDLES	String	undefined
POWER_MANAGEMENT	String	battery:99%
DEPNOTIFY_URL	String	https://files.nomad.menu/DEPNotify.pkg
DEPNOTIFY_PICTURE_WELCOME	String	agnosys_logo.png
DEPNOTIFY_MAIN_TITLE_WELCOME	String	Telepod
DEPNOTIFY_MAIN_TEXT_WELCOME	String	Telepod is an automaton designed to streamline the lifecycle of an iOS device.\r\rPlease follow the instructions provided.
WORKFLOWS	Array	1 item
Item 0	Dictionary	50 items
WORKFLOW_NAME	String	Migration - Jamf School > Jamf Pro
WORKFLOW_TYPE	String	replacement
MDMSOLUTION	String	Jamf Pro
MDMLOCATION	String	Paris

Check the structure of the "config_1.plist" file that must match the above screenshot.

Multiple templates can be copied into the main configuration file to provide multiple workflows.

When multiple workflows are offered, the order of the Dictionaries in the WORKFLOWS array determines the order of the workflows in the workflow selector.

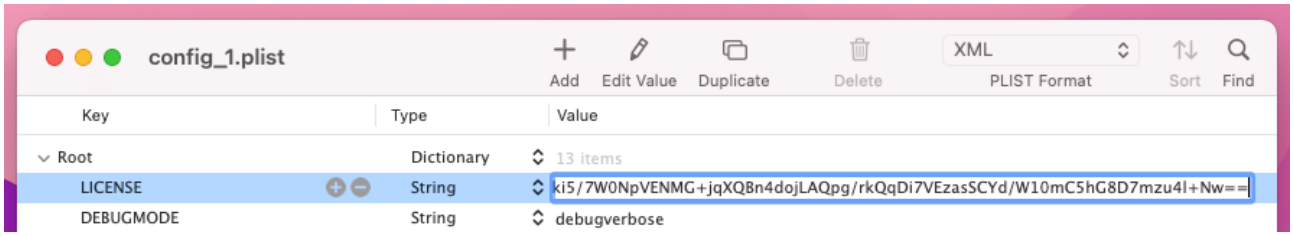
Reference for keys

Please consult the Telepod Dictionary, whose filename is "3. Telepod_Dictionary.pdf", to learn how to edit a configuration file.

All keys are important so it is recommended to take the time to read the document completely.

Some keys require extra informations that are detailed in this section.

License key



Paste the Telepod license key in the LICENSE key.

The license key is a one-line string ending exactly with two "=" characters.

This table shows the workflows authorized by each Telepod license.

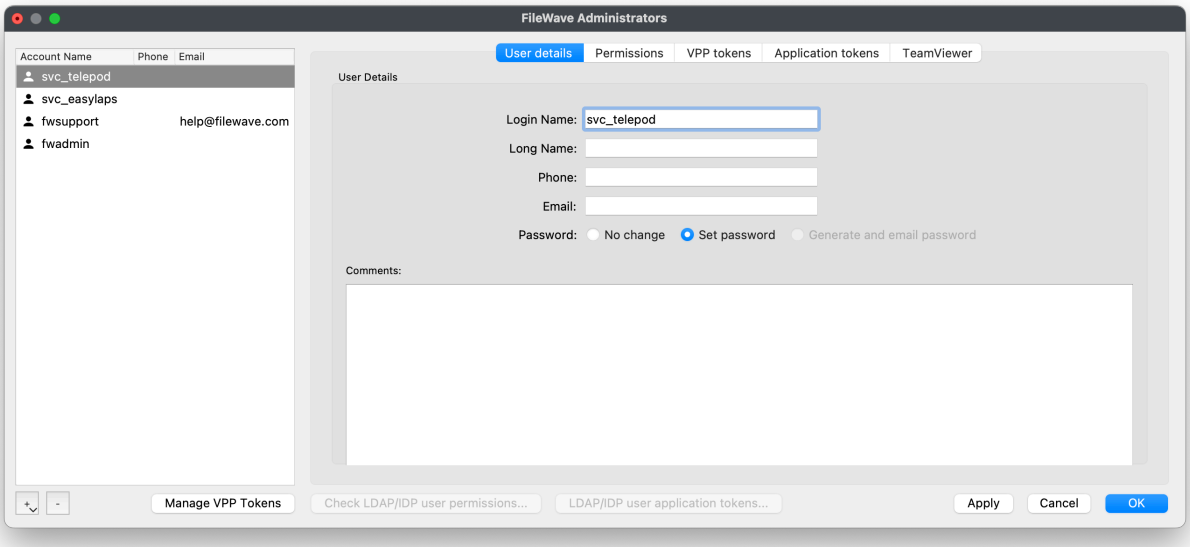
Workflow	Setup	Setup en masse	Switch	Switch en masse	Sorting
Backup	✓	✓	✓	✓	✗
Migration	✗	✗	✓	✓	✗
Migration Back to my device	✗	✗	✓	✓	✗
Replacement	✗	✗	✓	✓	✗
Replacement en masse	✗	✗	✗	✓	✗
Setup	✓	✓	✓	✓	✗
Setup en masse	✗	✓	✗	✓	✗
Sorting	✓	✓	✓	✓	✓

FileWave : APIAUTHENTICATIONSTRING key

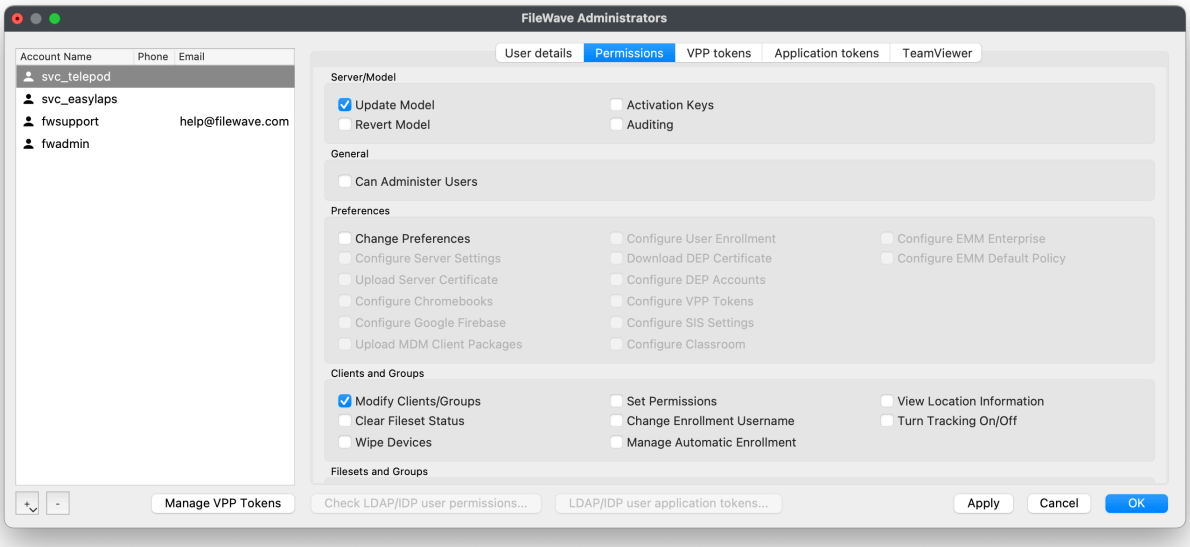
This section only applies if the management solution is FileWave.

First create a new administrator that will be used by Telepod to make API calls.

FileWave Admin > Assistants > Manage Administrators > + Local Account



Select "User details" then fill in the "Login Name" field and set a password.



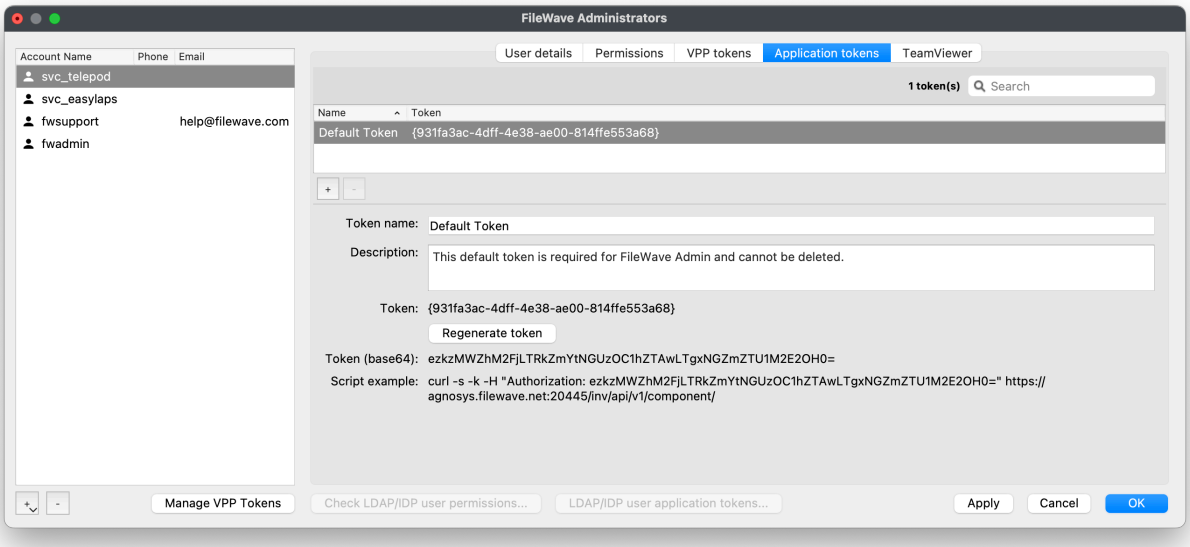
Select "Permissions".

The administrator requires the following permission : "Modify Clients/Groups".

If you want to authorize Telepod to make an API call to remotely unenroll a device, the administrator must have this supplemental permission : "Update Model".

All Custom Fields specified in the configuration file for both the contexts of an onboarding or a migration should be created manually before Telepod is deployed. However, Telepod can create these Custom Fields when detected as missing if the account has this supplemental permission :

- Modify Custom Fields



Select "Application tokens".

Copy the value of "Token (base64)" (exactly) then follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the Token
- the Token is encrypted, displayed and then decrypted for sanity check
- copy the encrypted Token (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Hexnode UEM : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Hexnode UEM.

Go to Admin > API > Configure API. Click on "Enable".

Click on the padlock to reveal the API Key.

Copy the API Key displayed (exactly) then follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the API Key
- the API Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Jamf Pro - API Roles and Clients : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Jamf Pro and the authentication mechanism is based on the use of API Roles and Clients available since Jamf Pro 10.49 (recommended).

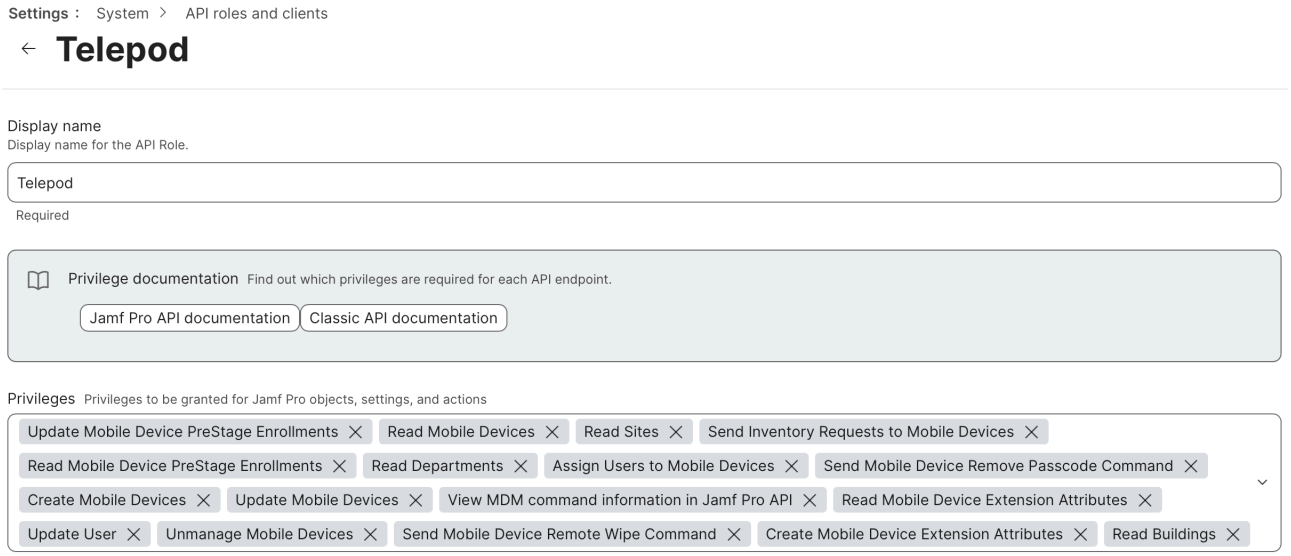
The key will be used by Telepod to make API calls.

Create a new text document with 2 lines :
- Client ID :
- Client Secret :

Open Settings then click on "API Roles and Clients".

First create a new role with limited API privileges.

Click on the "API Roles" tab then on the "+ New" button.



Enter a name like "Telepod".

Click in the "Jamf Pro API role privileges" field and select the following privileges :

- Read Mobile Device Extension Attributes
  (**not required** if Jamf Pro API is enabled)

- Read Mobile Devices

- Create Mobile Devices

- Update Mobile Devices

- Update User

- Assign Users to Mobile Devices

- Send Inventory Requests to Mobile Devices

Warning : Omitting the Update User privilege prevents the update of the device inventory.

If you want to authorize Telepod to make an API call to remotely unlock a device, the Role must have this supplemental privilege :

- Send Mobile Device Remove Passcode Command

If you want to authorize Telepod to make an API call to remotely wipe a device, the Role must have this supplemental privilege :

- Send Mobile Device Remote Wipe Command

If you want to authorize Telepod to make an API call to remotely unenroll a device, the Role must have this supplemental privilege :

- Unmanage Mobile Devices

If you want to authorize Telepod to automatically assign a device to a specific Automated Device Enrollment profile, the Role must have these supplemental privileges :

- Read Mobile Device PreStage Enrollments

- Update Mobile Device PreStage Enrollments

If you want to authorize Telepod to refresh a device using Return to Service, the Role must have this supplemental privilege :

- View MDM command information in Jamf Pro API

All computer attributes specified in the configuration file should be created manually before Telepod is deployed. However, Telepod can create these attributes when detected as missing if the Role has this supplemental privilege :

- Create Mobile Device Extension Attributes

If you want to authorize Telepod to retrieve the buildings, the departments and the sites to dynamically populate the menus planned in the SETTINGS_PANE > LIST array, the Role must have these supplemental privileges :

- Read Buildings

- Read Departments

- Read Sites

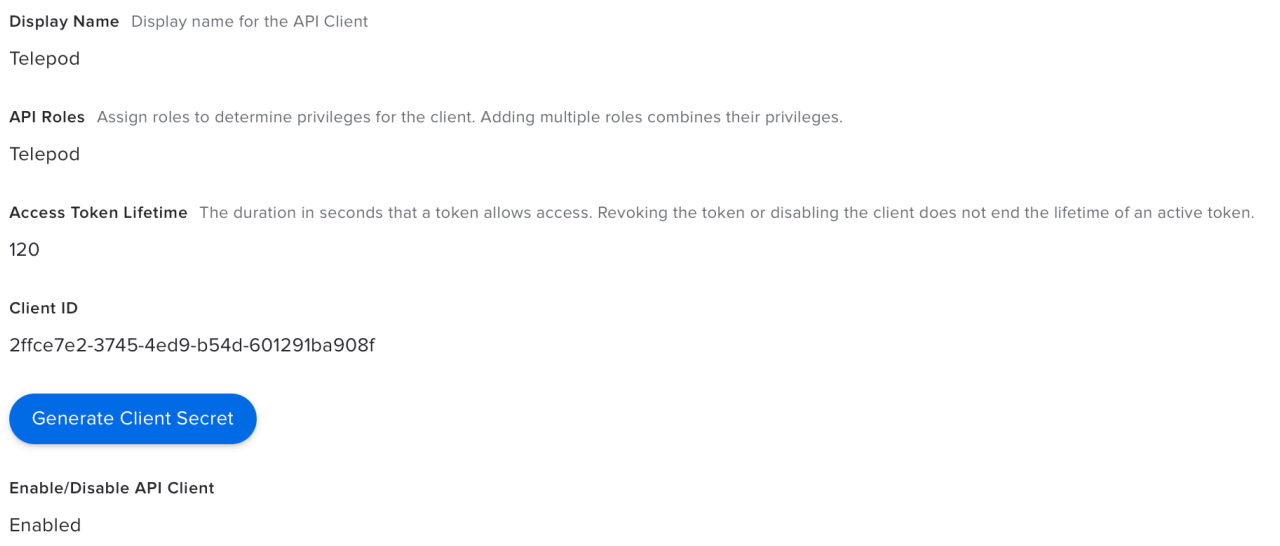
Click on "Save".

Go back to "API Roles and Clients" to create a new API Client associated to the Telepod API Role.

Click on the "API Clients" tab then on the "+ New" button.

Enter a name like "Telepod", select the Telepod API Role and enter "120" (2 minutes) in the "Access Token Lifetime" field.

Click on "Enable API Client" then on "Save".



Click on "Generate Client Secret" then on "Create Secret".

Copy both the Client ID and the Client Secret in the text document then click on "Close".

Concatenate in one string the Client ID and the Client Secret, separated by the character : (colon), then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string

- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Jamf Pro - User account : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Jamf Pro and the authentication mechanism is based on the use of a Jamf Pro User account (not recommended).

First create a new Jamf Pro User Account that will be used by Telepod to make API calls.

This account requires the following set of privileges :

- Jamf Pro Server Objects
    - Mobile Device Extension Attributes : Read
      (**not required** if Jamf Pro API is enabled)
    - Mobile Devices : Create - Read - Update
    - Users : Update
- Jamf Pro Server Actions
    - Assign Users to Mobile Devices
    - Send Inventory Requests to Mobile Devices

Warning : Omitting the Users - Update privilege prevents the update of the device inventory.

If you want to authorize Telepod to make an API call to remotely unlock a device, the account must have this supplemental privilege :

- Jamf Pro Server Actions
    - Send Mobile Device Remove Passcode Command

If you want to authorize Telepod to make an API call to remotely wipe a device, the account must have this supplemental privilege :

- Jamf Pro Server Actions
    - Send Mobile Device Remote Wipe Command

If you want to authorize Telepod to make an API call to remotely unenroll a device, the account must have these supplemental privileges :

- Jamf Pro Server Actions
    - Unmanage Mobile Devices

If you want to authorize Telepod to automatically assign a device to a specific Automated Device Enrollment profile, the account must have these supplemental privileges :

- Jamf Pro Server Objects

    - Mobile Device PreStage Enrollments : Read - Update

If you want to authorize Telepod to refresh a device using Return to Service, the account must have this supplemental privilege :

- Jamf Pro Server Actions

    - View MDM command information in Jamf Pro API

All computer attributes specified in the configuration file should be created manually before Telepod is deployed. However, Telepod can create these attributes when detected as missing if the account has this supplemental privilege :

- Jamf Pro Server Objects

    - Mobile Device Extension Attributes : Create

If you want to authorize Telepod to retrieve the buildings, the departments and the sites to dynamically populate the menus planned in the SETTINGS_PANE > LIST array, the account must have these supplemental privileges :

- Jamf Pro Server Objects

    - Buildings : Read

    - Departments : Read

    - Sites : Read

Concatenate in one string the username and the password of this account, separated by the character : (colon), then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Jamf School : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Jamf School.

First create a new API Key that will be used by Telepod to make API calls.

Go to School > Settings > API. Click on "Add API Key" and enter "Telepod" in the "Name" field. Select the two access rights "Read" and "Add". Unselect the two access rights "Edit" and "Delete". Click on "Apply".

Go to School > Devices > Enroll Device(s) > On-device enrollment and note the Network ID.

Concatenate in one string the Network ID and the API Key, separated by the character : (colon), then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

JumpCloud : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is JumpCloud.

First create a new JumpCloud Administrator account whose API Key will be used by Telepod to make API calls.

Go to Settings > Administrators.

Create a new account with the "manager" role and tick the option "Enable API access".

Connect to JumpCloud console with this new administrator account.

Click on your account icon in the upper right corner, then select "My API Key".

Expiration Date : No Expiration

Click on "Generate New API Key"

Click the copy button to retrieve the API Key then follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the API Key
- the API Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Meraki Systems Manager : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Meraki Systems Manager.

First create a new API Key that will be used by Telepod to make API calls.

Go to Organization > Configure > Settings > Dashboard API access. Select "Enable access to the Cisco Meraki Dashboard API" and click on "Save Changes".

Click on your account (email address) displayed in the upper right corner and select "My profile". In the API access section, click on "Generate new API key". Copy the API Key that is displayed **only once**, select "I have stored my new API key" and click on "Done".

Follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the API Key
- the API Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

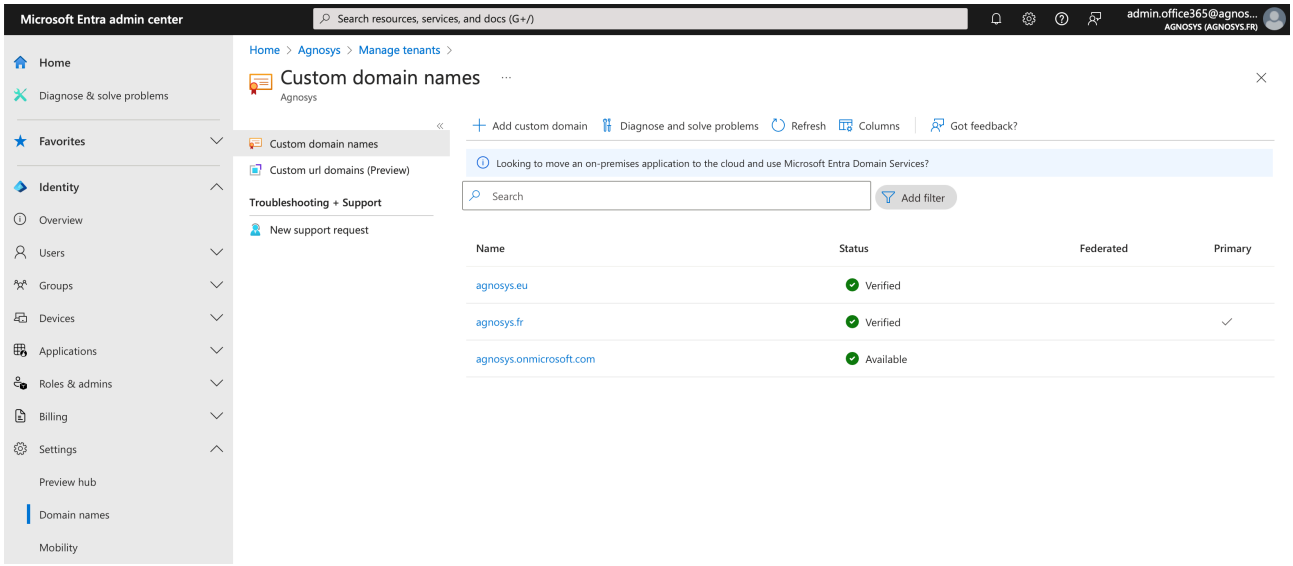
Microsoft Intune : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Microsoft Intune.

The key will be used by Telepod to make API calls.

Create a new text document with 3 lines :
- Tenant domain :
- Application (client) ID :
- Client secret value :

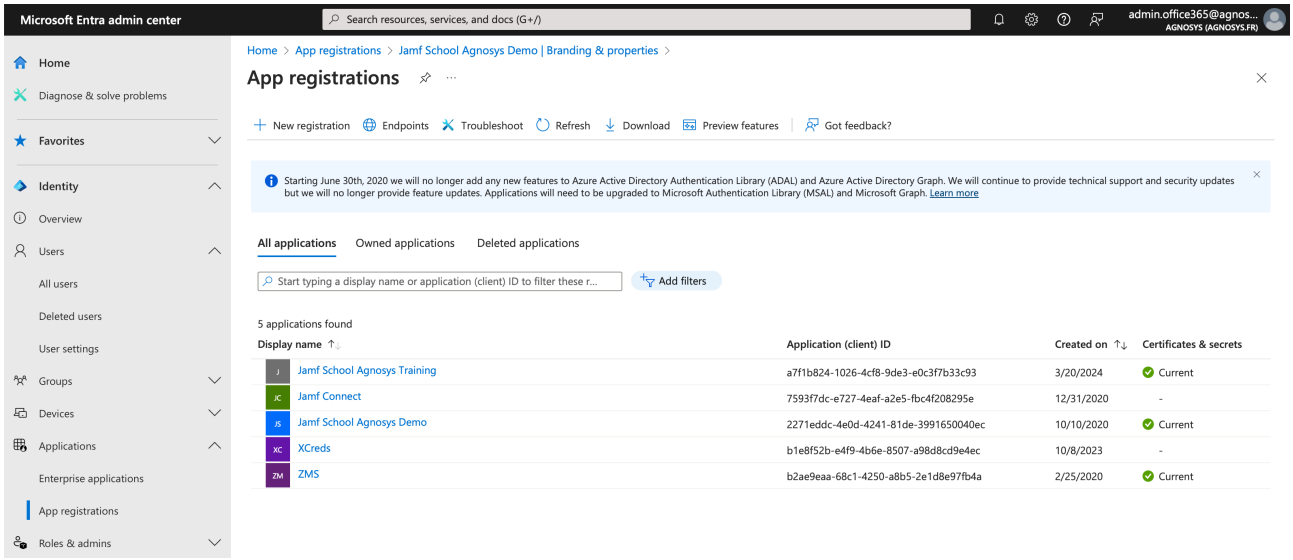
Connect to Microsoft Entra admin center.



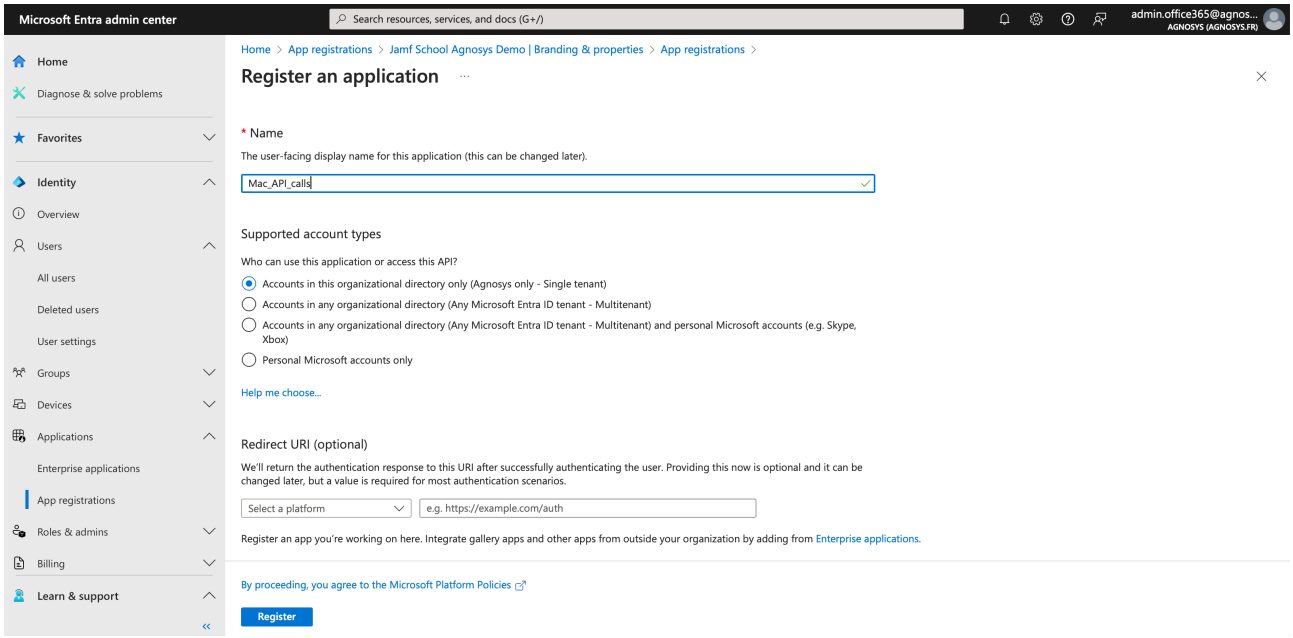
Go to Identity > Settings > Domain names.

Copy / paste the name including the extension ".onmicrosoft.com" in the text document for the value "Tenant domain".

Go to Identity > Applications > App registrations.



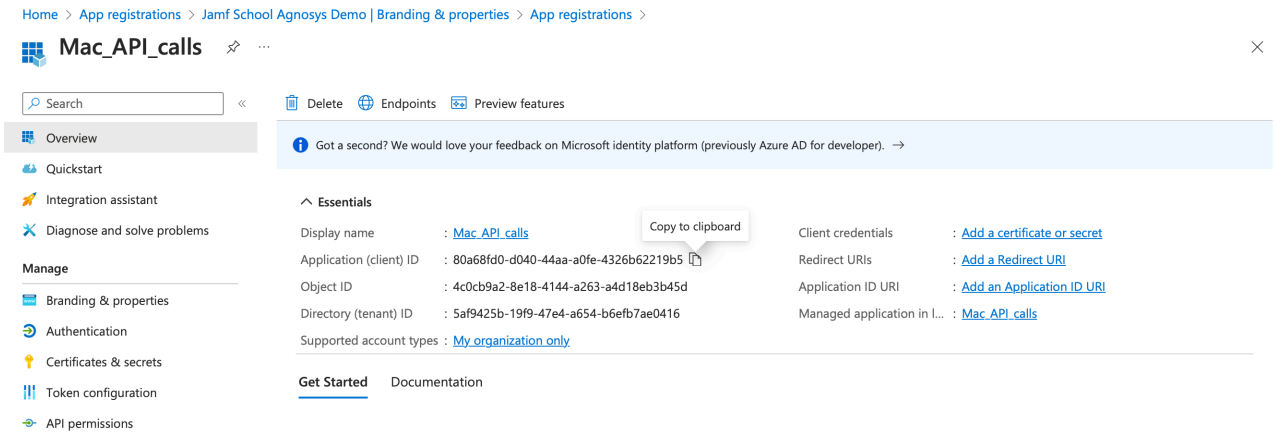
Click on "All applications", then on "New registration".



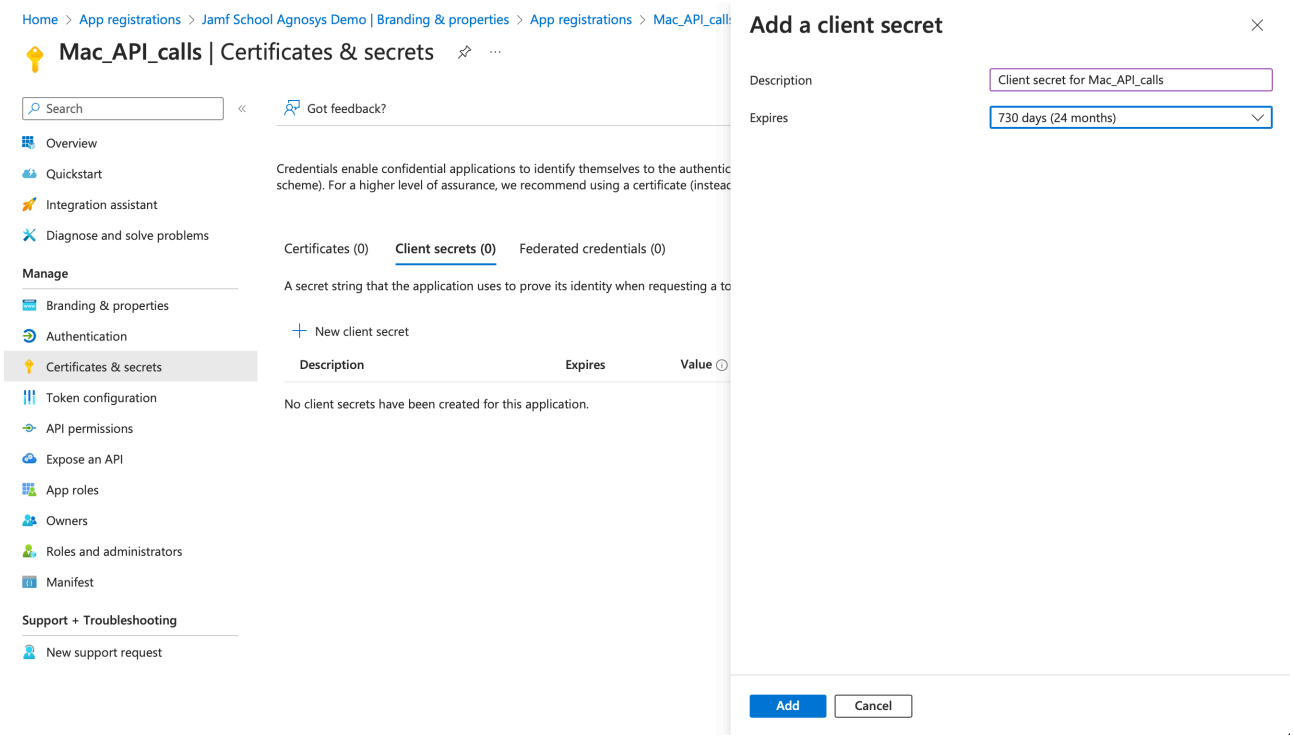
Enter a name for the application.

Select "Accounts in this organizational directory only (*Company* only - Single tenant)".

Click on "Register".



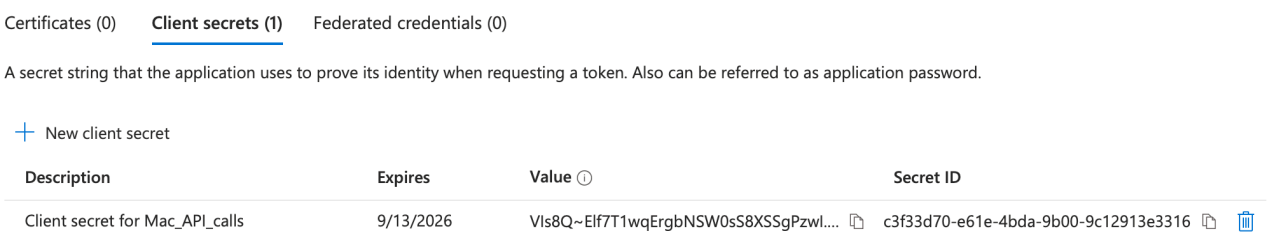
Copy / paste the Application (client) ID in the text document.



Click on "Certificates & secrets" then click on "New client secret".

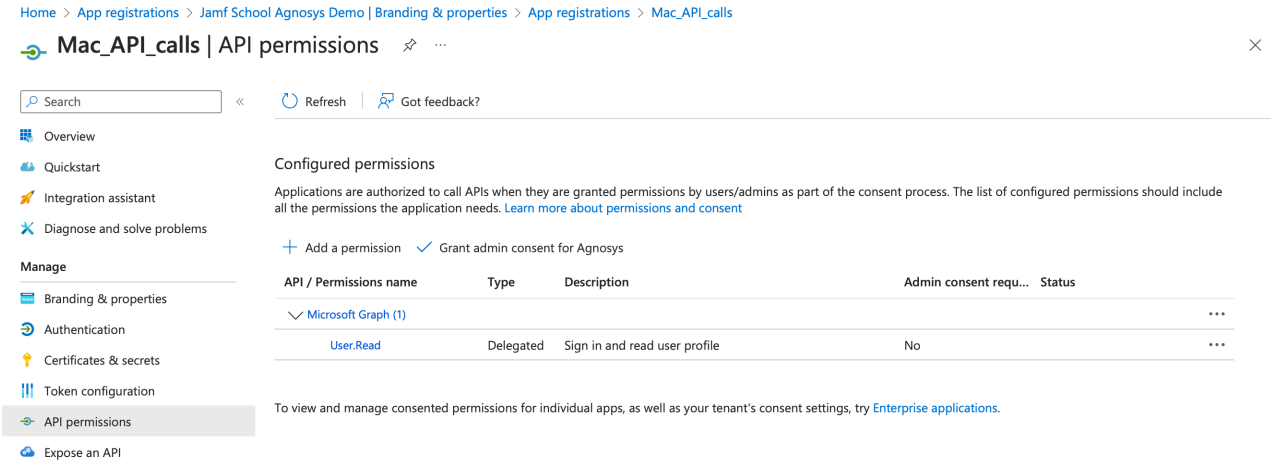
Enter a description and select a life time.

Click on "Add".

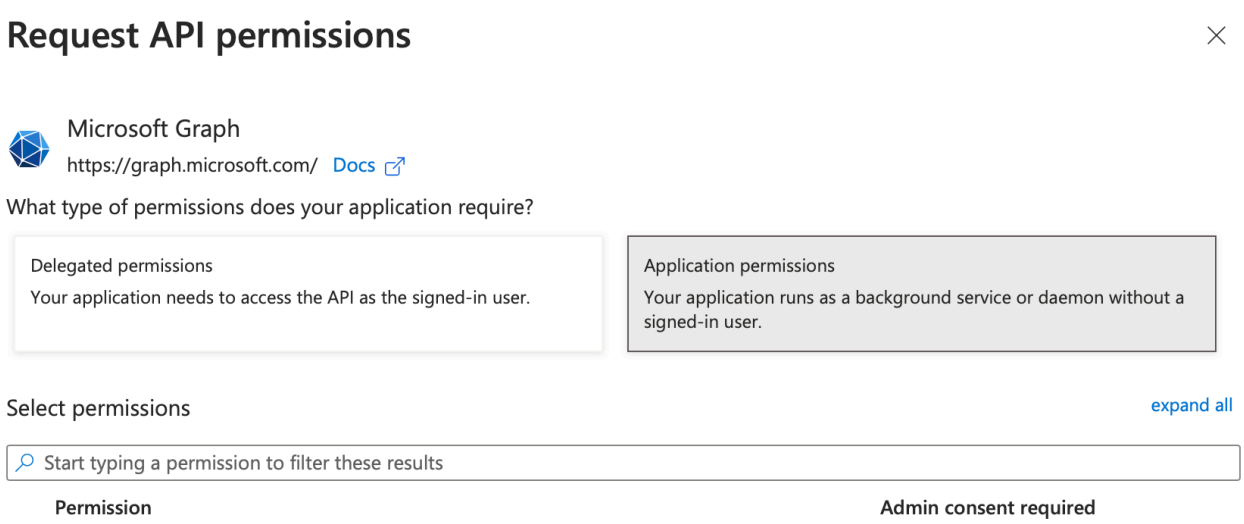


You will see this information **only once**.

Click on the "Copy" button right to the "**Value**" field and paste the value in the text document.



Click on "API permissions", then click on "Microsoft Graph (1)".

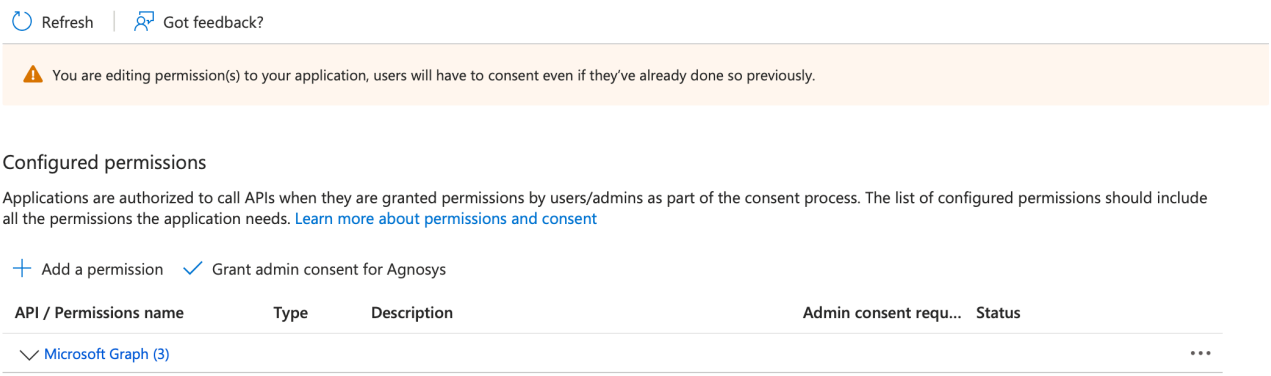


Click on "**Application permissions**".

Select the API permission "DeviceManagementManagedDevices.**ReadWrite**.All".

If you want to authorize Telepod to make an API call to remotely wipe a device or to remotely unenroll a device, the API permission "DeviceManagementManagedDevices.**PrivilegedOperations**.All" must be selected.

Click on "Update permissions".



Click on "Grant admin consent for *Company*". In the message "Grant admin consent confirmation", click on "Yes".

Check that the "Type" of every permission added is "Application" and that its status is "Granted for *Company*".

```
Tenant domain : agnosys.onmicrosoft.com
Application (client) ID : 235c8367-328a-4bf3-bd4c-1a52ba086fd3
Client secret value : -9b88W5BQhnZB3TGJ.K~X08_lDX_noTOoB

agnosys.onmicrosoft.com,235c8367-328a-4bf3-bd4c-1a52ba086fd3,-9b88W5BQhnZB3TGJ.K~X08_lDX_noTOoB
```

Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted password in the APIAUTHENTICATIONSTRING key.

Miradore : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Miradore.

First create a new API key that will be used by Telepod to make API calls.

Go to System > Infrastructure diagram > Site > API > Create key.

Step 1 of 3: Enter a descriptive name for the API key :
Name : Telepod
Click on "Next".

Step 2 of 3: Confirm to create
Copy the displayed API key then click on "Create key".

Follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the API key
- the API key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Mosyle Business : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Mosyle Business.

The key will be used by Telepod to make API calls.

Create a new text document with 3 lines :
- Service account email :
- Service account password :
- Access Token :

First create a new administrator account.

Go to Organization > Users and Groups > Administrators. Click "Add Administrator". Enter a Name, a User ID, an Email and set a Password. Select the Account type "Administrator". Deselect "Send welcome e-mail with the first steps". Click on "View Advanced Options" and check "Limit user permissions". Click on "Select".

Click on "New Role". Define the new role :
- Name : Telepod Role
- Organization > Integrations :
    - API Integration : View - Create

All other privileges should be disabled.

Click on "Save". Back to the "Role Selector", click on "Telepod Role". Check that the new administrator account is limited to the "Telepod Role". Click on "Save".

Add the Service account email and the Service account password to the text document.

Go to Organization > Integrations > Mosyle API Integration. Click on "Add new token" and enter "Telepod Token" in the "Profile name" field. Select "Public" for the "Access Method". Unselect "Allow all current and future endpoints" then select only "Devices". Click on "Save".

In the API Information pane, copy the "Access Token" displayed (exactly).

Paste the Access Token in the text document.

Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Mosyle Manager : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Mosyle Manager.

The key will be used by Telepold to make API calls.

Create a new text document with 3 lines :
- Service account email :
- Service account password :
- Access Token :

First create a new leader account.

Go to My School > Users > Administrators. Click "Add new administrator". Enter a Name, a User ID, an Email and select the Account type "Leader". Deselect "Send welcome e-mail with the first steps". Click on "Save". Click on "Edit". Set a Password. Click on "View Advanced Options" and check "Limit user permissions". Click on "Select".

Click on "New Role". Define the new role :
- Name : Telepod Role
- My School > Integrations :
    - API Integration : View - Update

All other privileges should be disabled.

Click on "Save". Back to the "Role Selector", click on "Telepod Role". Check that the new administrator account is limited to the "Telepod Role". Click on "Save".

Add the Service account email and the Service account password to the text document.

Go to My School > Integrations > Mosyle API Integration. Enable "API Integration". Click on Access Method > Edit, select "Public" and click "Save".

Copy the "Access Token" displayed (exactly) and paste it in the text document.

Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

SimpleMDM : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is SimpleMDM.

First create a new API Key that will be used by Telepod to make API calls.

Go to Account > API. Click on "Add API Key" and enter "Telepod" in the "Name" field.

Select the following permissions :

- Custom Attributes : Write

- Devices : Write

All other permissions should be set to "None".

Click on "Save".

Click on Secret Access Key > Reveal.

Copy the "Secret Access Key" displayed (exactly) then follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the Secret Access Key
- the Secret Access Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted Secret Access Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

VMware Workspace ONE - OAuth authentication : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is VMware Workspace ONE and the authentication mechanism is OAuth2 (recommended).

The key will be used by Telepod to make API calls.

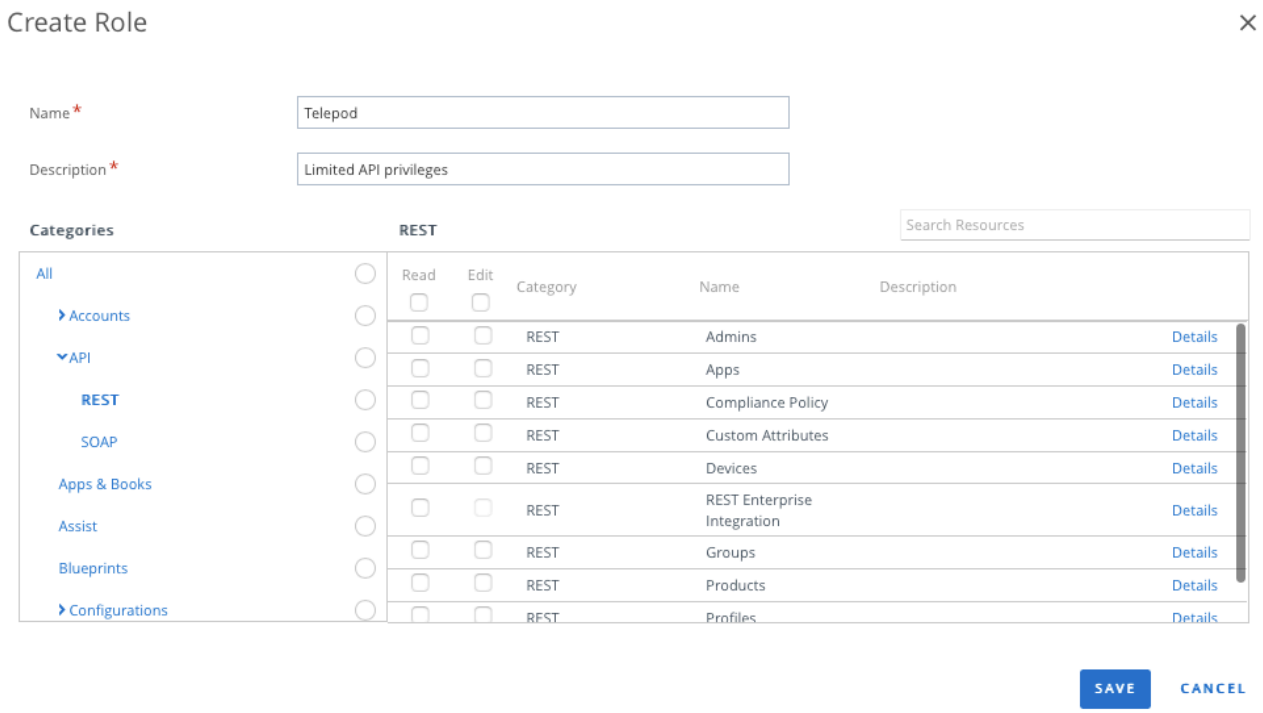
Create a new text document with 4 lines :
- Token URL :
- Client ID :
- Client Secret :

To define the Token URL, please consult this article : https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_ConsoleBasics/GUID-UsingUEMFunctionalityWithRESTAPI.html

Create a new role with limited API privileges.

Go to Accounts > Administrators > Roles.

Click on "Add Role".



Enter a specific name like "Telepod" and a description, then in the "Categories" sidebar, select All > API > REST.

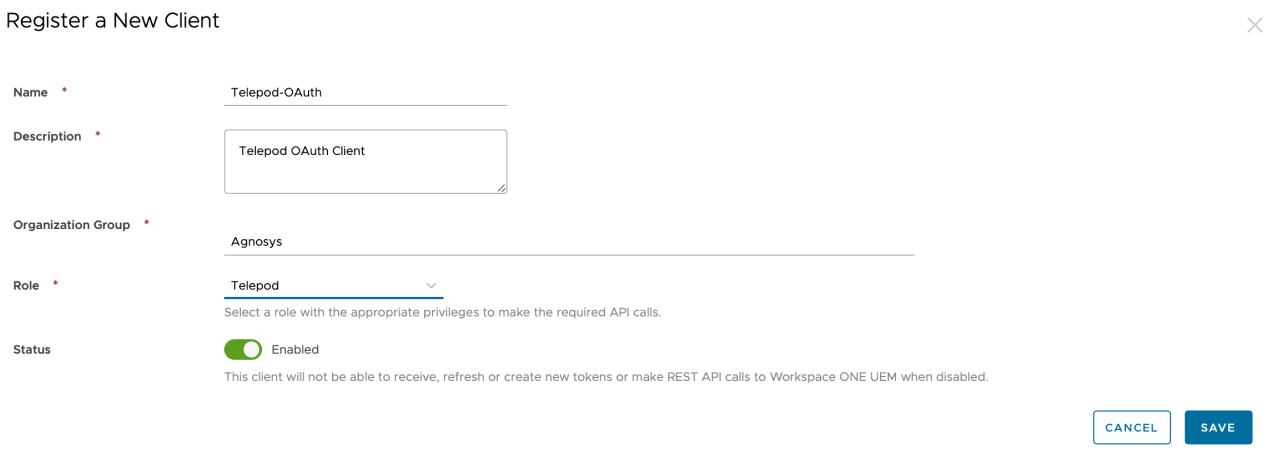
The role requires the following set of privileges :

- Custom Attributes > Details
    - Edit — Rest API Custom Attributes Write
    - Read — Rest API Custom Attributes Read
- Devices > Details
    - Edit — REST API Devices Execute
    - Edit — REST API Devices Delete
    - Read — REST API Devices Read

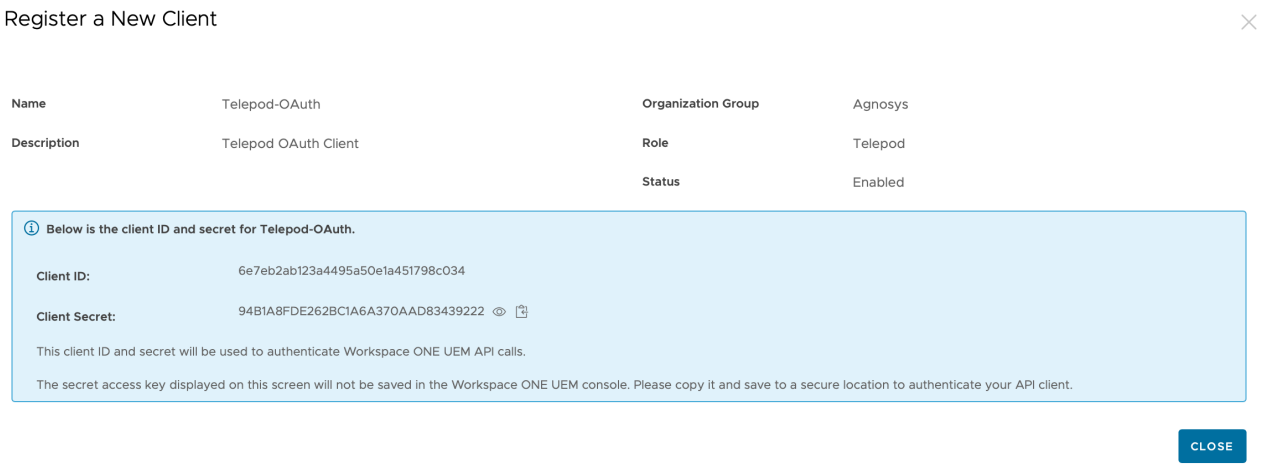
Click on "Save".

Go to Groups & Settings > Configurations > OAuth Client Management.

Click on "Add".



Enter a name and a description. Select the Organization Group that encompasses the devices that are to be installed with Telepod then select the "Telepod" role. Click on "Save".



Copy both the Client ID and the Client Secret in the text document then click on "Close".

```
Token URL     : https://uat.uemauth.vmwservices.com/connect/token
Client ID     : 3c46dbb9377c4491896989ea2fdae1f0
Client Secret : 9A78D983F619CB7873A90908F6AA1409

https://uat.uemauth.vmwservices.com/connect/token,3c46dbb9377c4491896989ea2fdae1f0,9A78D983F619CB7873A90908F6AA1409
```

Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

VMware Workspace ONE - Basic authentication : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is VMware Workspace ONE and the authentication mechanism is Basic (not recommended).

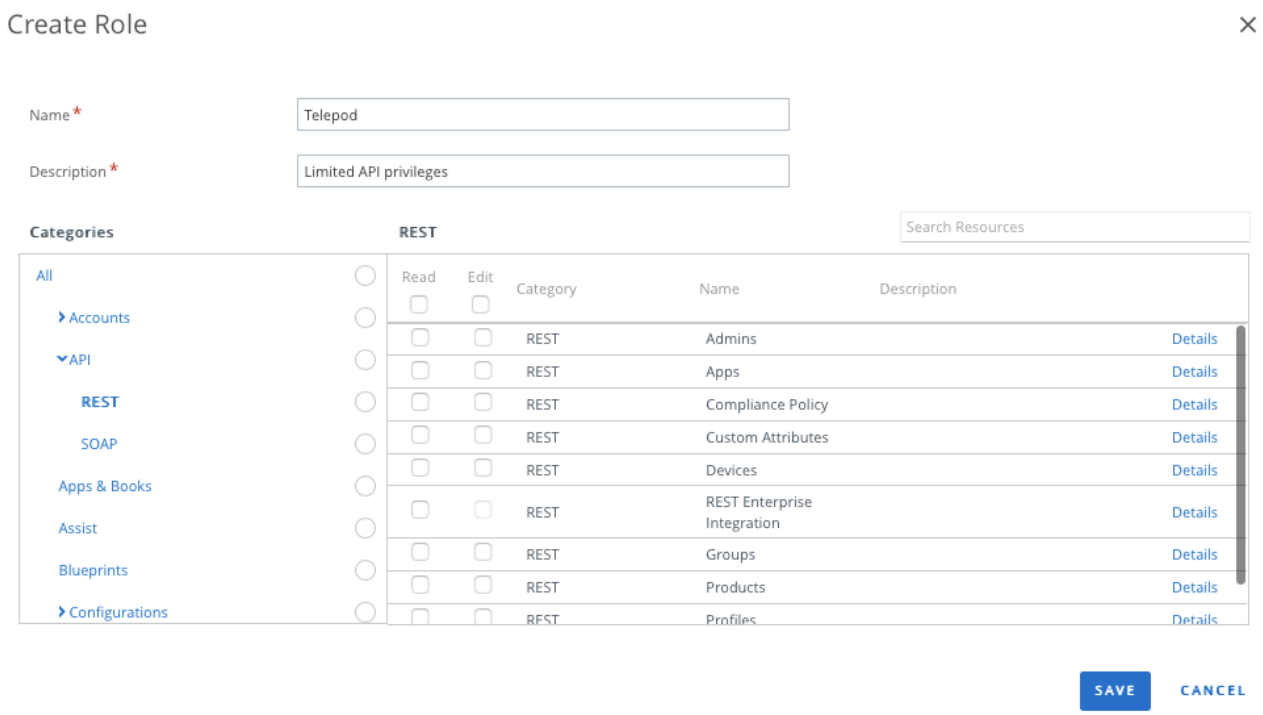
The key will be used by Telepod to make API calls.

Create a new text document with 3 lines :
- Username :
- Password :
- API Key :

First create a new role with limited API privileges.

Go to Accounts > Administrators > Roles.

Click on "Add Role".



Enter a specific name like "Telepod" and a description, then in the "Categories" sidebar, select All > API > REST.

The role requires the following set of privileges :

- Custom Attributes > Details
    - Edit — Rest API Custom Attributes Write
    - Read — Rest API Custom Attributes Read
- Devices > Details
    - Edit — REST API Devices Execute
    - Edit — REST API Devices Delete
    - Read — REST API Devices Read

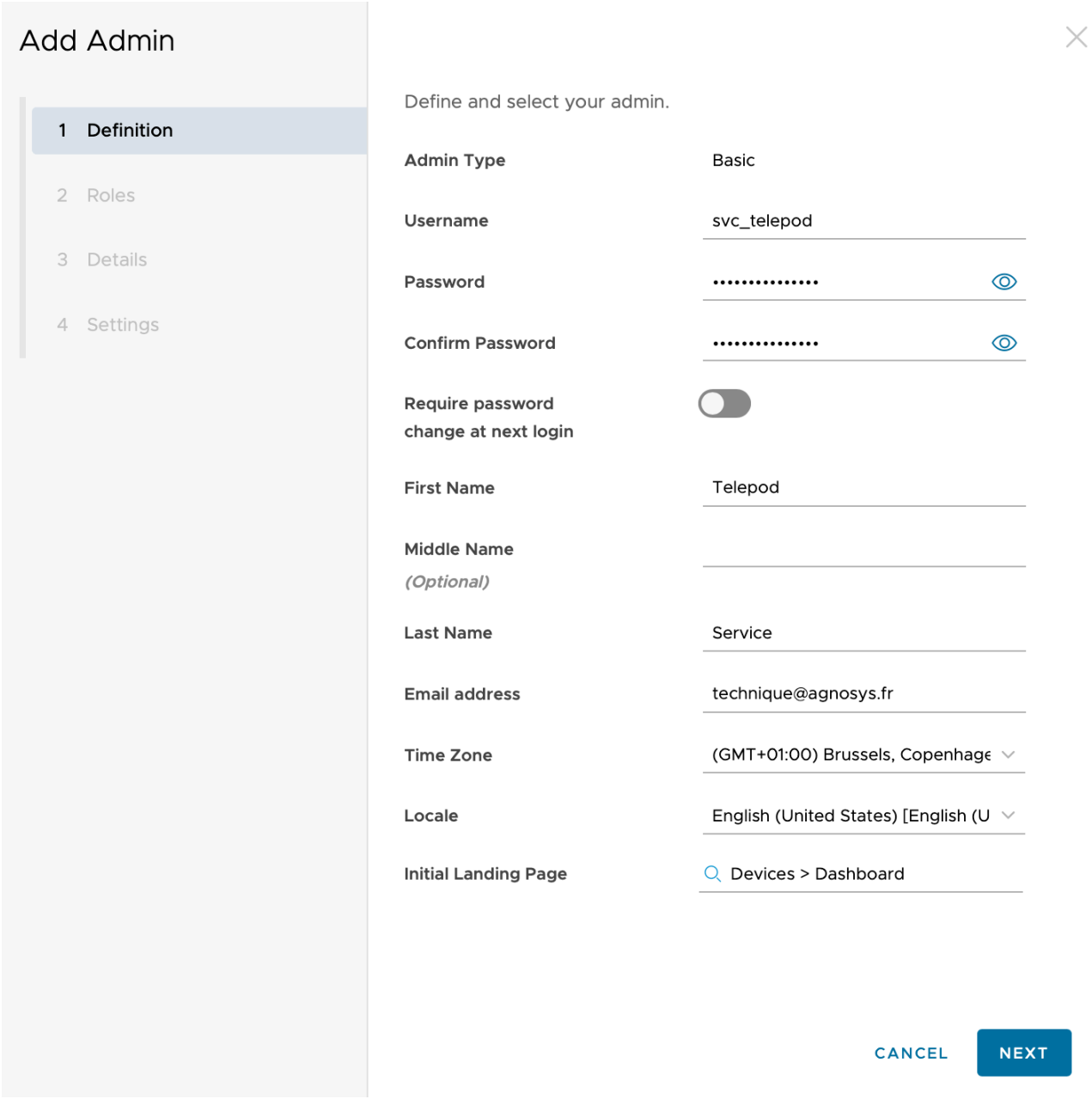
Click on "Save".

Then create a new Workspace ONE Administrator account that will be used by Telepod to make API calls.

Go to Accounts > Administrators > List View.

Click on "Add" > "Add Admin".

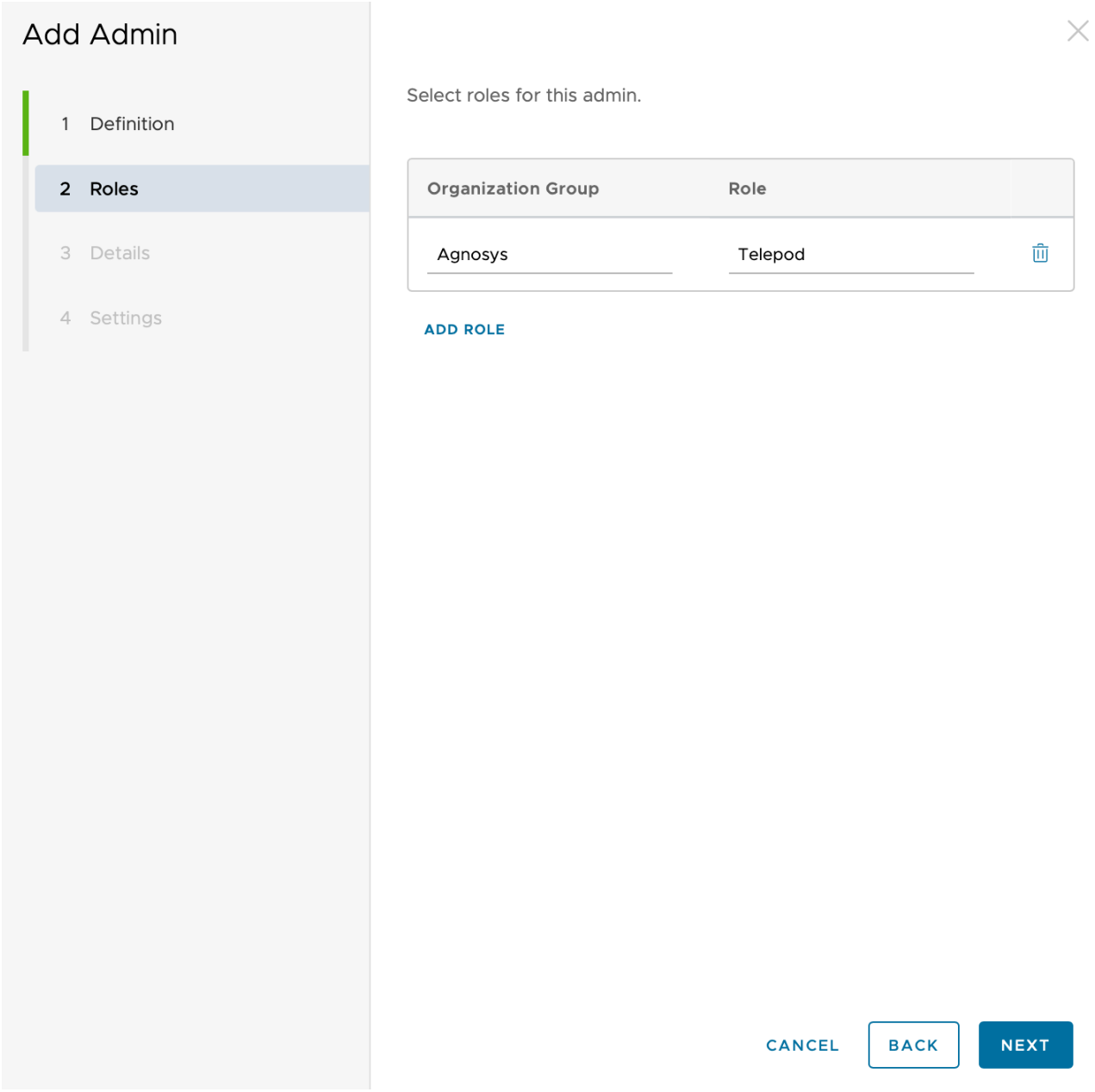
Select "Basic" then click on "Next".



Fill in the required fields.

Complete the text document with the chosen username and password.

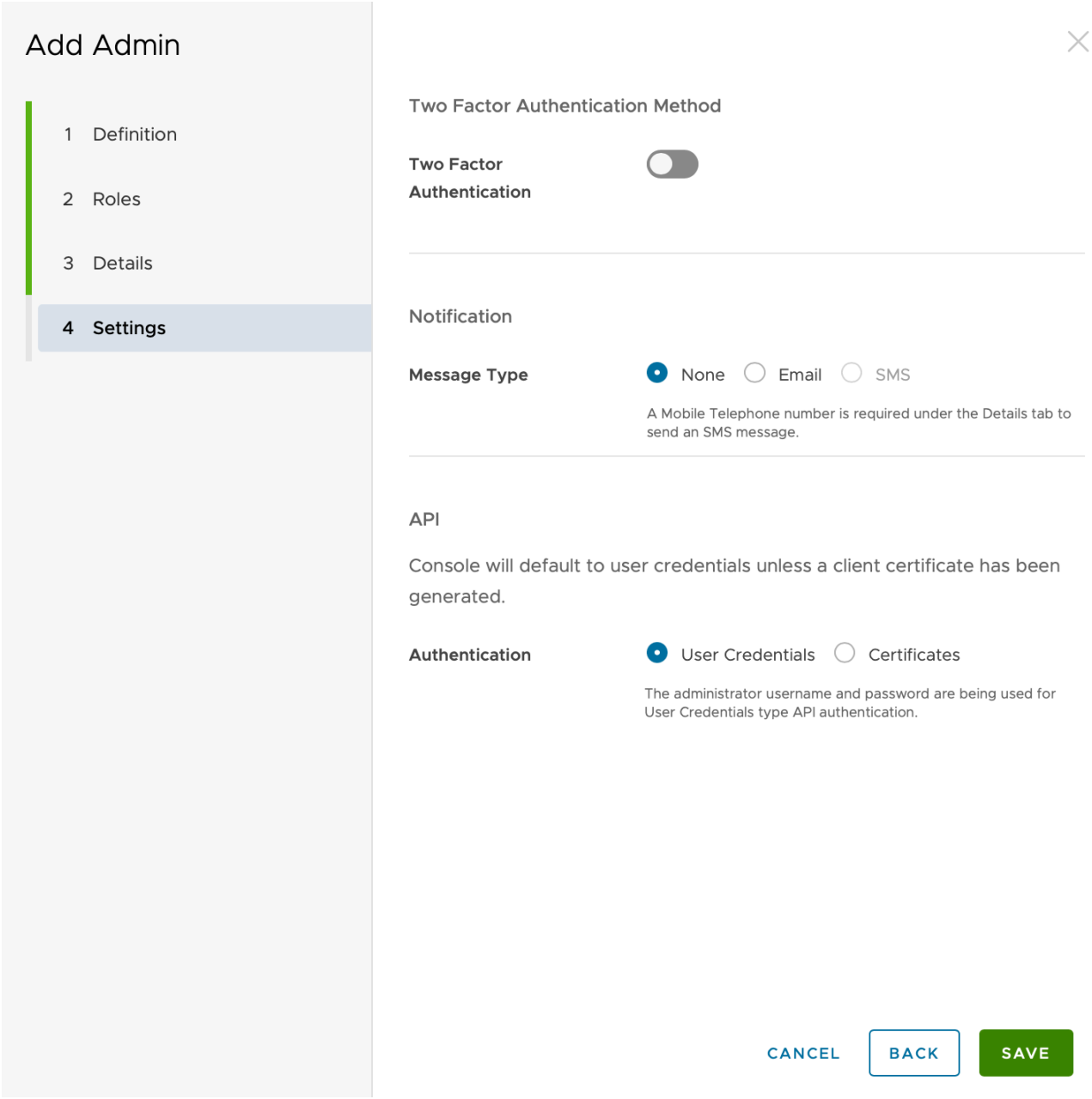
Click on "Next".



Select the Organization Group that encompasses the devices that are to be installed with Telepod, followed by the "Telepod" role.

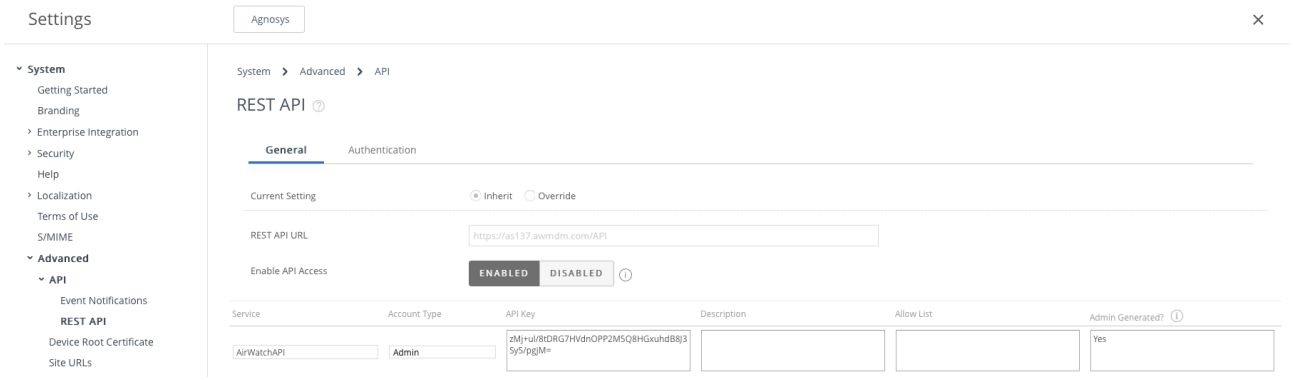
Click on "Next".

On the pane "3 Details", click on "Next".



Disable "Two Factor Authentication". For "Message Type", select "None". For "Authentication", select "User Credentials". Click on "Save".

Go to Groups & Settings > All Settings > System > Advanced > API > Rest API.



Identify the service named "AirWatchAPI" with the Account Type "Admin".

Copy the API Key and paste it in the text document.

```
Username : svc_telepod
Password : SuperSecretPassword
API Key  : zMj+ul/8tDRG7HVdnOPP2M5Q8HGxuhdB8J3Sy5/pgjM=

svc_telepod,SuperSecretPassword,zMj+ul/8tDRG7HVdnOPP2M5Q8HGxuhdB8J3Sy5/pgjM=
```

Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Supervision identities and Supervision certificates

Supervision gives organizations greater control over the devices that they own. Once a device is supervised, additional configurations can be applied.

• About Supervision

Supervision and management are two different concepts that should not be confused. A device is "managed" once enrolled in an MDM. A device can be neither supervised nor managed, only supervised, only managed, or both supervised and managed.

Organizations generally want their devices to be at least supervised and, if an MDM is available, to be supervised and managed. The process for supervising a device depends on the type of enrollment planned.

In the context of Device Enrollment, devices must be supervised over a wired connection using an additional tool. In the context of Automated Device Enrollment, devices running iOS 13 and later are forcibly supervised upon their over-the-air enrollment.

Telepod is able to supervise a device enrolled with Device Enrollment given that the workflow is configured with a Supervision identity or a Supervision certificate, the first being superior to the second. A Supervision identity contains both a private key and a certificate, while the Supervision certificate is only the certificate part of the Supervision identity. When a workflow is configured both with a Supervision identity and a Supervision certificate, the validation of the first cancels the second.

• Using Supervision identities and Supervision certificates

The use of a Supervision identity offers to supervise a device but also to allow the communication between the Mac and the device even if this last received a configuration profile which restricts the capability to "Pair with non-Apple Configurator hosts".

The use of a Supervision certificate only offers to supervise a device. If the communication between the Mac and the device is prevented by the above restriction, Telepod displays the following alert : "The new [Device] is not allowed to pair, therefore the Mac cannot communicate with it. Please contact the IT support to have the restriction removed.". The workflow is then paused until the removal is done, at least temporarily.

In addition, the use of a Supervision identity allows on a supervised device that the installation of configuration and enrollment profiles does not require a user interaction, and is a requirement for the installation of wallpapers or a locally triggered shutdown command.

Keep in mind that for a fleet of devices managed by an MDM, the Supervision identity is intended to be unique across the organization and shared between the MDM and Mac equipped with Apple Configurator and by extension Telepod. Once a device is supervised based on a Supervision identity, this last cannot be changed without wiping the device.

• **Implementing Supervision identities and Supervision certificates**

In the context of a workflow of type **Backup**, Telepod supports one Supervision identity, defined in the SUPERVISION Dictionary. It is used to pair the device to be backed up with the Mac running Telepod when pairing is prohibited by an MDM profile. If multiple Supervision identities have been previously used, the recommandation is to remove the restriction that prohibits the pairing.

In the context of a workflow of type **Migration**, Telepod supports one Supervision identity, defined in the MIGRATION_SUPERVISION Dictionary. It is used to pair the device to be migrated with the Mac running Telepod when pairing is prohibited by an MDM profile, and then to enable the non-interactive installation of an enrollment profile.

In the context of a workflow of type **Migration Back to my device**, Telepod supports two Supervision identities.

The Supervision identity defined in the MIGRATION_SUPERVISION Dictionary is used to pair the device to be migrated, enrolled in the current MDM, with the Mac running Telepod when pairing is prohibited by an MDM profile. If multiple Supervision identities have been used to supervise the devices to be migrated, the recommandation is to remove the restriction that prohibits the pairing.

The Supervision identity defined in the SUPERVISION Dictionary is used to pair the device to be migrated, enrolled in the new MDM, with the Mac running Telepod when pairing is prohibited by an MDM profile.

In the context of a workflow of type **Replacement** and **Replacement en masse**, Telepod supports two Supervision identities or one Supervision certificate and one Supervision identity.

The Supervision identity defined in the MIGRATION_SUPERVISION Dictionary is used to pair the current (source) device with the Mac running Telepod when pairing is prohibited by an MDM profile. If multiple Supervision identities have been used to supervise the current devices, the recommandation is to remove the restriction that prohibits the pairing.

The Supervision identity defined in the SUPERVISION Dictionary is used to supervise the new (destination) device and to pair it with the Mac running Telepod when pairing is prohibited by an MDM profile. Alternatively, the Supervision certificate also defined in the SUPERVISION Dictionary is used to supervise the new device only, expecting pairing is never restricted.

In the context of a workflow of type **Setup** and **Setup en masse**, Telepod supports one Supervision identity or certificate. The Supervision identity defined in the SUPERVISION Dictionary is used to supervise the device and to pair it with the Mac running Telepod when pairing is prohibited by an MDM profile. Alternatively, the Supervision certificate also defined in the SUPERVISION Dictionary is used to supervise the new device only, expecting pairing is never restricted.

In the context of a workflow of type **Sorting**, Telepod supports one Supervision identity, defined in the SUPERVISION Dictionary. It is used to pair the device to inspect with the Mac running Telepod when pairing is prohibited by an MDM profile. If multiple Supervision identities have been previously used, the recommandation is to remove the restriction that prohibits the pairing.

• **Defining the correct Supervision identities**

The challenge is to define where a Supervision identity comes from in the first place. The answer to this question depends on the MDM involved.

Some MDMs can forge a Supervision identity than can be exported for sharing with Apple Configuration hosts, but are not able to import an existing Supervision identity. In this situation, the Supervision identity must be exported from the MDM, declared in the SUPERVISION Dictionary and embedded in the Telepod Content.

Other MDMs can forge a Supervision identity but can also import an existing Supervision identity. In this situation, an evaluation of the situation is required, where history is critical. First focus to decide which Supervision identity should be used between one created in the MDM and imported in Apple Configurator, or another one created in Apple Configurator and imported in the MDM. This choice is yours and depends on how devices have been supervised to date. Once the correct Supervision identity is defined, it must be configured in the SUPERVISION Dictionary and embedded in the Telepod Content.

In the context of a workflow of type Migration, Migration Back to my device, Replacement or Replacement en masse, the Supervision identity used to supervise the devices to be migrated or the current (source) devices must be configured in the MIGRATION_SUPERVISION Dictionary and embedded in the Telepod Content.

Please refer to the MDM documentation to know what it offers for exporting and importing Supervision identities. Do not hesitate to open a support ticket with the MDM support or the Telepod support to get clarifications.

• **Preparing Supervision identities or Supervision certificates for Telepod**

Once a Supervision identity has been defined, it must be prepared for its usage with Telepod.

A PKCS#12 (P12) file is an archive file format for storing cryptographic objects as a single file. The keystore contains both the private and the public key and is protected by a password.

When exported from an MDM, the Supervision identity is expected to be provided as a PKCS#12 (P12) file, protected by a password of your choice or provided by the MDM.

To export an existing Supervision identity from Apple Configurator :
- open Settings > Organizations
- select the organization associated to the Supervision identity to export
- click on the More button (...) then select Export Supervision Identity
- select an output folder, the Encrypted PKCS12 format then click on Save
- enter the password of your choice, verify the password then click on OK
- the Supervision identity is exported as a PKCS#12 (P12) file protected by the chosen password.

To configure a Supervision identity, proceed with the following steps :
- move the archive file to the "Content" folder of the Telepod Content (refer to the "Telepod Content building" chapter for more information)
- inside a SUPERVISION or MIGRATION_SUPERVISION Dictionary, set the "IDENTITY" key to the name of the file
- use the script "telepod_rsa_engine" to generate an encrypted value of the file password
- use this value including the "RSA-" prefix as the value for the corresponding "IDENTITY_PASSWORD" key.

Alternatively, if a Supervision identity cannot be added to the Telepod Content for security concerns, proceed with the following steps to configure a Supervision certificate extracted from a Supervision identity :
- while holding the Option key, right-click the archive file and select 'Copy "*archive_file*.p12" as Pathname'
- execute the script "telepod_rsa_supervision_identity_engine.command"
- after "Paste here the copied pathname", paste the pathname to the archive file
- after "Enter the password", enter the password that protects the archive file
- open /Users/Shared
- delete the file named "privateKey.der"
- move the file named "publicCert.der" to the "Content" folder of the Telepod Content (refer to the "Telepod Content building" chapter for more information)
- inside a SUPERVISION Dictionary, set the "CERTIFICATE" key to the name of the file.

The Telepod Content can embed multiple Supervision identities or Supervision certificates with distinct file names. Then each workflow defined by the Telepod configuration file can refer to the same items provided by the Telepod Content.

• Verifying the supervision identity shared between the MDM and Telepod

A Supervision identity is intended to be unique across the organization and shared between the MDM and the Mac hosts running Telepod.

To verify that devices supervised by the MDM via Automated Device Enrollment use the same supervision identity as Telepod, create a Sorting workflow that includes the "Device Shutdown" task in its Blueprint.

If the device pane displays the message "Waiting for shutdown completion..." and the device eventually shuts down, the verification is successful.

If the device pane displays the message "Workflow and device supervision identities do not match." and the device does not shut down, the verification fails. In this context, Telepod’s functionality may not be optimal, and certain tasks may not be performed.

Table of workflow settings supported by the MDM solutions

• Replacement workflow

A workflow of type Replacement offers to trigger an unenroll or erase action for the device to be replaced by making an API call to the MDM in which this device is enrolled.

In the SETTINGS Dictionary :

- Action on the current device after it has been backed up :

    Set the key to "unenroll" to trigger this action by the MDM

    Note : The key can also be set to "erase" but the action is then managed locally as the device to be replaced is still connected to the Mac after it has been backed up.

- Action on the current device after the new device is enrolled :

    Set the key to "unenroll" or "erase" to trigger the desired action by the MDM

    Note : The device to be replaced must be erased remotely as it is not connected to the Mac after the new device is enrolled.

If "Action on the current device after it has been backed up" is set to "unenroll" or "erase", "Action on the current device after the new device is enrolled" is forcibly disabled because a device remotely unenrolled or locally erased after its backup cannot be remotely unenrolled nor erase afterwards.

Please refer to the following table to define if the MDM in which the replaced device is enrolled can be driven by an API call for the unenroll and erase actions.

• Replacement en masse workflow

A workflow of type Replacement en masse offers to trigger an unenroll or erase action for the device to be replaced by making an API call to the MDM in which this device is enrolled.

In the SETTINGS Dictionary : Action on the source device after the destination device is ready

    Set the key to "unenroll" or "erase" to trigger the desired action by the MDM

    Note : The device to be replaced is locally erased if it is still connected when the destination device is ready ; otherwise, a remote erase is triggered as a fallback.

• Support for unenroll and erase actions by the supported MDM solutions

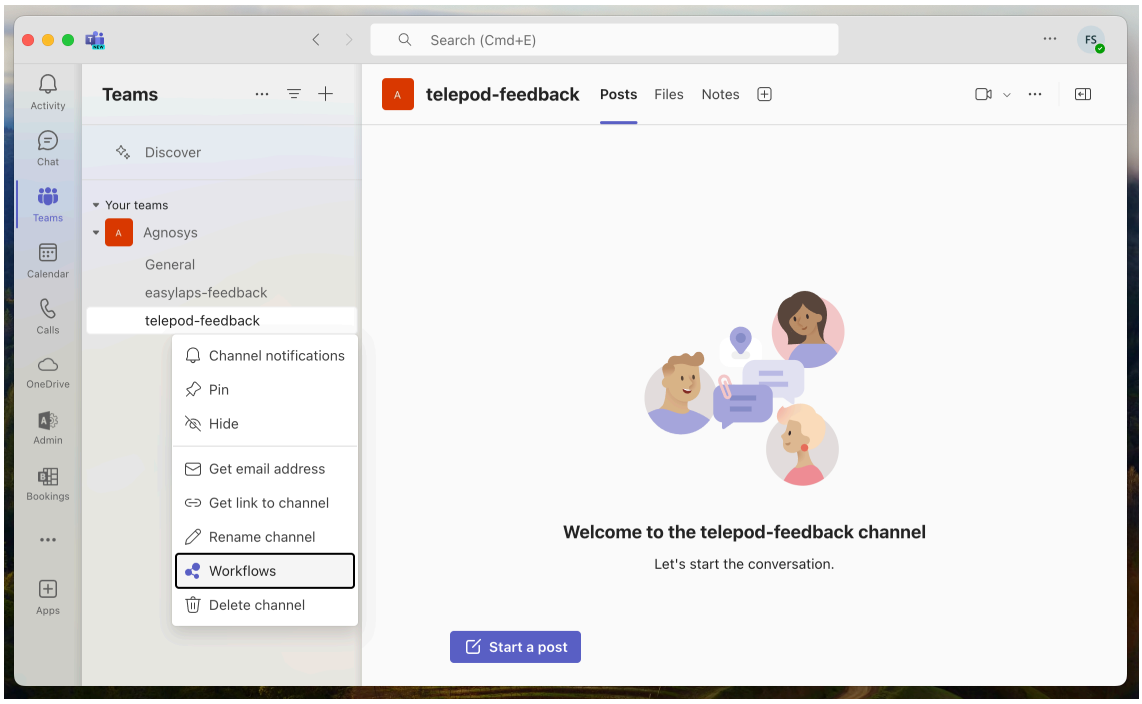
MDM Solution	Unenroll action	Erase action
FileWave	✓ Device unenrolled and deleted in MDM	✓ Device wiped
Hexnode UEM	✓ Device unenrolled and deleted in MDM	✗ Wipe device action not available
Jamf Now	✗ No API	✗ No API
Jamf Pro	✓ Device unenrolled	✓ Device wiped, Activation Lock cleared
Jamf School	✓ Device unenrolled	✓ Device wiped, Activation Lock cleared
JumpCloud	✓ Device unenrolled and deleted in MDM	✓ Device wiped, Activation Lock cleared
Kandji	✓ Device unenrolled and deleted in MDM	✓ Device wiped
ManageEngine MDM	✗ No API	✗ No API
Meraki Systems Manager	✓ Device unenrolled	✓ Device wiped, Activation Lock cleared
Microsoft Intune	✓ Device unenrolled	✓ Device wiped, Activation Lock cleared
Miradore	✓ Device unenrolled	✓ Device wiped
Mosyle Business	✗ Unenroll device action not available	✓ Device wiped
Mosyle Manager	✗ Unenroll device action not available	✓ Device wiped
SimpleMDM	✓ Device unenrolled and deleted in MDM	✓ Device wiped
VMware Workspace ONE	✓ Device unenrolled	✓ Device wiped

Note : After an Activation Lock has been successfully disabled, even if a limited to owner pane is still displayed on reboot, the Activation Lock is really gone.

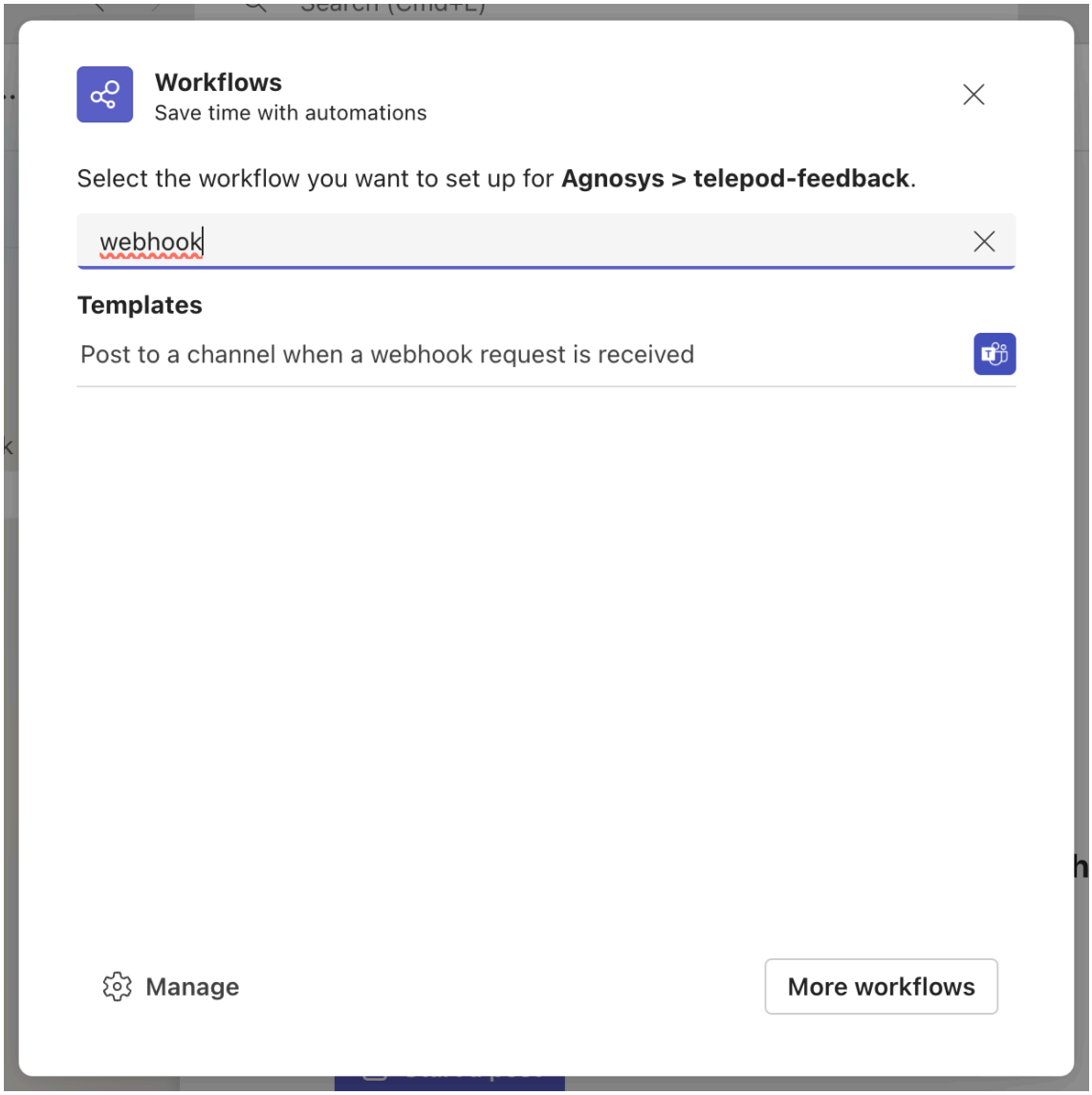
Microsoft Teams integration

Telepod can report to a dedicated Microsoft Teams channel the successive status of a running workflow.

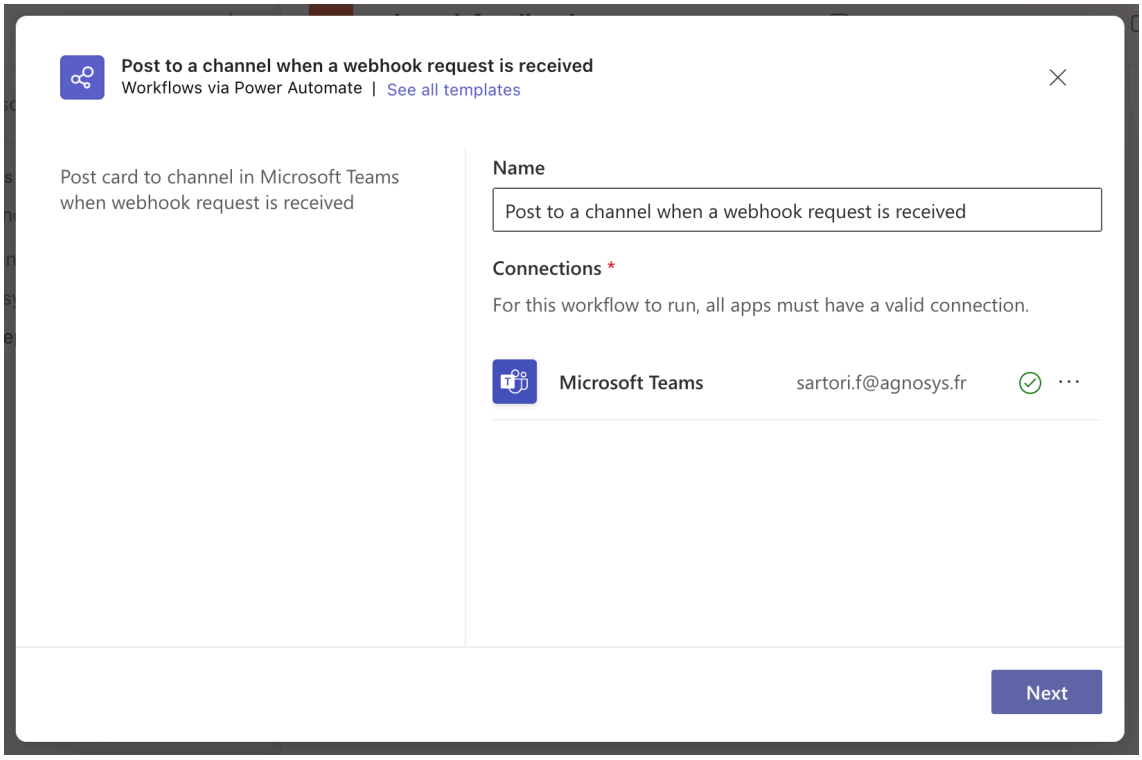
First create a dedicated Microsoft Teams channel of type "Standard" (everyone on the team has access).



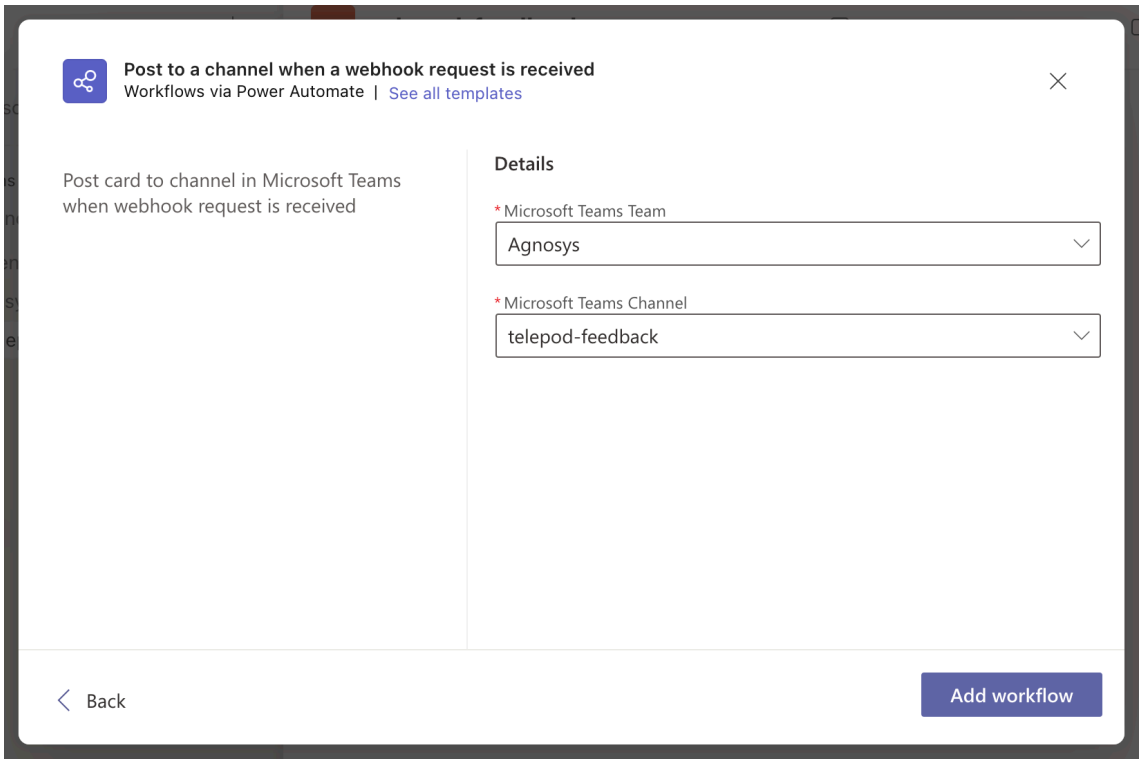
Click on the "..." button to the right of the channel name, then select "Workflows".



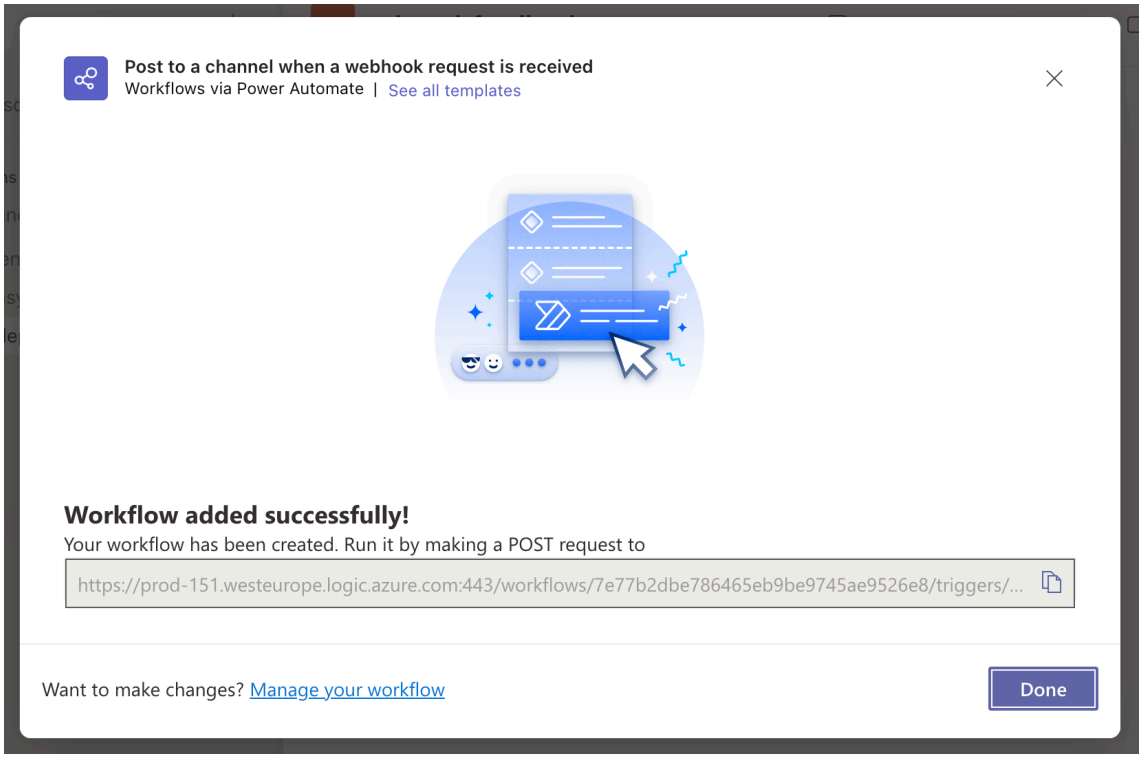
Type "webhook" in the search field, then click on "Post to a channel when a webhook request is received".



Once the connection is indicated as valid with a green tick, click on "Next".



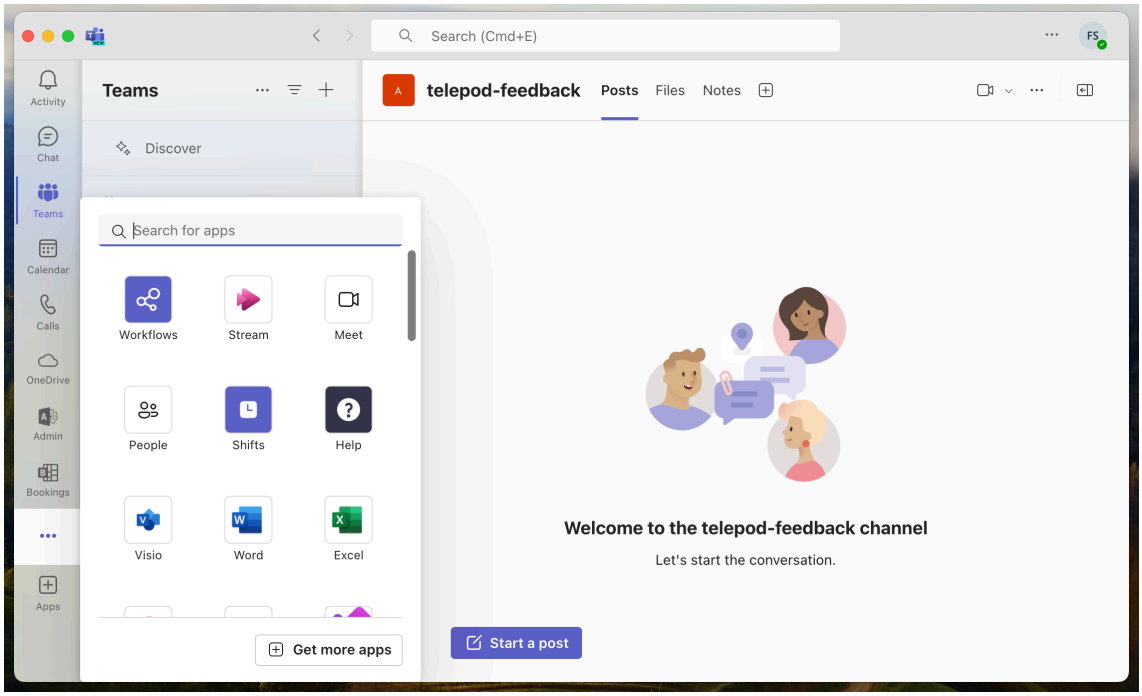
Check the Microsoft Teams team and the Microsoft Teams channel, then click on "Add workflow".



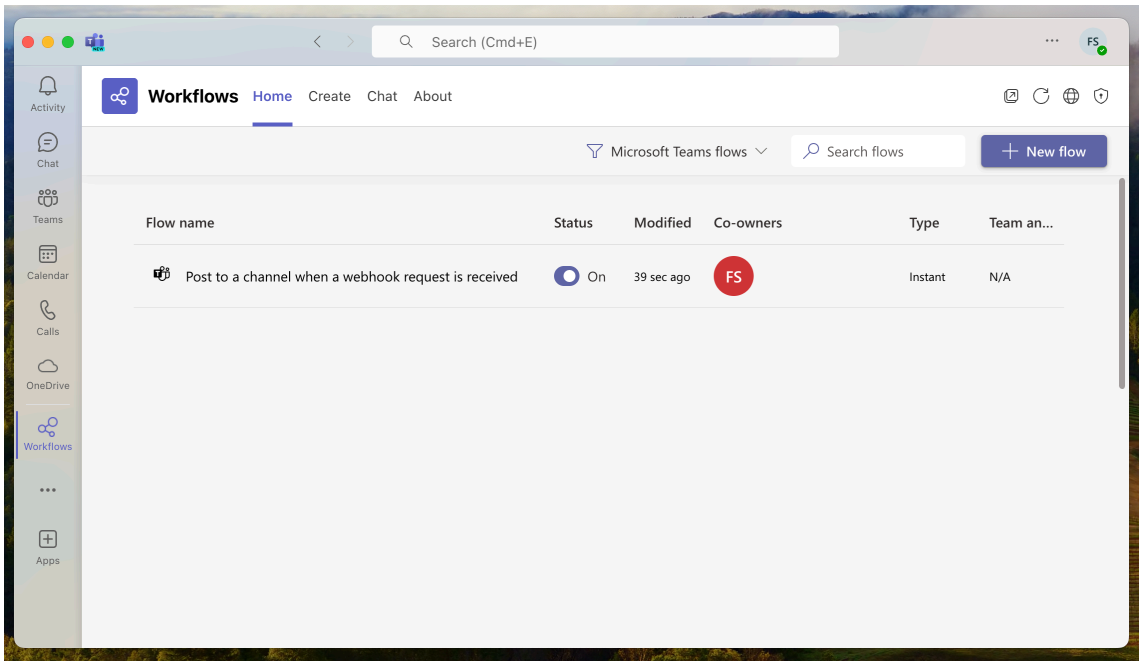
Click on the button to the right of the URL displayed to copy it, then follow these instructions :
- open the "Telepod-Toolkit" folder
- open the "telepod_secrets" subfolder
- execute the "telepod_rsa_engine" script (double-click on the .command file)
- paste the copied URL
- the URL is encrypted, displayed and then decrypted for sanity check
- copy the encrypted URL (one-line string ending exactly with two "=" characters)
- paste the encrypted URL in the INTEGRATIONS > TEAMS_CONFIGURATION > INCOMING_WEBHOOK_URL key.

Make sure that :
- the INTEGRATIONS > TEAMS_INTEGRATION key is set to "true"
- the INTEGRATIONS > TEAMS_CONFIGURATION > INCOMING_WEBHOOK_PROCESSING key is set to "workflows".

Back in the pane, click on "Done".



Click on the "..." Button in the sidebar, then click on "Workflows" to display this app.



Click on the created workflow to display its details if you want to.

Telepod configuration files to Custom configuration profiles conversion

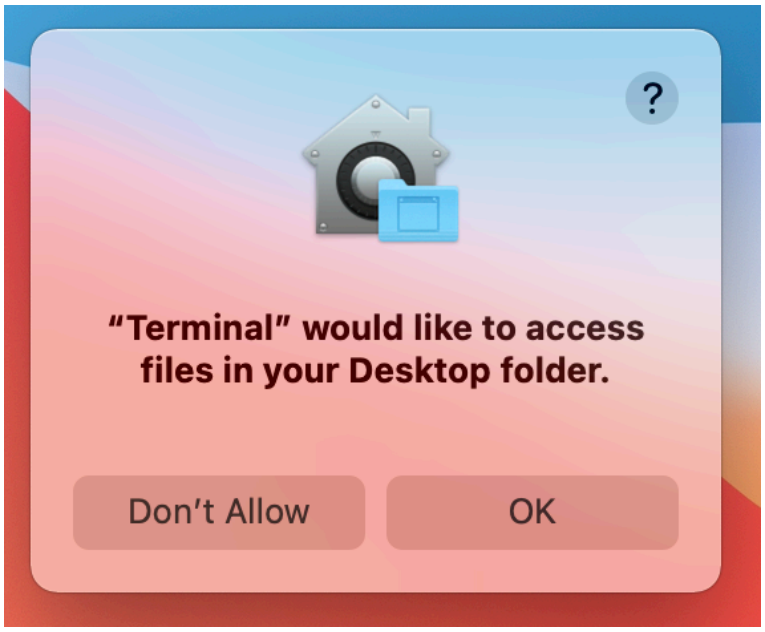
If the MDM solution is Jamf Pro, this step is optional because this MDM offers to upload a Telepod configuration file directly into a Configuration profile that includes an "Application & Custom Settings" payload. However, if you prefer to upload in Jamf Pro a pre-built Custom configuration profile, follow these instructions.

Open the "Telepod-Toolkit" folder.

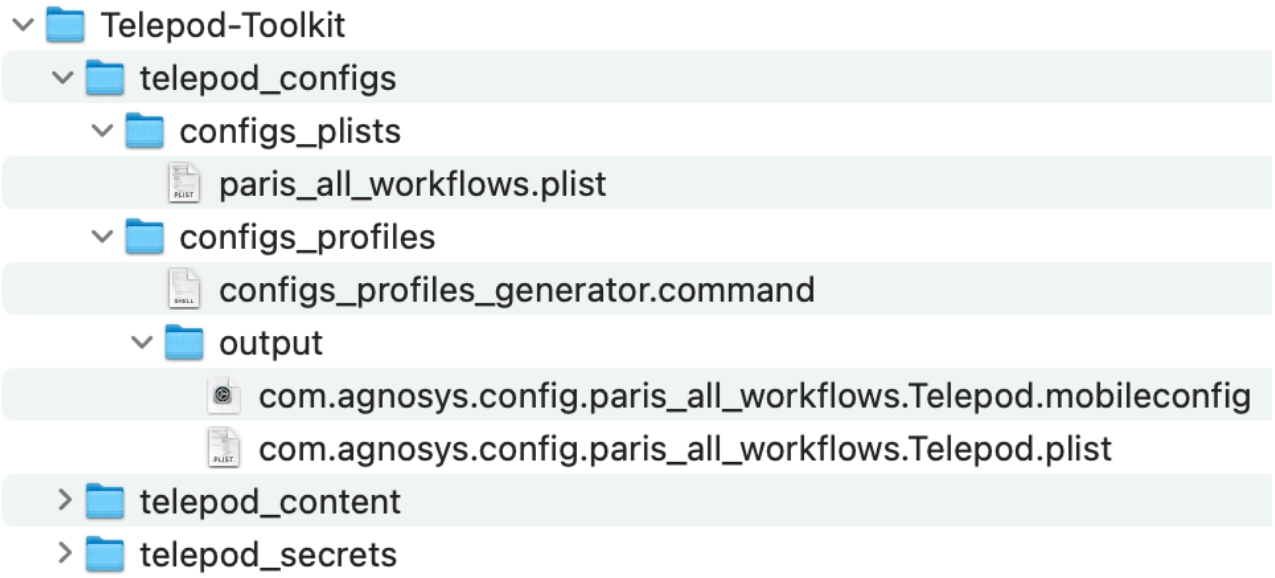
Open the "telepod_configs" subfolder.

Open the "configs_profiles" folder.

Execute the "configs_profiles_generator" script (select the script > right-click > Open).



If prompted to authorize the Terminal app to access files in a specific folder like your Desktop folder, click on "OK".



In this example, the script has converted one Telepod configuration file into two files :
- one Telepod Custom configuration profile with the extension ".mobileconfig"
- one Telepod Custom configuration profile with the extension ".plist".

Those two profiles are ready to be deployed by an MDM (only one must be scoped to a specific Mac host) :
- the one with the extension ".plist" is needed if the MDM solution is VMware Workspace ONE, and its content is used to populate a Custom Settings payload
- the one with the extension ".mobileconfig" is needed for all other MDM solutions.

Telepod Content building

All pictures (.png), files (.csv, .md, .txt), identities (.p12), certificates (.crt, .der), configuration profiles (.mobileconfig), documents (.pdf) and bundles (.bundle) referenced in the Telepod configuration file(s) must be embedded in the Telepod-Content package.

The Telepod-Content package is deployed alongside the Custom configuration profile derived from the Telepod configuration file, via the MDM.

Depending of the MDM used and the distribution method implemented, the signature of the package, even always recommended, may become a requirement. However, the notarization is never required.

Package signature requirement

• **FileWave**

No signature required.

• **Hexnode UEM**

Signature required.

• **Jamf Now**

Signature required.

• **Jamf Pro**

This documentation plans that the Telepod-Content package is deployed via the Packages payload of a policy which does not require that the package is signed.

• **Jamf School**

No signature required.

• **JumpCloud**

Signature required since the package is hosted in the JumpCloud Private Repo.

• **Kandji**

No signature required.

• **Meraki Systems Manager**

No signature required.

• **Microsoft Intune**

No signature required when the package is provisioned as a macOS app.

• **Miradore**

Signature required.

• **Mosyle Business**

No signature required unless the option "Install with Apple Protocol" is enabled in the deployment configuration.

• **Mosyle Manager**

No signature required unless the option "Install with Apple Protocol" is enabled in the deployment configuration.

• **SimpleMDM**

Signature required.

• **VMware Workspace ONE**

This documentation plans that the Telepod-Content package is deployed as a regular package with the "Full Software Management" deployment type which does not require that the package is signed.

Package signature options

These are some options to sign the Telepod-Content package.

• Subscribe to an Apple Developer program, create a "Developer ID Installer" certificate and use it to sign the package.

• With Jamf Pro : create a certificate with the Jamf Pro's Built-in CA and use it to sign the package with these informations in mind :

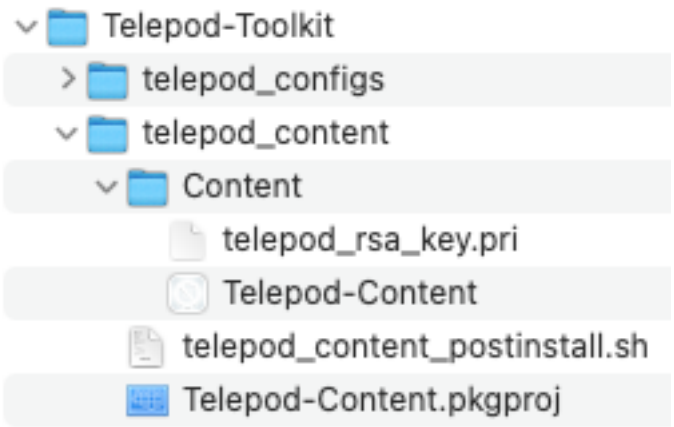
- the certificate forged with the Jamf Pro's Built-in CA can be validated by a device only if it is already enrolled in Jamf Pro
- for more information, please consult this article : https://docs.jamf.com/technical-articles/Creating_a_Signing_Certificate_Using_Jamf_Pros_Built-in_CA_to_Use_for_Signing_Configuration_Profiles_and_Packages.html
- once the signing identity is available in the "login" keychain, click on "Certificates" to check the certificate associated with the private key, then sign the unsigned package produced by the Packages app with the following command :

```
productsign --sign "name_of_certificate" Telepod-Content.pkg Telepod-Content_signed.pkg
```

- ignore the section below entitled "Signing configuration" as the package is now signed.

• Open a Telepod support ticket to get the package signed by Agnosys or your integrator.

Content gathering



Open the "Telepod-Toolkit" folder.

Open the "telepod_content" subfolder.

Open the "Content" folder.

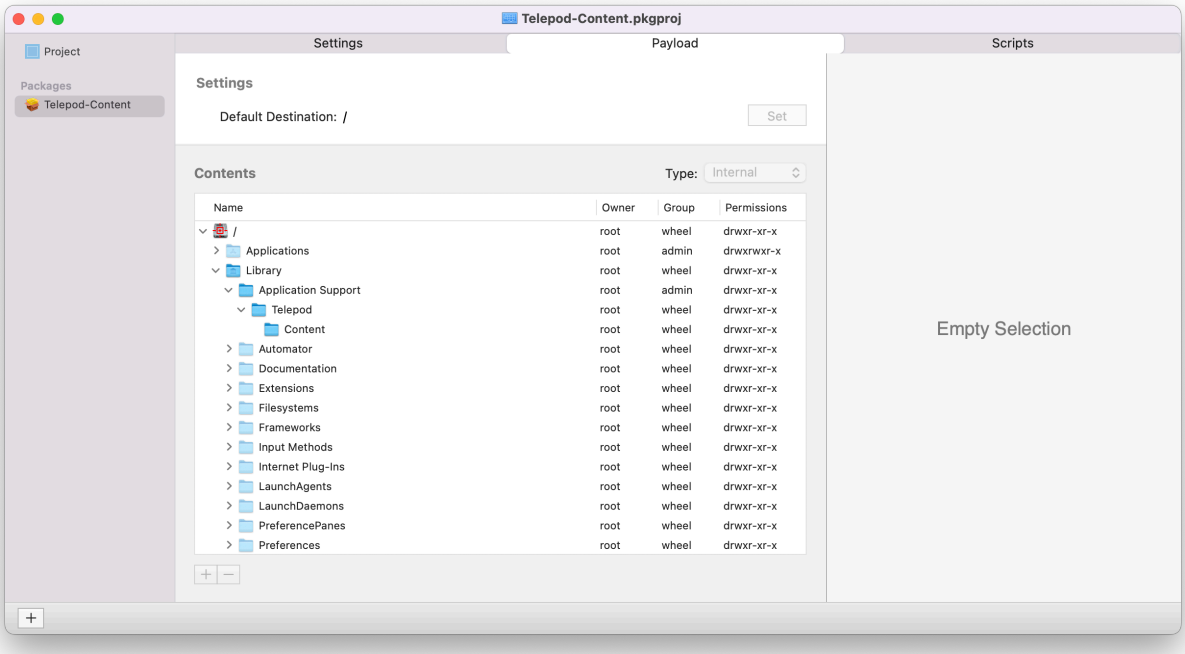
Copy your content in the "Content" folder, alongside the "telepod_rsa_key.pri" file and the detection app named "Telepod-Content.app".

Project opening

Open the "Telepod-Toolkit" folder.

Open the "telepod_content" subfolder.

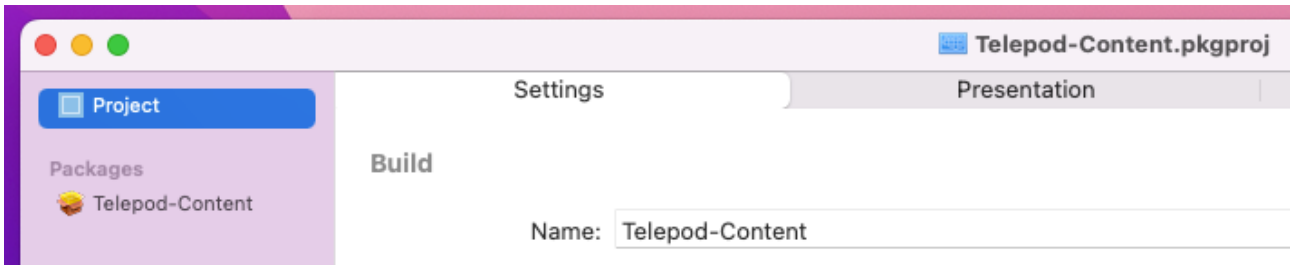
Open the "Telepod-Content.pkgproj" file with the Packages app.



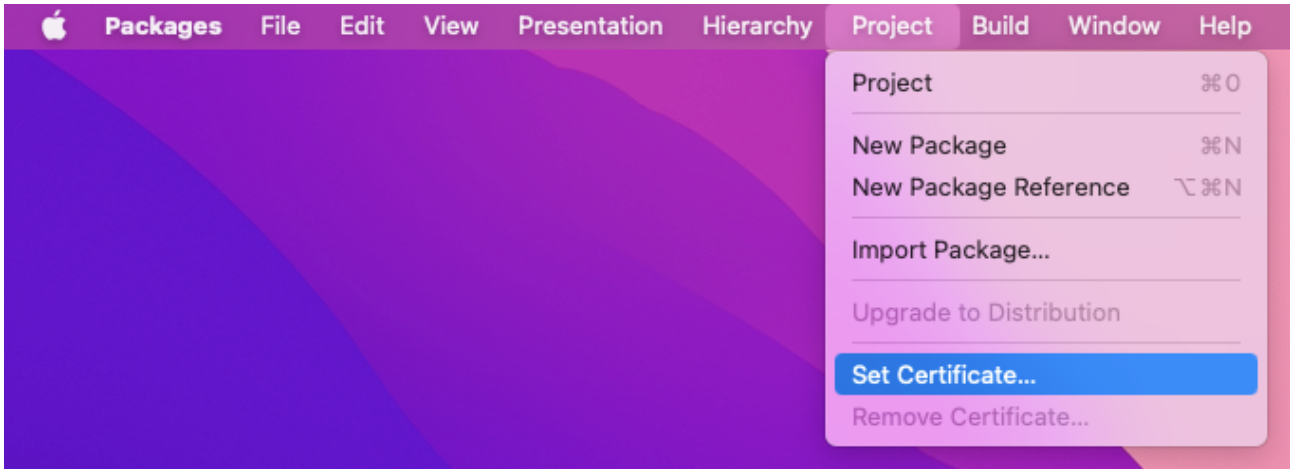
The generated package will embed the "Content" folder for an installation in /Library/Application Support/Telepod/

Signing configuration

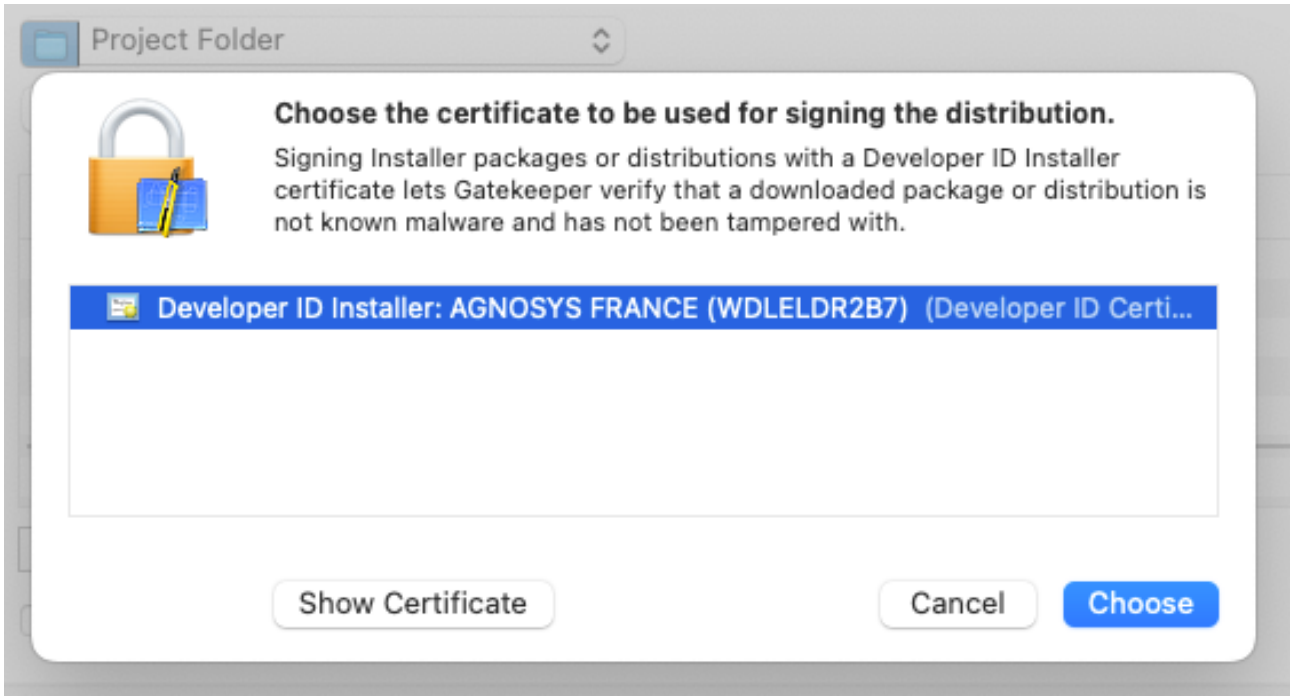
Open the Keychain Access app and check that your "Developer ID Installer" certificate is installed in the "login" keychain.



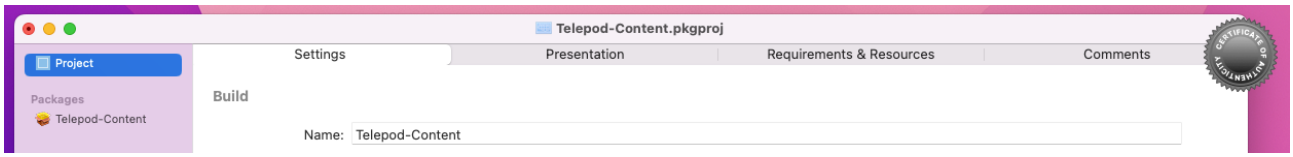
Click on "Project" then select the "Settings" tab.



Select Project > Set Certificate.

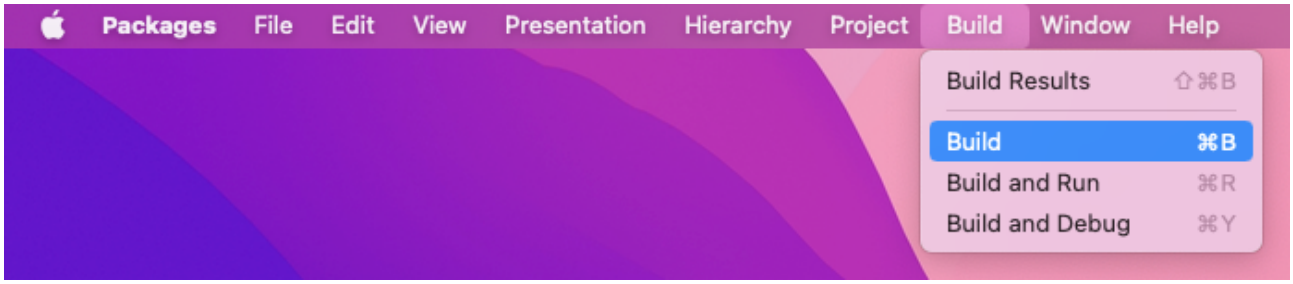


Select your "Developer ID Installer" certificate and click on "Choose".

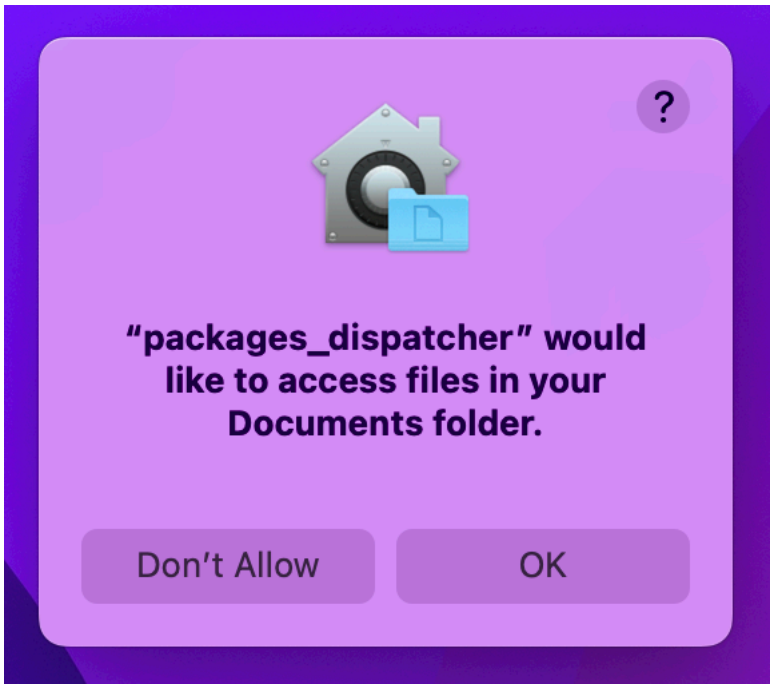


A "Certificate of authenticity" badge is now visible in the upper right corner of the project window.

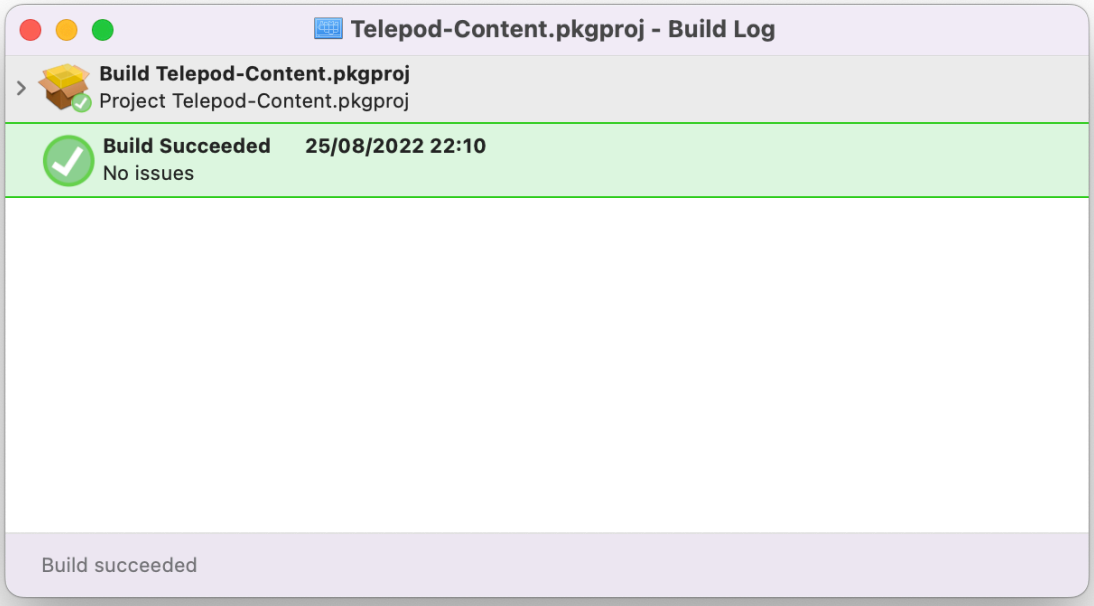
Project building



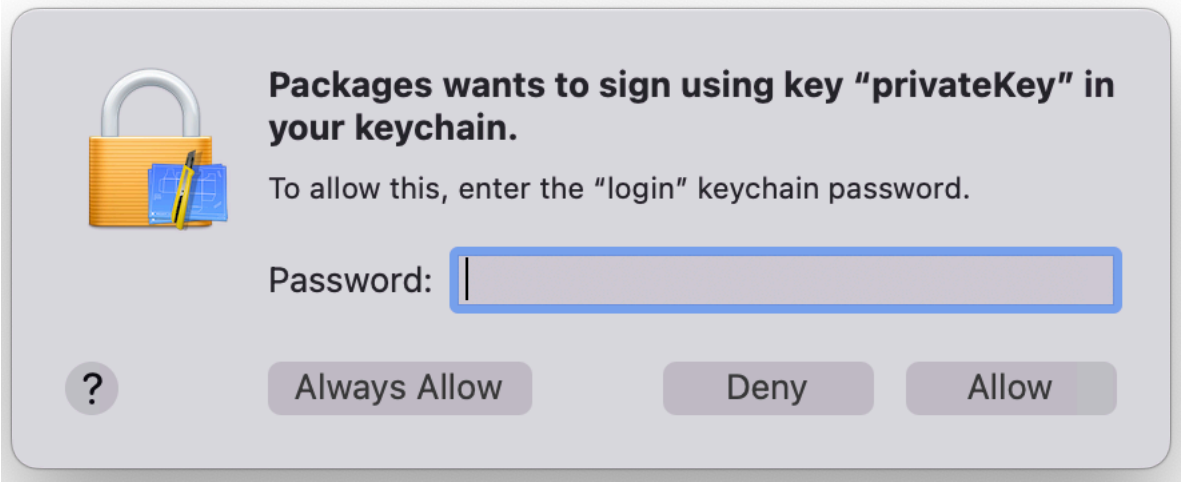
Select Build > Build.



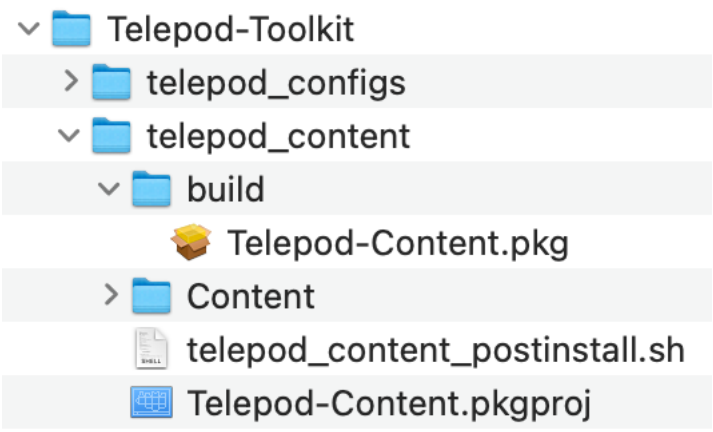
If prompted to authorize the Packages app to access files in a specific folder like your Desktop folder, click on "OK".



The Build Log must display "Build Succeeded — No issues".



During the building, if you previously set a signing certificate, you may be prompted to authorize Packages to access the private key of your "Developer ID Installer" certificate. Enter your account's password and click on "Always Allow".



The package is built at the following path :
Telepod-Toolkit > telepod_content > build

You can now quit the Packages app. Choose to save the changes made to the project if you are offered to do so.

Configuration profiles requirements

This section details the configuration profiles required by Telepod in addition to the Telepod Custom configuration profile.

Privacy Preferences Policy Control

A PPPC configuration profile must be deployed so Telepod is able to :

- workflow of type Backup :
    - collect the size of the backup of the connected device
    - collect the size of the other devices backups
    - delete the backups of other devices
    - collect the size of the created backup
    - move the created backup from the logged in user's home to the cache (*)
    - remediate the ownership of the MobileSync folder and its Backup subfolder
- workflow of type Migration Back to my Device :
    - collect the size of the backup of the current device
    - collect the size of the other devices backups
    - delete the backups of other devices
    - delete the backup of the device to be migrated after the pivot device is enrolled
    - delete the backup of the pivot device after the device to be migrated is enrolled
    - remediate the ownership of the MobileSync folder and its Backup subfolder
- workflow of type Replacement :
    - collect the size of the backup of the current device
    - collect the size of the other devices backups
    - delete the backups of other devices
    - delete the backup of the current device once it is replaced
    - remediate the ownership of the MobileSync folder and its Backup subfolder
- workflow of type Replacement en masse :
    - collect the size of the backup of a source device
    - delete the backup of a source device once the destination device is ready
    - remediate the ownership of the MobileSync folder and its Backup subfolder
    - upload the Device Mapping CSV file from the logged in user's home
    - upload the Placeholders CSV file from the logged in user's home

- workflow of type Setup and Setup en masse :

    - collect the size of the backup to be restored
    - collect the product type of the backup to be restored
    - collect the operating system version of the backup to be restored
    - move the backup to be restored from the cache to the logged in user's home (**)
    - upload the Digital signage CSV file from the logged in user's home
    - upload the Placeholders CSV file from the logged in user's home

(*) Requirement to upload the created backup from the local cache to the distribution point.

(**) Requirement to restore a backup synched from the distribution point to the local cache.

Payload required : Privacy Preferences Policy Control

- Identifier Type : Bundle ID

- Identifier : `com.agnosys.telepod_privileged_helper`

- Code Requirement : `identifier "com.agnosys.telepod_privileged_helper" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = WDLELDR2B7`

    Note : The string is a single-line string when pasted into the Code Requirement field, with no line breaks.

- Validate the Static Code Requirement : No

- App or Service :

    - System Policy All Files : Allow

Please find below the known issues and limitations when the configuration profile is missing.

For a workflow of type **Backup** :
- the sizes of the backups that cannot be collected are ignored during the storage requirement evaluation
- the backups of other devices cannot be deleted to free up space for the backup of the connected device
- the created backup cannot be uploaded to the distribution point ; the error "Preparation of the backup of device *UUID* for upload to the distribution point *Share* failed" is visible in the log and reported by the webhooks
- the ownership of the MobileSync folder and its Backup subfolder cannot be remediated to the logged in user.

For a workflow of type **Migration Back to my Device** :
- the sizes of the backups that cannot be collected are ignored during the storage requirement evaluation
- the backups of other devices cannot be deleted to free up space for backing up the current device
- the backup of the current device cannot be deleted ; the error "Backup deletion of the current device failed" is visible in the log and reported by the webhooks
- the backup of the pivot device cannot be deleted ; the error "Backup deletion of the pivot device failed" is visible in the log and reported by the webhooks
- the ownership of the MobileSync folder and its Backup subfolder cannot be remediated to the logged in user.

For a workflow of type **Replacement** :
- the sizes of the backups that cannot be collected are ignored during the storage requirement evaluation
- the backups of other devices cannot be deleted to free up space for backing up the current device
- the backup of the current device cannot be deleted ; the error "Backup deletion of the current device failed" is visible in the log and reported by the webhooks
- the ownership of the MobileSync folder and its Backup subfolder cannot be remediated to the logged in user.

For a workflow of type **Replacement en masse** :
- the sizes of the backups that cannot be collected are ignored during the storage requirement evaluation
- the backups of source devices whose peers are ready cannot be deleted to free up space for backing up other source devices ; the error "Backup deletion of the source device failed" is visible in the log and reported by the webhooks
- the ownership of the MobileSync folder and its Backup subfolder cannot be remediated to the logged in user
- uploading the Device Mapping CSV file from the logged-in user’s home directory fails
- uploading the Placeholders CSV file from the logged-in user’s home directory fails.

For a workflow of type **Setup** and **Setup en masse** :
- a backup cannot be cached from a distribution point ; the error "Provisioning the backup UDID *UDID* in the home of the logged in user account *FullName* (*AccountName*) failed" is visible in the log and reported by the webhooks
- when the backup is not retrieved from the distribution point : the size, the product type and the operating system version of the backup to be restored are read respectively from the SIZE_UNIT_MB, PRODUCT_TYPE and PRODUCT_VERSION keys (refer to the Telepod Dictionary for more information)
- when the backup is retrieved from the distribution point : the size, the product type and the operating system version of the backup to be restored are read from a file embedded in the disk image and therefore the three keys listed above are ignored
- uploading the Digital Signage CSV file from the logged-in user’s home directory fails
- uploading the Placeholders CSV file from the logged-in user’s home directory fails.

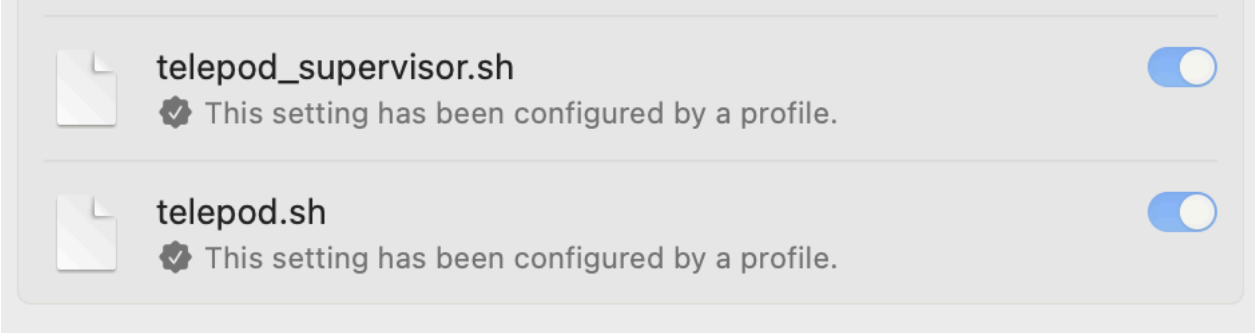
Background Item Management

With macOS 13 and later, a Background Item Management configuration profile must be deployed so that the system does not display a notification that Telepod has installed a Login item that can run in the background and that can be managed in System Settings.

Payload required : Background Item Management

- Rule Type : Label
- Rule Value : com.agnosys.telepod

- Rule Type : Label
- Rule Value : com.agnosys.telepod_supervisor



Once the configuration profile is deployed on a Mac host running Telepod, open System Settings > Login Items and check that the provisioned Login Items are enabled and cannot be disabled.

If the MDM solution does not yet offer the payload "Background Item Management", you may deploy the signed profile titled "telepod_btm_signed.mobileconfig" provided in the subfolder "telepod_library" of the Telepod Toolkit.

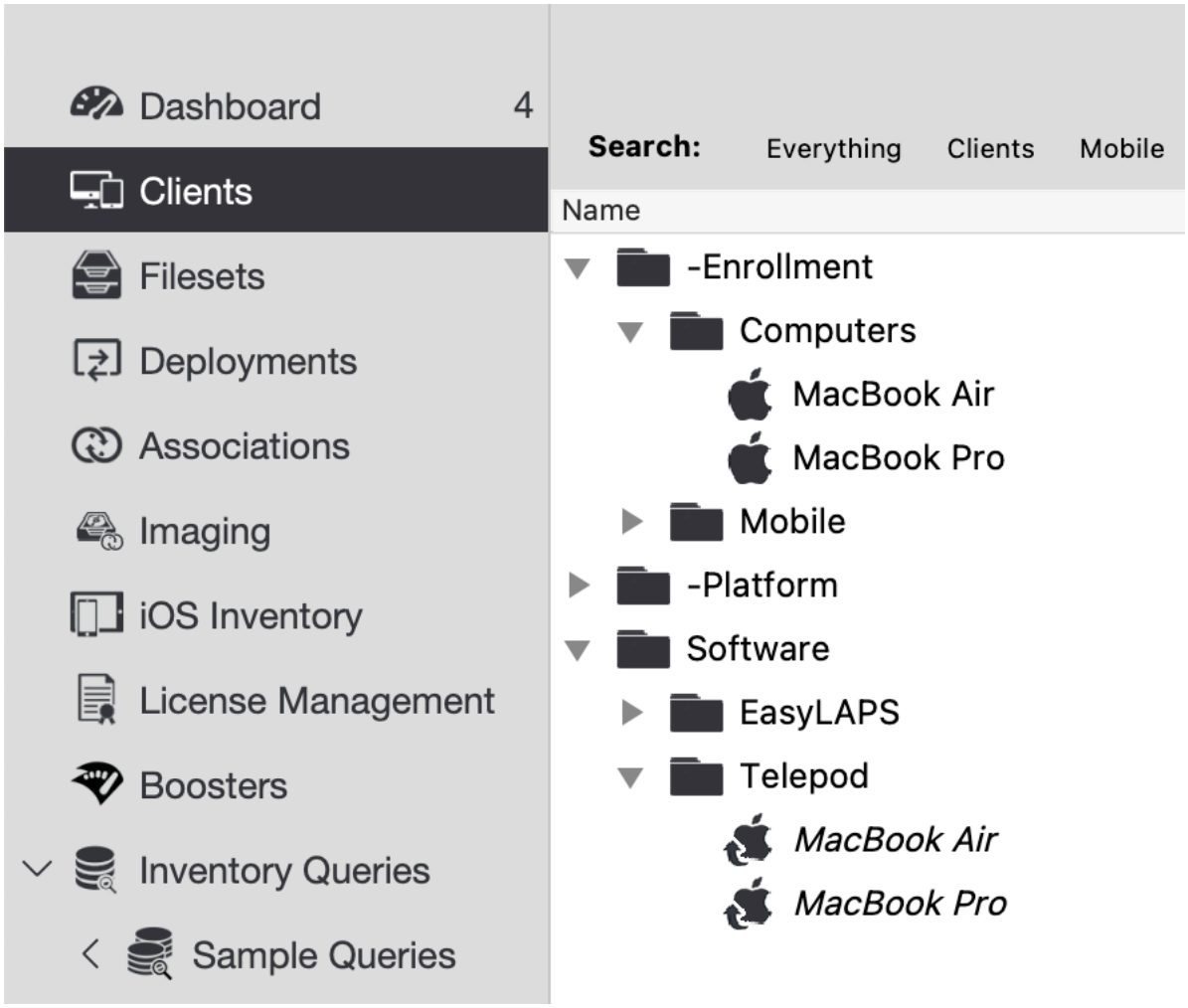
Provisioning FileWave

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-App package (administrative privileges required to run the embedded app).

This section outlines the key points for the provisioning of these three components in FileWave. Please refer to FileWave documentation for details not specific to Telepod.

General configuration

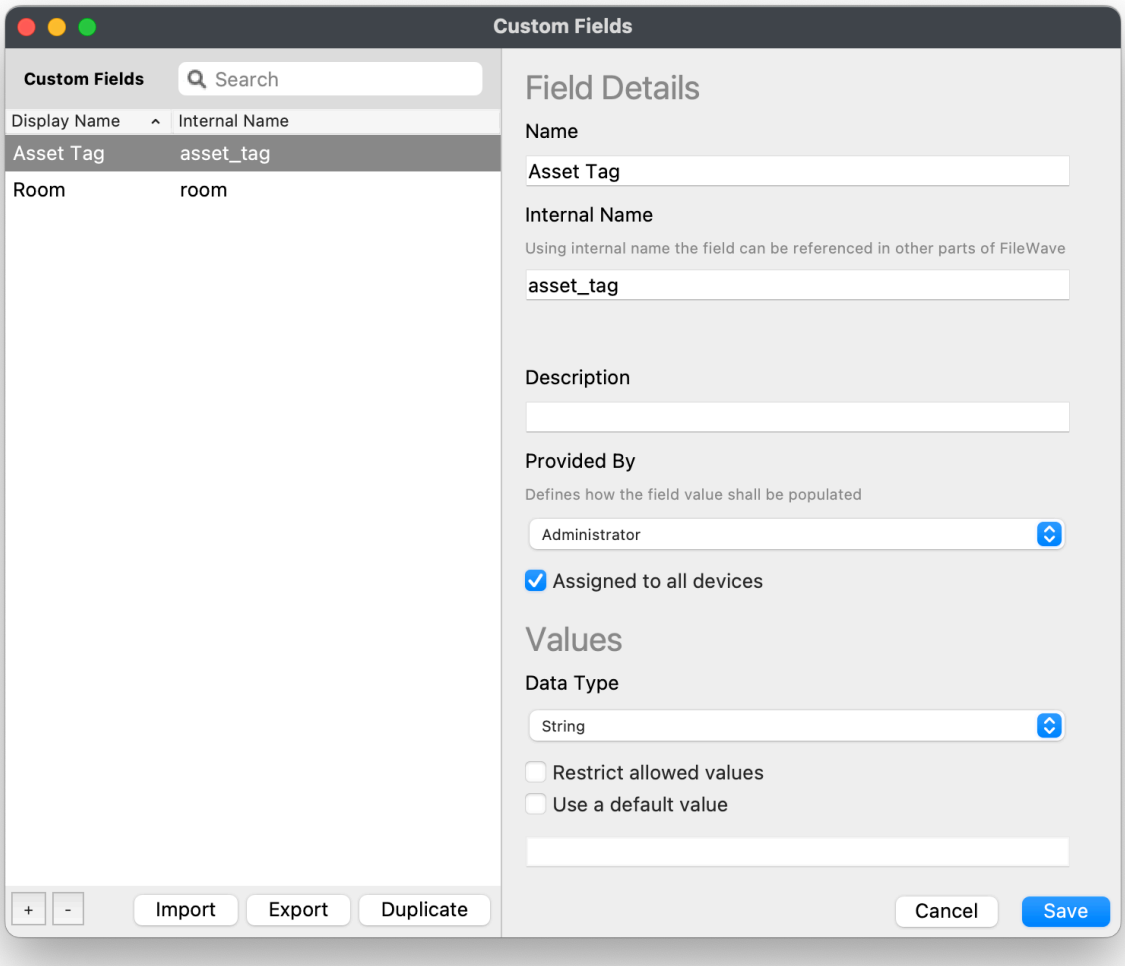
In this example, the devices are part of group named "Telepod" following this structure.



Custom Fields

Custom Fields must be created manually.

FileWave Admin > Assistants > Custom Fields > Edit Custom Fields



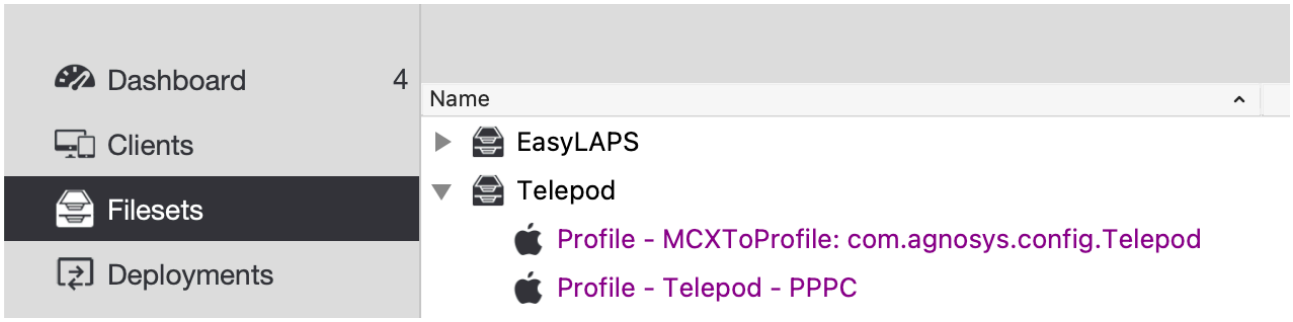
Enter the name of the Custom Field in the Name field and its internal name in the Internal Name field.

In the "Provided By" menu, select "Administrator".

Tick the option "Assigned to all devices" then click on "Save".

Custom configuration profile

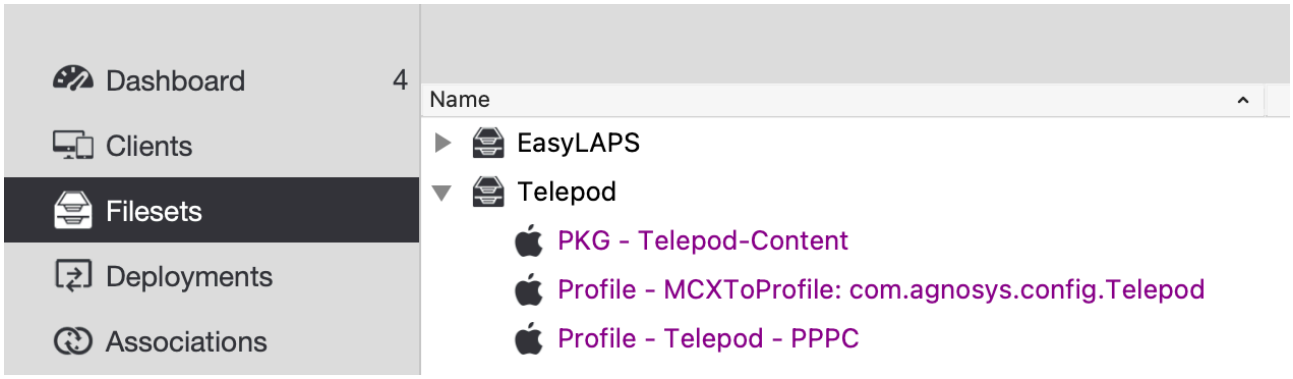
The Custom configuration profile is provisioned with the following steps :
- Filesets > New Fileset Group > Name : Telepod
- Select the Fileset Group "Telepod"
- Click on "New Desktop Fileset" then click on "Profile"
- In the Profile Editor, click on "Load Profile"
- Select the file : com.agnosys.config.config_1.Telepod.mobileconfig > Open
- Back to the Profile Editor, click on "Save".



The Custom configuration profile is linked to the "Telepod" Fileset Group, as the expected PPPC configuration profile.

Telepod-Content package

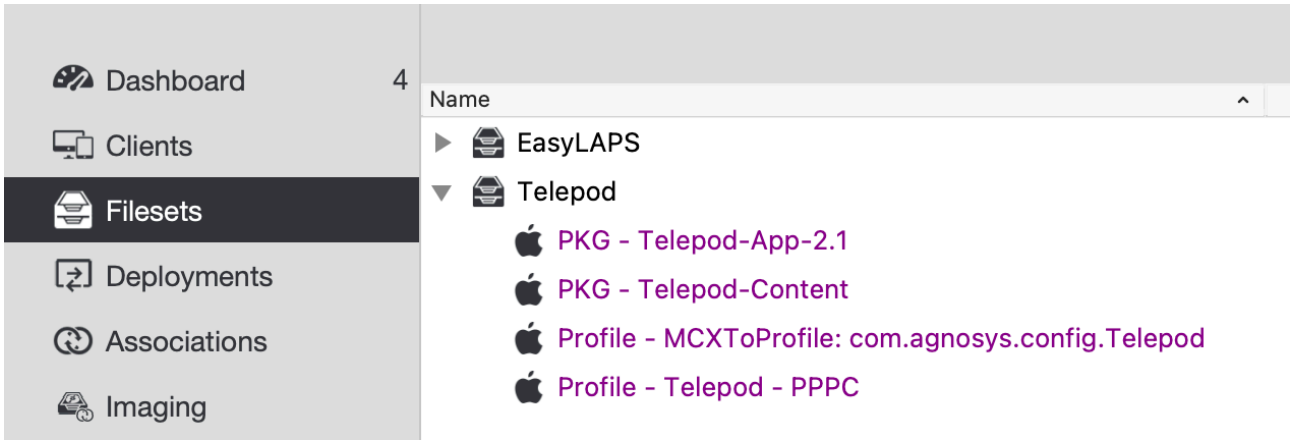
The Telepod-Content package is defined with the following steps :
- Filesets > Telepod
- Click on "New Desktop Fileset" then click on "MSI / PKG"
- Select the file : Telepod-Content.pkg > Open.



The Telepod-Content package is linked to the "Telepod" Fileset Group.

Telepod-App package

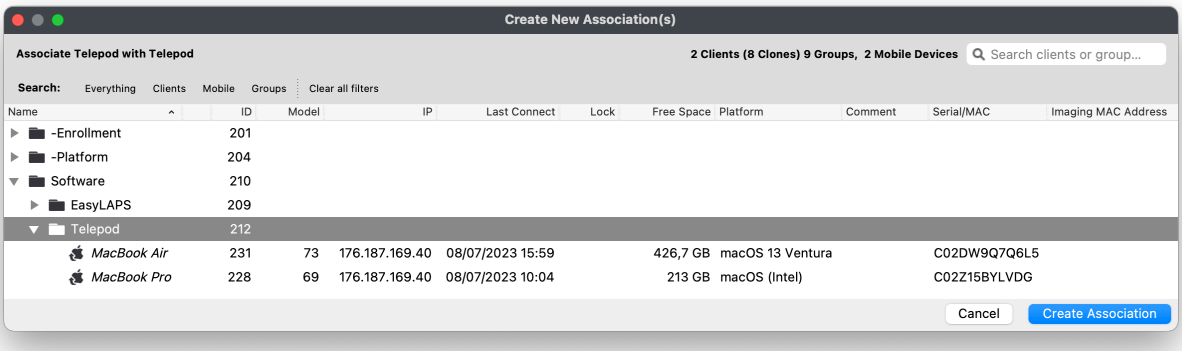
The Telepod-App package is defined with the following steps :
- Filesets > Telepod
- Click on "New Desktop Fileset" then click on "MSI / PKG"
- Select the file : Telepod-App.pkg > Open.



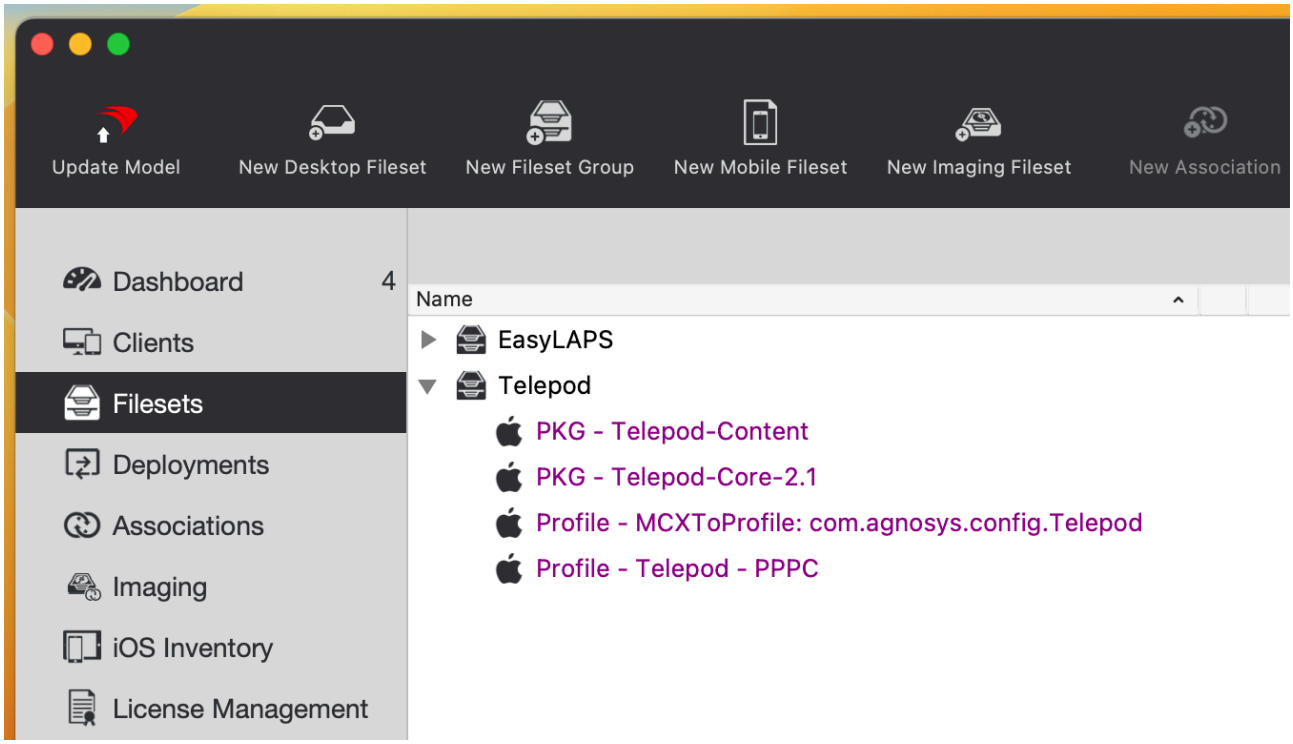
The Telepod-App package is linked to the "Telepod" Fileset Group.

Deployment on the Telepod group

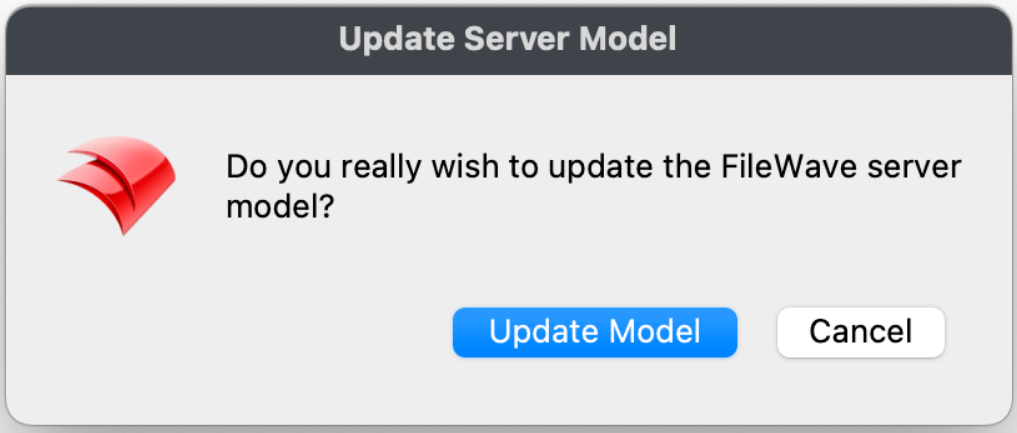
The Telepod Fileset is associated to the Telepod group with the following steps :
- Filesets > Telepod
- In the toolbar, click on "New Association".



Select the Telepod group and click on "Create Association".



In the toolbar, click on "Update Model".



Click on "Update Model".

Telepod execution

Open /Applications/Telepod.app.

Enter the credentials of a user with administrative privileges.

The Telepod assistant opens automatically a few seconds later.

Provisioning Hexnode UEM

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

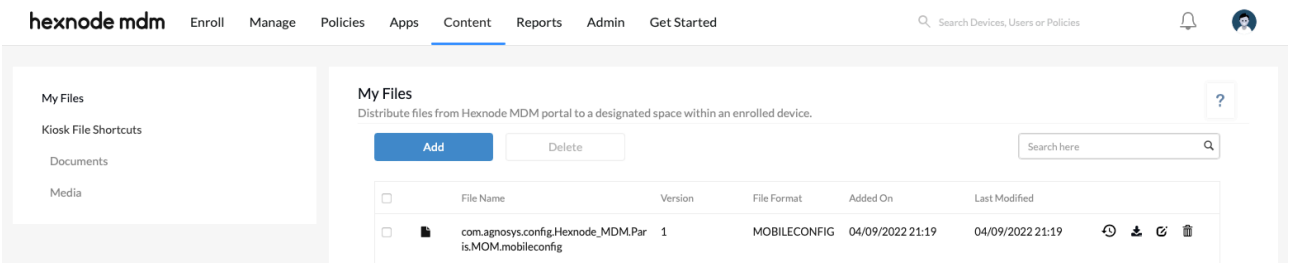
This section outlines the key points for the provisioning of these three components in Hexnode UEM. Please refer to Hexnode UEM documentation for details not specific to Telepod.

General configuration

In this example, the Mac is part of a device group named "Telepod".

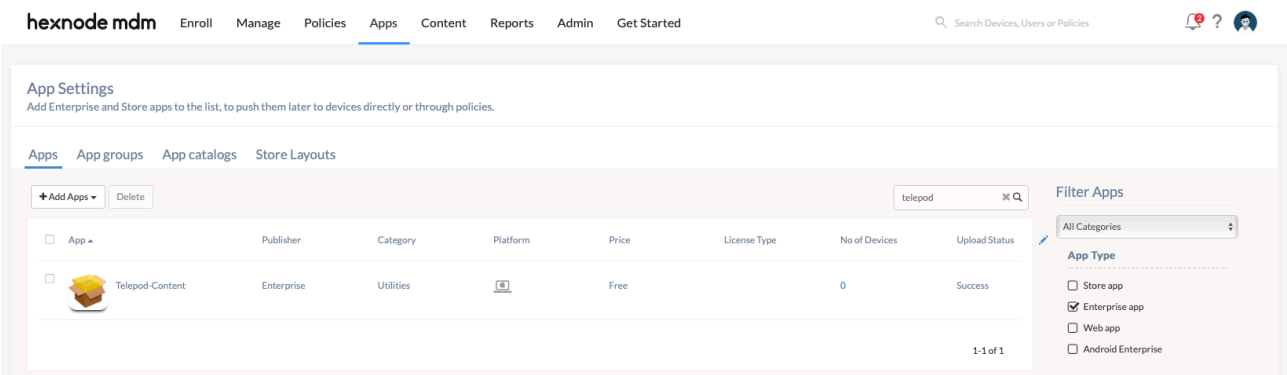
Custom configuration profile

The Custom configuration profile is uploaded with the following steps :
- Content > Add
- Select the file : com.agnosys.config.config_1.Telepod.mobileconfig > Upload
- Save



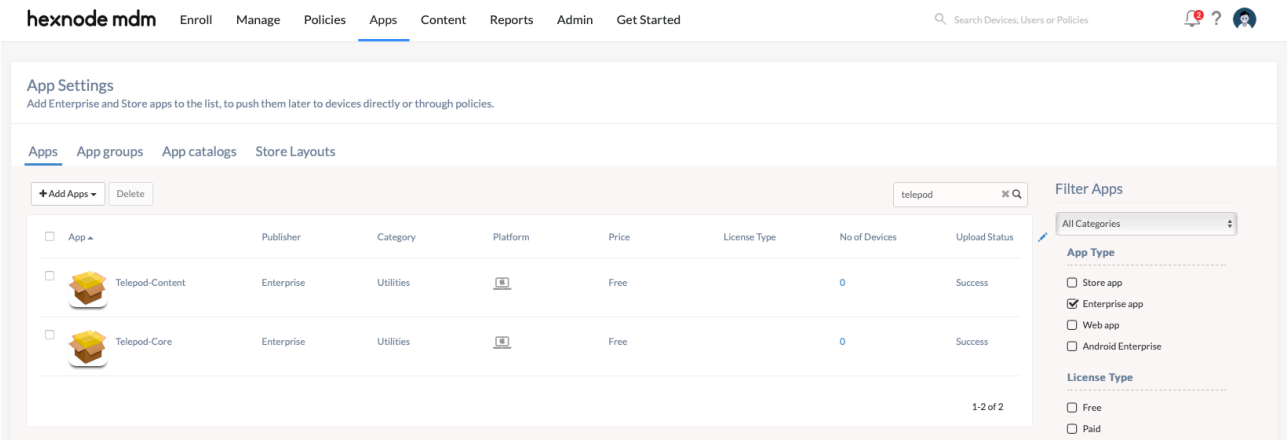
Telepod-Content package

The Telepod-Content package is uploaded with the following steps :
- Apps > Apps > Add Apps > Enterprise App
- Select the Platform "macOS" (laptop with Apple logo)
- App Name : Telepod-Content
- Upload with : PKG/MPKG/DMG File
- Category : Utilities
- Description : Telepod-Content
- Choose the PKG/MPKG/DMG File > Choose File > Telepod-Content.pkg > Upload
- Add



Telepod-Core package

The Telepod-Core package is uploaded with the following steps :
- Apps > Apps > Add Apps > Enterprise App
- Select the Platform "macOS" (laptop with Apple logo)
- App Name : Telepod-Core
- Upload with : PKG/MPKG/DMG File
- Category : Utilities
- Description : Telepod-Core
- Choose the PKG/MPKG/DMG File > Choose File > Telepod-Core.pkg > Upload
- Add



Create an App catalog with the following steps :
- Apps > App catalogs > New :
    - Name : Telepod
    - Apps > Add Apps
    - Select "Telepod-Core"
    - Click "OK"
    - Click "Save Catalog"

Provisioning policies configuration

The three components are provisioned via two policies.

Create the policy for the Custom configuration profile and the Telepod-Content package with the following steps :
- Policies > New Policy > New Blank Policy
- Policy Name : Telepod Resources
- Click on the "macOS" tab
    - Configurations > Deploy Custom Configuration
        - Configure
        - Choose File
        - Select "com.agnosys.config.config_1.Telepod.mobileconfig"
        - Click "OK"
    - App Management > Mandatory Apps
        - Configure
        - Add > Add App
        - Select "Telepod-Content" (only)
        - Click "Done"
- Click on the "Policy Targets" tab
        - Device Groups > Add Device Groups
        - Select "Telepod"
        - Click "OK"
- Click "Save"
- In the "Associate Policy" message, click on "Yes"

The first policy is validated.

Create the policy for the Telepod-Core package with the following steps :
- Policies > New Policy > New Blank Policy
- Policy Name : Telepod Execution
- Click on the "macOS" tab
    - App Management > App Catalog
        - Configure
        - Add Catalogs
        - Select "Telepod"
        - Click "Done"
- Click on the "Policy Targets" tab
        - Device Groups > Add Device Groups
        - Select "Telepod"
        - Click "OK"
- Click "Save"
- In the "Associate Policy" message, click on "Yes"

The second policy is validated.

Telepod execution

Open the Hexnode MDM app.

Click on "App Catalog".

Click on "Telepod-Core" then on "Get".

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning Jamf Now

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in Jamf Now. Please refer to Jamf Now documentation for details not specific to Telepod.

General configuration

In this example, the Mac is assigned to the "Paris" Blueprint.

Custom configuration profile

In "Paris" Blueprint, the Custom configuration profile is provisioned with the following steps :
- Manage > Blueprints > Paris
- Custom Profiles > Add a Custom Profile
- Select the file : com.agnosys.config.config_1.Telepod.mobileconfig > Add Custom Profile

Telepod-Content package

In "Paris" Blueprint, the Telepod-Content package is provisioned with the following steps :
- Manage > Apps > Add an App > Upload Your App
- Select the file : Telepod-Content.pkg
- App Name : Telepod-Content > Done
- Manage > Blueprints > Paris
- Apps > Edit Apps > "Telepod-Content" > check "Install Automatically"
- Save Changes

Telepod-Core package

In "Paris" Blueprint, the Telepod-Core package is provisioned with the following steps :
- Manage > Apps > Add an App > Upload Your App
- Select the file : Telepod-Core.pkg
- App Name : Telepod-Core > Done
- Manage > Blueprints > Paris
- Apps > Edit Apps > "Telepod-Core" > check "Display in Self Service"
- Save Changes

Telepod execution

Open the Jamf Now Self Service.

Click on "Install" (or "Reinstall") under the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning Jamf Pro

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in Jamf Pro. Please refer to Jamf Pro documentation for details not specific to Telepod.

General configuration

In this example, the Mac is part of a computer group named "Telepod".

Custom configuration profile : importing a .plist file

Follow these instructions if you want to upload in Jamf Pro a Telepod configuration file (.plist file) via a Configuration profile that includes an "Application & Custom Settings" payload.

The Custom configuration profile is provisioned with the following steps :
- Computers > Content Management > Configuration Profiles > New
- General
    - Name : a name of your choice (e.g. Telepod-Custom configuration profile)
    - Level : Computer Level
    - Distribution Method : Install Automatically
- Application & Custom Settings > Upload > Add
    - Preference Domain : com.agnosys.config.Telepod
    - Upload > config_1.plist
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Telepod > Add
- Save

Custom configuration profile : importing a .mobileconfig file

Follow these instructions if you want to upload in Jamf Pro a pre-built Custom configuration profile (.mobileconfig file) generated by a Telepod configuration file to Custom configuration profile conversion.

The Custom configuration profile is provisioned with the following steps :
- Computers > Content Management > Configuration Profiles > Upload
- Choose File : com.agnosys.config.config_1.Telepod.mobileconfig
- General
    - Name : a name of your choice (e.g. Telepod-Custom configuration profile)
    - Level : Computer Level
    - Distribution Method : Install Automatically
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Telepod > Add
- Save

Please note that the "Upload" button to use is the one positioned to the right of the "New" button in the upper right corner of the Configuration Profiles window and not the "Upload" button available inside an "Application & Custom Settings" payload.

Telepod-Content package

The Telepod-Content package is defined with the following steps :
- Settings > Computer Management > Packages > New
- General
    - Display Name : Telepod-Content
    - Filename > browse for a file : Telepod-Content.pkg
- Save

The Telepod-Content package is provisioned with the following steps :
- Computers > Policies > New
- Options
    - General
        - Display Name : Telepod-Content Install
        - Trigger : Recurring Check-in — Execution Frequency : Once per computer
    - Packages
        - Configure > Telepod-Content.pkg > Add
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Telepod > Add
- Save

Telepod-Core package

The Telepod-Core package is defined with the following steps :
- Settings > Computer Management > Packages > New
- General
    - Display Name : Telepod-Core
    - Filename > browse for a file : Telepod-Core.pkg
- Save

The Telepod-Core package is provisioned with the following steps :
- Computers > Policies > New
- Options
    - General
        - Display Name : Telepod-Core Install
        - Trigger : *none* — Execution Frequency : Ongoing
    - Packages
        - Configure > Telepod-Core.pkg > Add
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Telepod > Add
- Self Service
    - Make the policy available in Self Service
    - Self Service Display Name : Telepod
    - Button Name Before Initiation : Execute
    - Button Name After Initiation : Execute
    - Icon : you can use the "telepod-icon.png" file provided in the Telepod Toolkit
- Save

Telepod execution

Open the Jamf Pro Self Service.

Click on "Execute" under the "Telepod" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Telepod emergency stop

An emergency stop can be created with the following steps :
- Computers > Policies > New
- Options
    - General
        - Display Name : Telepod-Stop
        - Trigger : *none* — Execution Frequency : Ongoing
    - Files and Processes
        - Execute Command

```
launchctl bootout system/com.agnosys.telepod_supervisor ; launchctl bootout system/com.agnosys.telepod
```

Note : The string is a single-line string with no line breaks.

- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Telepod > Add

- Self Service
    - Make the policy available in Self Service
    - Self Service Display Name : Telepod
    - Button Name Before Initiation : Stop
    - Button Name After Initiation : Stop
    - Icon : you can use the "telepod-icon-stop.png" file provided in the Telepod Toolkit
- Save

Provisioning Jamf School

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-App package (administrative privileges required to run the embedded app).

This section outlines the key points for the provisioning of these three components in Jamf School. Please refer to Jamf School documentation for details not specific to Telepod.

General configuration

In this example, the Mac is part of a device group named "Telepod" in "Paris" location.

Custom configuration profile

In "Paris" location, the Custom configuration profile is provisioned with the following steps :
- Profiles > Overview > Create Profile
- Upload Custom Profile
- Profile file (.mobileconfig) : com.agnosys.config.config_1.Telepod.mobileconfig
- Profile name : Telepod-Custom configuration profile
- This profile will be distributed to the following device groups > + > Telepod
- By default, "Automatic installation" is selected for this scope.
- Save

Telepod-Content package

In "Paris" location, the Telepod-Content package is provisioned with the following steps :
- Apps > Inventory > Add App > Add In-House macOS Package
- Select "Telepod-Content.pkg"
- This app will be distributed to the following device groups > + > Telepod
- By default, "Automatic installation" is selected for this scope.
- Save

Telepod-App package

In "Paris" location, the Telepod-App package is provisioned with the following steps :
- Apps > Inventory > Add App > Add In-House macOS Package
- Select "Telepod-App.pkg"
- This app will be distributed to the following device groups > + > Telepod
- By default, "Automatic installation" is selected for this scope.
- Save

Telepod execution

Open /Applications/Telepod.app.

Enter the credentials of a user with administrative privileges.

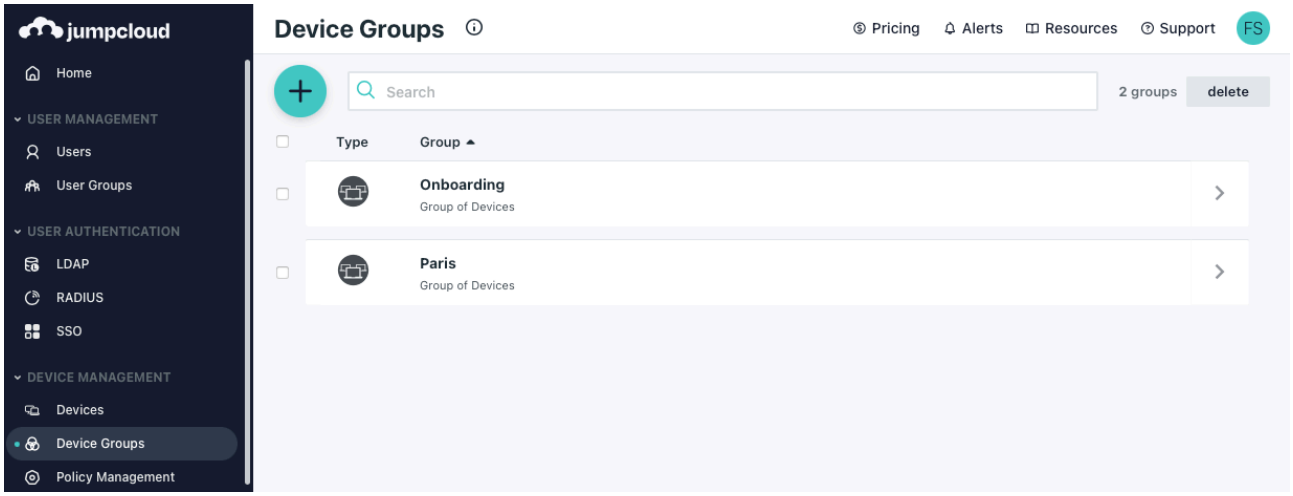
The Telepod assistant opens automatically a few seconds later.

Provisioning JumpCloud

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-App package (administrative privileges required to run the embedded app).

This section outlines the key points for the provisioning of these three components in JumpCloud. Please refer to JumpCloud documentation for details not specific to Telepod.

General configuration



Go to Device management > Device Groups and identify or create a device group (e.g. "Paris") that encompasses the devices that are to be installed with Telepod.

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Device Management > Policy Management
- "+" button > Mac > MDM Custom Configuration Profile > configure
- Select the "Details" tab :
    - Policy Name : Telepod-Custom configuration profile
    - Settings > upload file : com.agnosys.config.config_1.Telepod.mobileconfig
- Select the "Device Groups" tab then select the "Paris" device group
- Save

Telepod-Content package

The Telepod-Content package is provisioned with the following steps :
- Device Management > Software Management
- Apple > "+" button > JumpCloud Private Repo
- From the "Details" tab :
    - Application Name : Telepod-Content
    - Choose A File > Telepod-Content.pkg > Upload
- Select the "Device Groups" tab then select the "Paris" device group
- Save & Install > Tick "I understand this can't be undone." > Install

If you need to update the package, delete the configuration and start it over.

Telepod-App package

The Telepod-App package is provisioned with the following steps :
- Device Management > Software Management
- Apple > "+" button > JumpCloud Private Repo
- From the "Details" tab :
    - Application Name : Telepod-App
    - Choose A File > Telepod-App.pkg > Upload
- Select the "Device Groups" tab then select the "Paris" device group
- Save & Install > Tick "I understand this can't be undone." > Install

If you need to update the package, delete the configuration and start it over.

Telepod execution

Open /Applications/Telepod.app.

Enter the credentials of a user with administrative privileges.

The Telepod assistant opens automatically a few seconds later.

Provisioning Kandji

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in Kandji. Please refer to Kandji documentation for details not specific to Telepod.

General configuration

In this example, the Mac is assigned to the "Telepod" Blueprint.

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Library > Add new > General > Custom Profile > Add & Configure
- Title : Telepod-Custom configuration profile
- Assignment :
    - Blueprint : Telepod
    - Install on : Mac
- Settings :
    - Profile > click to upload
    - Select the file : com.agnosys.config.config_1.Telepod.mobileconfig
- Save

Telepod-Content package

The Telepod-Content package is provisioned with the following steps :
- Library > Add new > General > Custom Apps > Add & Configure
- Title : Telepod-Content
- Assignment :
    - Blueprint : Telepod
- Settings :
    - Installation : Install once per device
    - Install Details
        - Installer Package
        - Installer Package > click to upload
        - Select the file : Telepod-Content.pkg
- Save

Telepod-Core package

The Telepod-Core package is provisioned with the following steps :
- Library > Add new > General > Custom Apps > Add & Configure
- Title : Telepod-Core
- Assignment :
    - Blueprint : Telepod
- Settings :
    - Installation : Install on-demand from Self Service
    - Self Service > Category > Utilities
    - Install Details
        - Installer Package
        - Installer Package > click to upload
        - Select the file : Telepod-Core.pkg
- Save

Telepod execution

Open the Kandji Self Service.

Click on "Install" (or "Reinstall") under the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning Meraki Systems Manager

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in Meraki Systems Manager. Please refer to Meraki Systems Manager documentation for details not specific to Telepod.

General configuration

In this example, the Mac is part of the "Paris" network and associated to the "telepod" tag.

The required macOS Agent is deployed with the following steps :
- Systems Manager > Configure > General
- Agent Version > Preferred agent version > Latest
- Save
- Systems Manager > Manage > Apps
- Add app > macOS > SM agent
- Scope > Manual > All devices
- Save Changes

The Self Service Portal is enabled with the following steps :
- Systems Manager > Configure > General
- Self Service Portal settings > Self Service Portal : Enable SSP for this network
- Portal link : Self Service Portal URL
- Save Changes

Check that the Mac is associated to the correct owner and that this owner has a password and is allowed to access the Self Service Portal.

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Systems Manager > Manage > Settings
- Add profile > Upload custom Apple profile
- Profile Configuration > Upload a .mobileconfig file
- Choose File > com.agnosys.config.config_1.Telepod.mobileconfig
- Deploy channel : Device
- Scope > Manual > with ANY of the followings tags
- Device tags : telepod
- Save

Telepod-Content package

The Telepod-Content package is provisioned with the following steps :
- Systems Manager > Manage > Apps
- Add app > macOS > Custom app
- Name : Telepod-Content
- Identifier : com.agnosys.pkg.Telepod-Content
- Vendor : Agnosys
- Type : Upload to the Meraki cloud
- Select the file : Telepod-Content.pkg
- Auto-install : **enabled**
- Visible in SSP : **disabled**
- Scope > Manual > with ANY of the followings tags
- Device tags : telepod
- Save

Telepod-Core package

The Telepod-Core package is provisioned with the following steps :
- Systems Manager > Manage > Apps
- Add app > macOS > Custom app
- Name : Telepod-Core
- Identifier : com.agnosys.pkg.Telepod-Core
- Vendor : Agnosys
- Type : Upload to the Meraki cloud
- Select the file : Telepod-Core.pkg
- Auto-install : **disabled**
- Visible in SSP : **enabled**
- Scope > Manual > with ANY of the followings tags
- Device tags : telepod
- Save

Telepod execution

Open the Self Service Portal (see Self Service Portal URL above).

Click on "Install" under the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning Microsoft Intune

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-App package (administrative privileges required to run the embedded app).

This section outlines the key points for the provisioning of these three components in Microsoft Intune. Please refer to Microsoft Intune documentation for details not specific to Telepod.

The packages must be provisioned as macOS apps. More informations about this new type of provisioning are available at https://learn.microsoft.com/en-us/mem/intune/apps/macos-unmanaged-pkg

General configuration

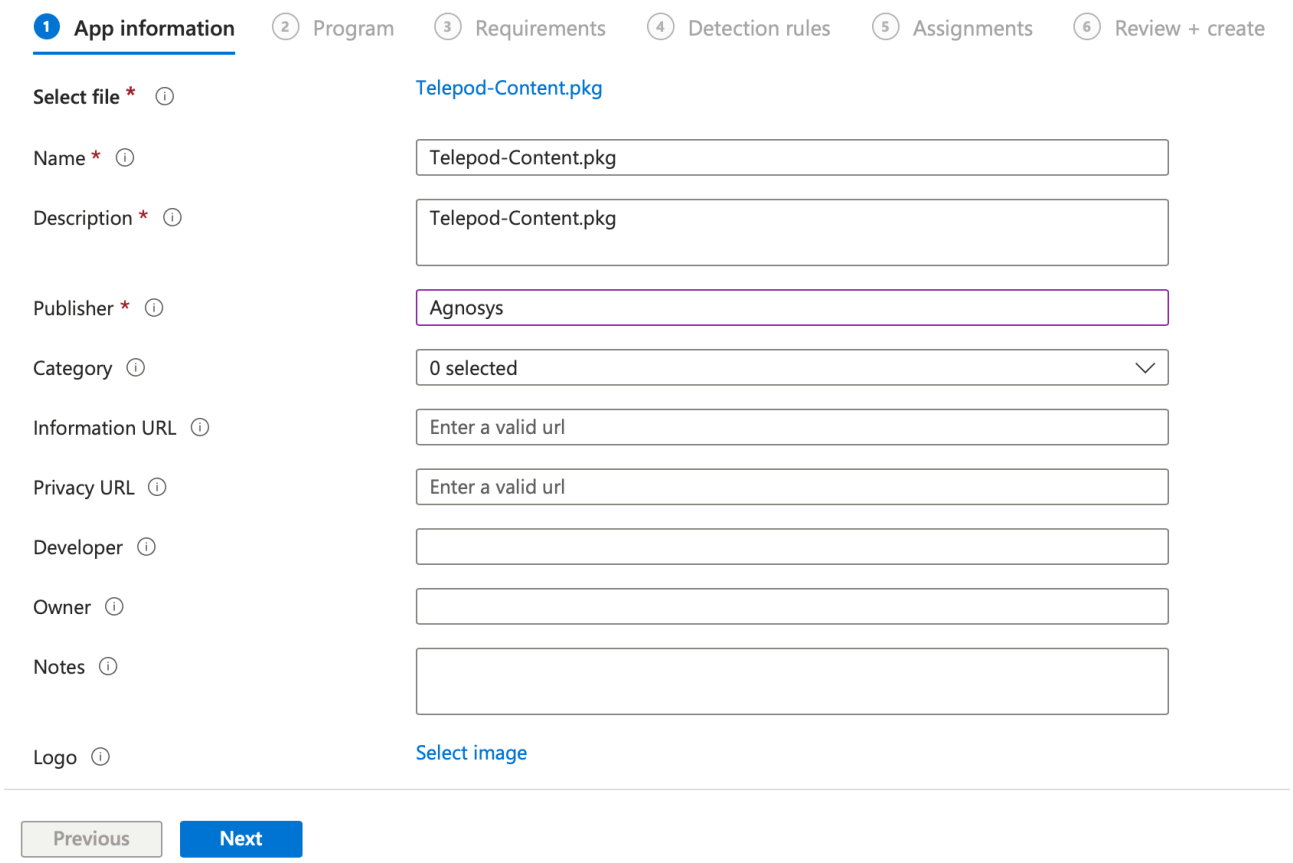
The scope of the components installation is here all devices.

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Devices > macOS > Configuration > Create > New Policy
- Profile type : Templates
- Select "Custom" > Create
- Basics
    - Name : Telepod-Custom configuration profile
- Configuration settings
    - Custom configuration profile name : Telepod-Custom configuration profile
    - Deployment channel : Device channel
    - Select a configuration profile file :
    com.agnosys.config.config_1.Telepod.mobileconfig
- Assignments
    - Included groups : Add all devices
- Review + create
    - Create

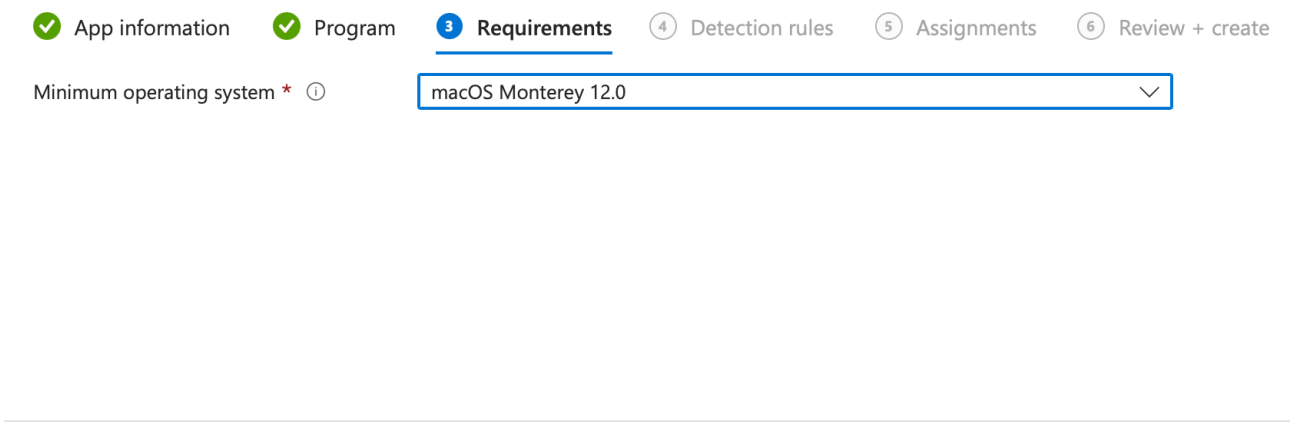
Telepod-Content package

The Telepod-Content package is provisioned with the following steps :
- Apps > macOS > Add
- App type : macOS app (PKG) > Select

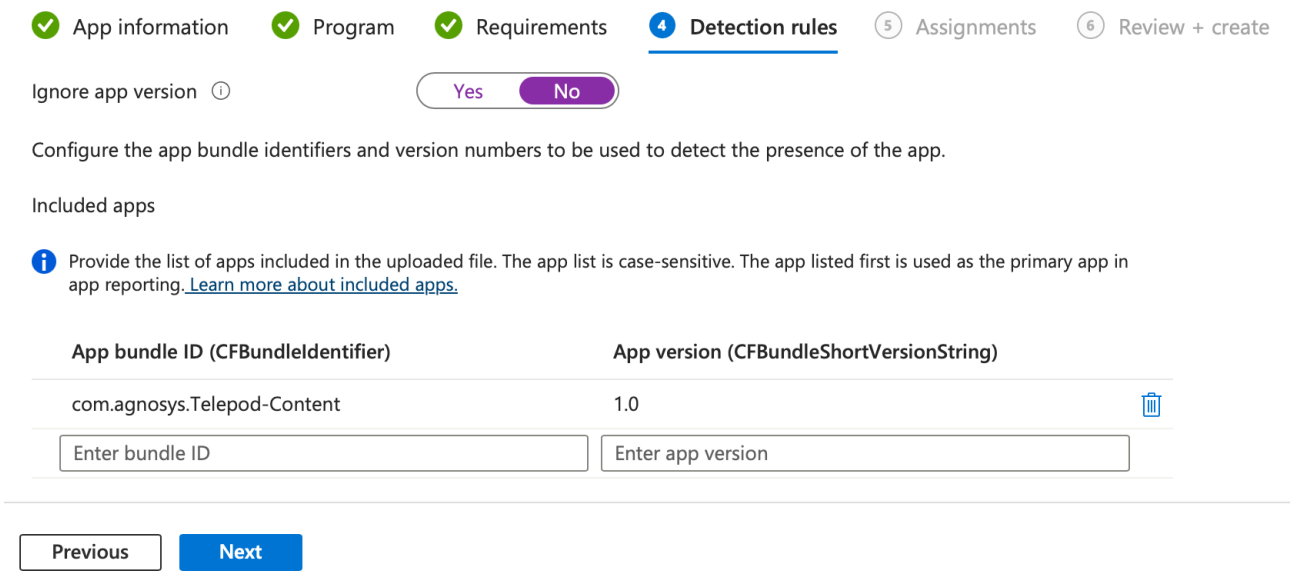


- App information
    - Select file > Select app package file
    - App package file > Select a file > Telepod-Content.pkg > OK
    - Publisher : Agnosys

- Program : no scripts need to be configured



- Requirements
    - Minimum operating system : macOS Monterey 12.0



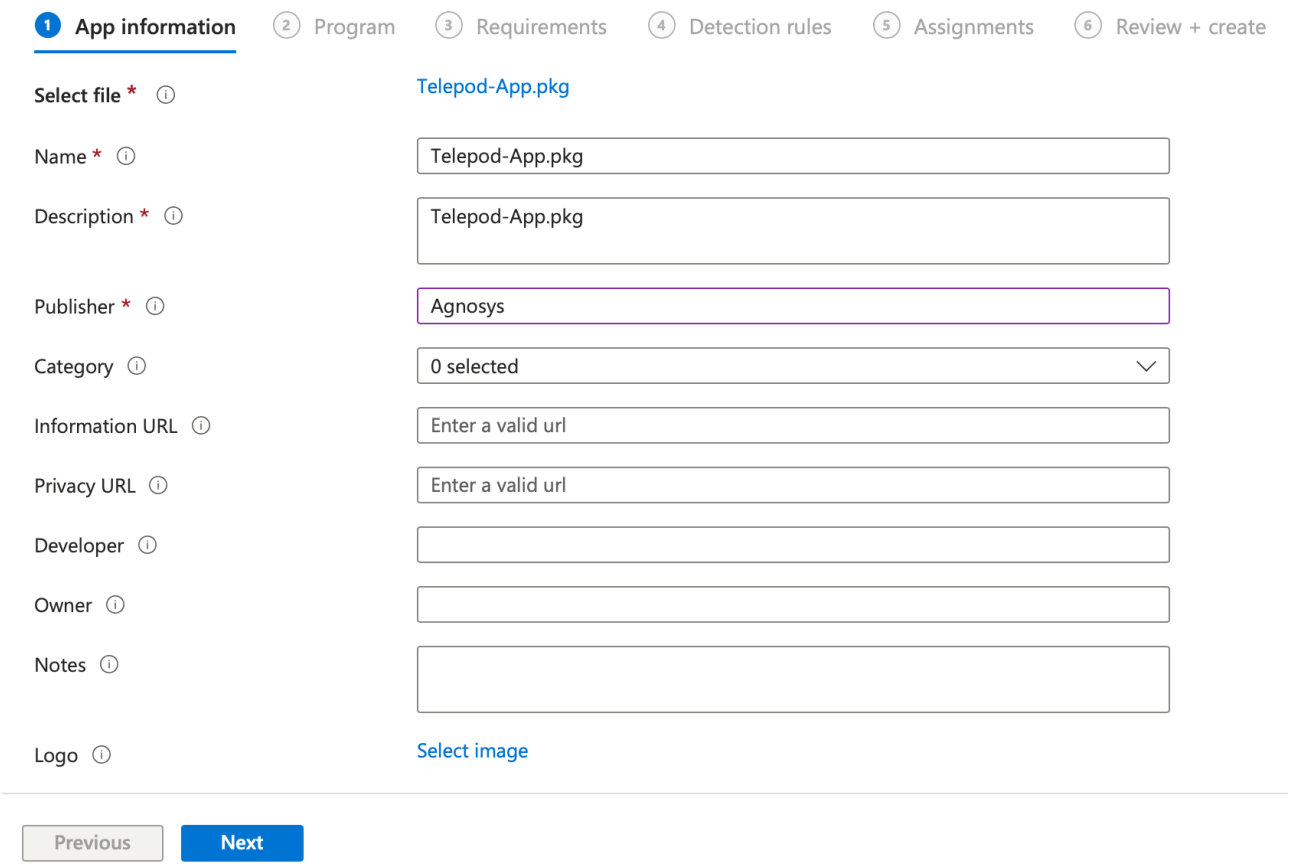
- Detection rules
    - Ignore app version : **No**
    - Detection method table :
        - App bundle ID : **com.agnosys.Telepod-Content**
          Warning : Keep only this App bundle ID if others have been automatically added.
        - Build number : keep current value (e.g. 1.0)

- Assignments
    - **Required** : Add all devices

- Review + create
    - Create

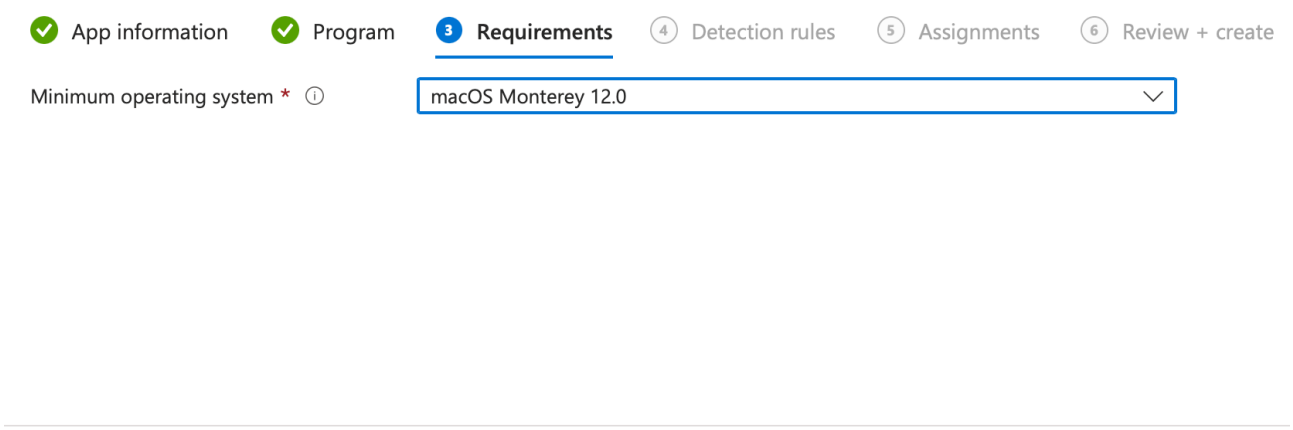
Telepod-App package

The Telepod-App package is provisioned with the following steps :
- Apps > macOS > Add
- App type : macOS app (PKG) > Select

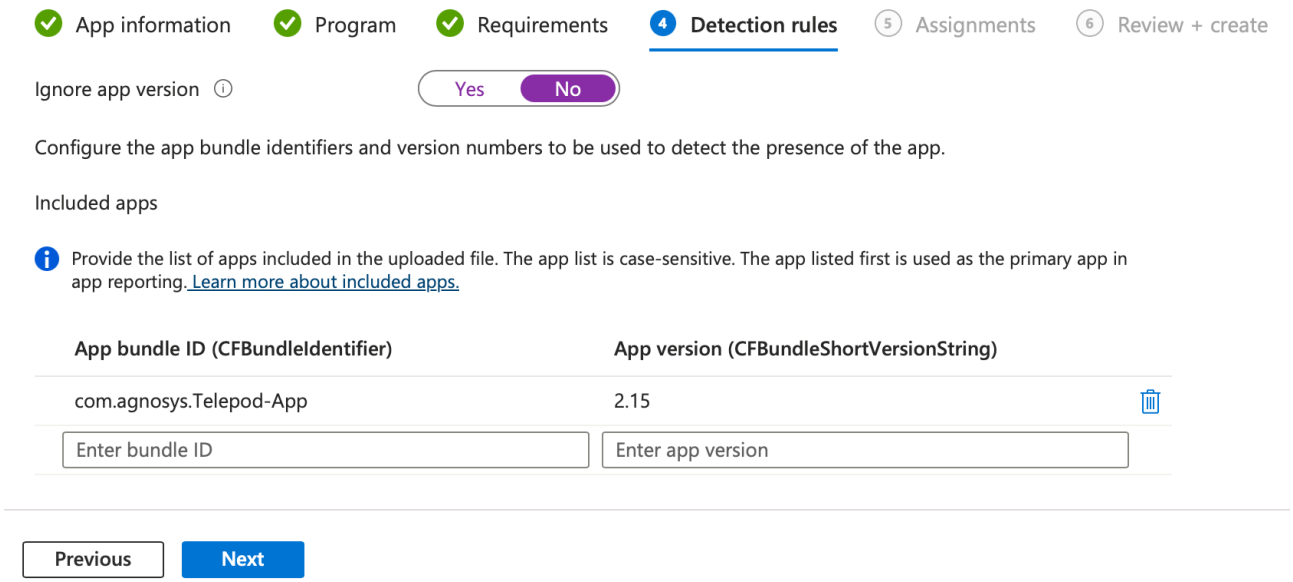


- App information
    - Select file > Select app package file
    - App package file > Select a file > Telepod-App.pkg > OK
    - Publisher : Agnosys

- Program : no scripts need to be configured



- Requirements
    - Minimum operating system : macOS Monterey 12.0



- Detection rules
    - Ignore app version : **No**
    - Detection method table :
        - App bundle ID : **com.agnosys.Telepod-App**
        - App version : keep current value (e.g. 2.15)

- Assignments
    - Required : Add all devices

- Review + create
    - Create

Telepod execution

Open /Applications/Telepod.app.

Enter the credentials of a user with administrative privileges.

The Telepod assistant opens automatically a few seconds later.

Provisioning Miradore

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-App package (administrative privileges required to run the embedded app).

This section outlines the key points for the provisioning of these three components in Miradore. Please refer to Miradore documentation for details not specific to Telepod.

General configuration

The scope of the components installation is here all devices.

Custom configuration profile

The Custom configuration profile is defined with the following steps :
- Management > Configuration profiles > Add
- macOS > Advanced (custom)
- Browse > com.agnosys.config.config_1.Telepod.mobileconfig
- Name : Telepod-Custom configuration profile > Create

Telepod-Content package

The Telepod-Content package is defined with the following steps :
- Management > Applications > Applications tab > Add
- macOS application > PKG (Uploaded)
- File > Select file > Telepod-Content.pkg
- Application name : Telepod-Content
- Bundle identifier : com.agnosys.Telepod-Content
- Version : 1.0
- Create

Telepod-App package

The Telepod-App package is defined with the following steps :
- Management > Applications > Applications tab > Add
- macOS application > PKG (Uploaded)
- File > Select file > Telepod-App.pkg
- Application name : Telepod-App
- Bundle identifier : com.agnosys.Telepod-App
- Version : the version imported (e.g. 1.12)
- Create

Provisioning policy configuration

The three components can be provisioned via a unique Business policy with the following steps :
- Management > Business policies > Add
- Apply to all devices
- Name : Telepod
- Double-click on the Business policy
- Add > Application > Check Telepod-App and Telepod-Content > Add
- Add > Configuration profile > Check Telepod-Custom configuration profile > Add
- Click on the Items tab and check the Business policy content
- Click on "Enable"

Telepod execution

Open /Applications/Telepod.app.

Enter the credentials of a user with administrative privileges.

The Telepod assistant opens automatically a few seconds later.

Provisioning Mosyle Business

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in Mosyle Business. Please refer to Mosyle Business documentation for details not specific to Telepod.

General configuration

In this example, the devices are part of a device group named "Paris".

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Management > macOS
- Management Profiles > Certificates / Custom Profiles > Add new profile
- Profile Name : Telepod-Custom configuration profile
- Select the file > com.agnosys.config.config_1.Telepod.mobileconfig
- Profile Assignment > Add Assignment > Device Enrollment > Devices from specific Device Groups > Paris > Tick
- Save

Telepod-Content package

Mosyle FUSE offers to host packages in Mosyle's CDN. With Mosyle Business Premium, the Telepod-Content package must be hosted on your own Web server.

The Telepod-Content package is defined with the following steps :
- Management > macOS
- Management Profiles > Install PKG > PKGs > Add new package
- Click on "Already have a .pkg"
- Select "A) Automatically set App info" then click on "Next"
- Mosyle FUSE :
    - Click on "Upload or Select File from CDN"
    - Upload > Choose a file > Telepod-Content.pkg
    - Public URL : the public URL is automatically defined
    - Click on "Add enterprise app"
- Mosyle Business Premium :
    - Public URL : enter the public URL to the package
    - Click on "Add enterprise app"
- **Only** if the Telepod-Content package is **signed** :
    - Management Profiles > Install PKG > PKGs > Telepod-Content
    - Enable "This app is Signed"
    - Save

The Telepod-Content package is provisioned with the following steps :
- Management > macOS
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : Telepod-Content
- Add application > Enterprise Apps > Telepod-Content > Tick
- **Only** if the Telepod-Content package is **signed** : enable "Install with Apple Protocol"
- Self-Service Apps > Do not show the apps in Self-Service
- Profile Assignment > Add Assignment > Device Enrollment > Devices from specific Device Groups > Paris > Tick
- Save

Telepod-Core package

Mosyle FUSE offers to host packages in Mosyle's CDN. With Mosyle Business Premium, the Telepod-Core package must be hosted on your own Web server.

The Telepod-Core package is defined with the following steps :
- Management > macOS
- Management Profiles > Install PKG > PKGs > Add new package
- Click on "Already have a .pkg"
- Select "A) Automatically set App info" then click on "Next"
- Mosyle FUSE :
    - Click on "Upload or Select File from CDN"
    - Upload > Choose a file > Telepod-Core.pkg
    - Public URL : the public URL is automatically defined
    - Click on "Add enterprise app"
- Mosyle Business Premium :
    - Public URL : enter the public URL to the package
    - Click on "Add enterprise app"
- Management Profiles > Install PKG > PKGs > Telepod-Core
- Enable "This app is Signed"
- Save

The Telepod-Core package is provisioned with the following steps :
- Management > macOS
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : Telepod-Core
- Add application > Enterprise Apps > Telepod-Core > Tick
- Enable "Install with Apple Protocol"
- **Disable** "Install all apps after saving the profile"
- Self-Service Apps > Show the apps in Self-Service
- Profile Assignment > Add Assignment > Device Enrollment > Devices from specific Device Groups > Paris > Tick
- Save

Telepod execution

Open the Mosyle Business Self Service.

Click on "Your Apps".

Click on "Install Now" under the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning Mosyle Manager

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in Mosyle Manager. Please refer to Mosyle Manager documentation for details not specific to Telepod.

General configuration

In this example, the devices are part of a device group named "Paris".

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- macOS > Management
- Management Profiles > Certificates / Custom Profiles > Add new profile
- Profile Name : Telepod-Custom configuration profile
- Select the file > com.agnosys.config.config_1.Telepod.mobileconfig
- Profile Assignment > Select specific users or devices
- Select the users and devices > Assign to Device Groups > Select > Paris > Tick
- Save

Telepod-Content package

The Telepod-Content package is hosted on a Web server.

The Telepod-Content package is defined with the following steps :
- macOS > Management
- Management Profiles > Install PKG > PKGs > Add new package
- Click on "Already have a .pkg"
- Select "A) Automatically set App info" then click on "Next"
- Public URL : enter the public URL to the package
- Click on "Add enterprise app"
- **Only** if the Telepod-Content package is **signed** :
    - Management Profiles > Install PKG > PKGs > Telepod-Content
    - Enable "This app is Signed"
    - Save

The Telepod-Content package is provisioned with the following steps :
- macOS > Management
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : Telepod-Content
- Add application > Enterprise Apps > Telepod-Content > Tick
- **Only** if the Telepod-Content package is **signed** : enable "Install with Apple Protocol"

- Self-Service Apps > Do not show the apps in Self-Service
- Profile Assignment > Select specific users or devices
- Select the users and devices > Assign to Device Groups > Select > Paris > Tick
- Save

Telepod-Core package

The Telepod-Core package is hosted on a Web server.

The Telepod-Core package is defined with the following steps :
- macOS > Management
- Management Profiles > Install PKG > PKGs > Add new package
- Click on "Already have a .pkg"
- Select "A) Automatically set App info" then click on "Next"
- Public URL : enter the public URL to the package
- Click on "Add enterprise app"
- Management Profiles > Install PKG > PKGs > Telepod-Core
- Enable "This app is Signed"
- Save

The Telepod-Core package is provisioned with the following steps :
- macOS > Management
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : Telepod-Core
- Add application > Enterprise Apps > Telepod-Core > Tick
- Enable "Install with Apple Protocol"
- **Disable** "Install all apps after saving the profile"
- Self-Service Apps > Show the apps in Self-Service
- Profile Assignment > Select specific users or devices
- Select the users and devices > Assign to Device Groups > Select > Paris > Tick
- Save

Telepod execution

Open the Mosyle Manager Self Service.

Click on "Your Apps".

Click on "Install" under the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning SimpleMDM

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in SimpleMDM. Please refer to SimpleMDM documentation for details not specific to Telepod.

General configuration

In this example, the Mac is part of a device group named "Paris".

First enable Munki Integration to provide a Self Service with the following steps :
- Apps & Media > Munki > Info > Enable Munki Integration
- Confirm the Integration.

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Configs > Profiles > Create Profile > Custom Configuration Profile
- Name : Telepod-Custom configuration profile
- Mobileconfig > Choose File > com.agnosys.config.config_1.Telepod.mobileconfig
- Enable "For macOS devices, deploy as a device profile instead of a user profile"
- In the Scope section, check only the OS "macOS"
- Save
- Devices > Groups > Paris > Profiles > Assign Profile
- Telepod-Custom configuration profile > Assign

Telepod-Content package

The Telepod-Content package is defined with the following steps :
- Apps & Media > Catalog > Apps > Add App > Custom App
- Select the file : Telepod-Content.pkg > Done

The Telepod-Content package is provisioned with the following steps :
- Apps & Media > Assignment
- Create Assignment Group
    - Name : Telepod-Content
    - Type : Munki
    - Install type : **Managed**
    - Save
- Telepod-Content
    - Search for an app or media to add > Telepod-Content.pkg
    - Search for a group or device to add > Paris

Telepod-Core package

The Telepod-Core package is defined with the following steps :
- Apps & Media > Catalog > Apps > Add App > Custom App
- Select the file : Telepod-Core.pkg > Done
- Catalog > Telepod-Core > Munki
- Enable "Use custom Pkginfo"
- Insert inside the main dictionary the two following lines in bold :

```
<plist version="1.0">
  <dict>
    <key>OnDemand</key>
    <true/>
    [...]
```

The Telepod-Core package is provisioned with the following steps :
- Apps & Media > Assignment
- Create Assignment Group
    - Name : Telepod-Core
    - Type : Munki
    - Install type : **Self serve**
    - Save
- Telepod-Core
    - Search for an app or media to add > Telepod-Core.pkg
    - Search for a group or device to add > Paris

Telepod execution

Open the Managed Software Center.

Click on "Software".

Click on "Install" under the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Provisioning VMware Workspace ONE

Three components must be deployed on the Mac to run Telepod :
- a Custom configuration profile
- a Telepod-Content package
- the Telepod-Core package.

This section outlines the key points for the provisioning of these three components in VMware Workspace ONE. Please refer to VMware Workspace ONE documentation for details not specific to Telepod.

General configuration

The scope of the components installation is here all devices.

Custom configuration profile

Open the VMware Workspace ONE console.

Go to Resources > Profiles & Baselines > Profiles.

Click on "Add" > "Add Profile".

Select the platform "macOS" then click on "Device Profile".

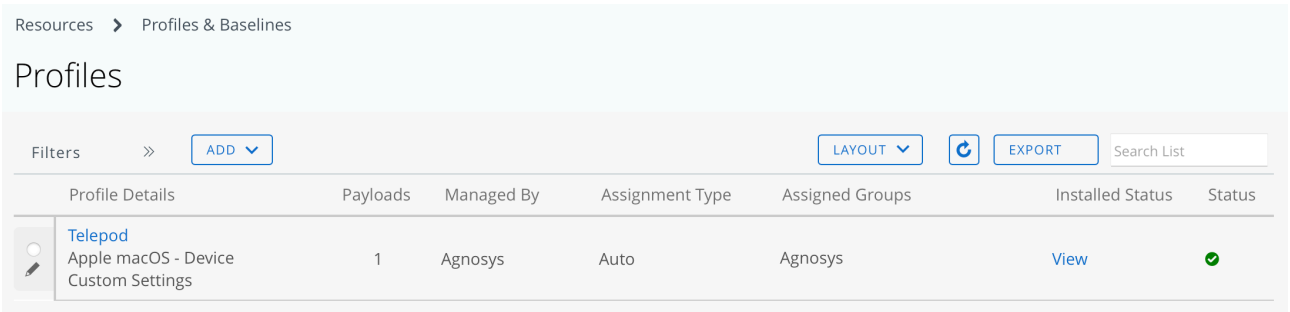
Name the configuration profile (e.g. "Telepod") and optionally add a description (e.g. "Telepod configuration").

Inside the "Custom Settings" payload, click on "Add" to reveal the XML field.

Open the Custom configuration profile (extension ".plist") with a Text Editor like Sublime Text, then copy and paste the whole content in the XML field.

Click on "Next".

In the "Assignment" section, click in the "Smart Group" field to add the Organization Group that encompasses the Mac that are to be installed with Telepod. Click on "Save and Publish".

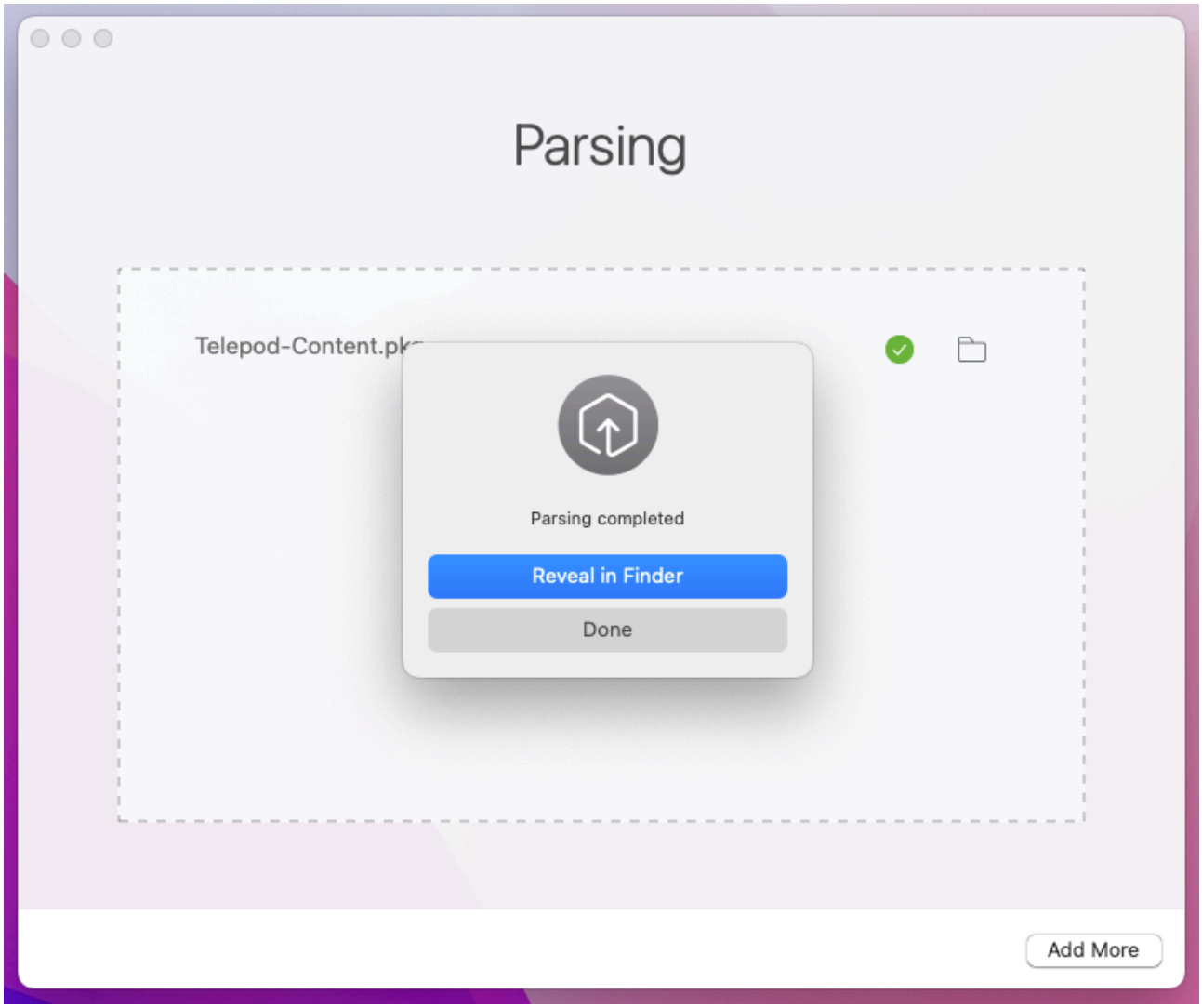


Check that the Custom configuration profile is published and assigned.

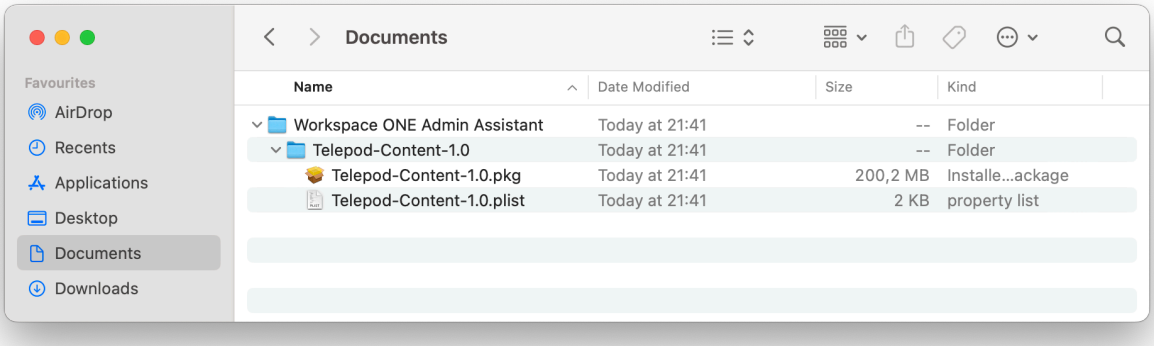
Telepod-Content package

Open /Applications/Workspace ONE Admin Assistant.

Drag and drop Telepod-Content.pkg in the main window.



Once the parsing is completed, click on "Reveal in Finder".

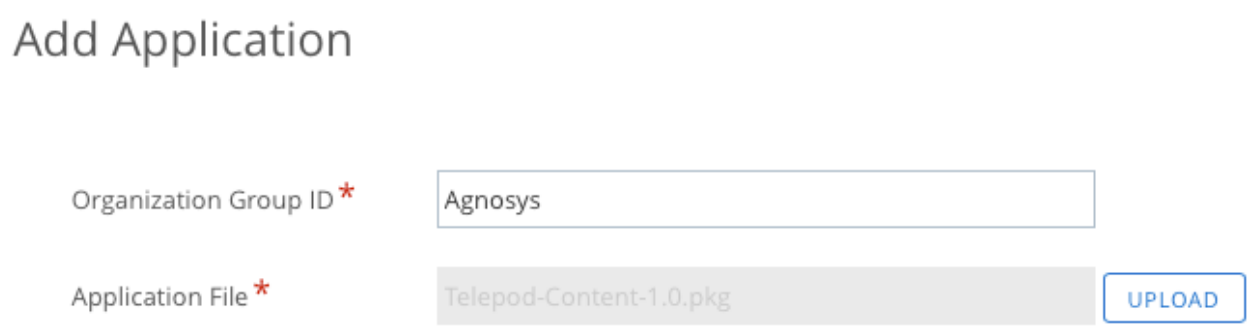


Identify the package and its associated property list file that are both going to be uploaded.

Open the VMware Workspace ONE console.

Go to Resources > Apps > Native.

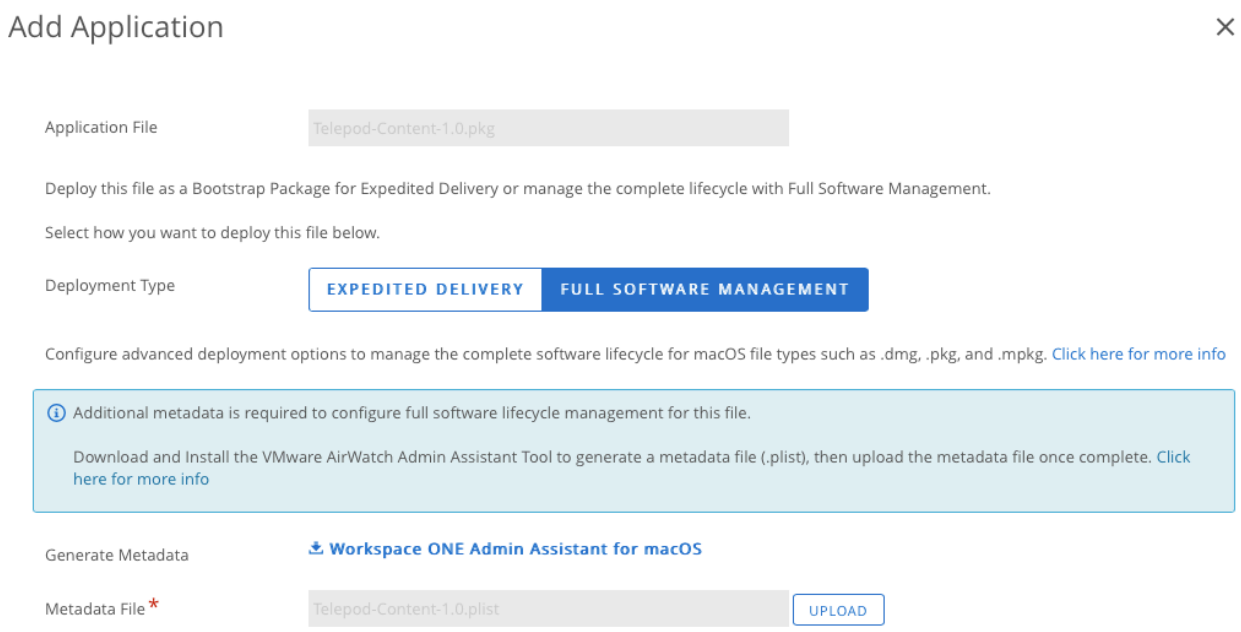
Click on "Add" > "Application File".



Select the Organization Group that encompasses the devices that must run Telepod.

Click on "Upload" and upload Telepod-Content.pkg (Type : Local File).

Click on "Continue".

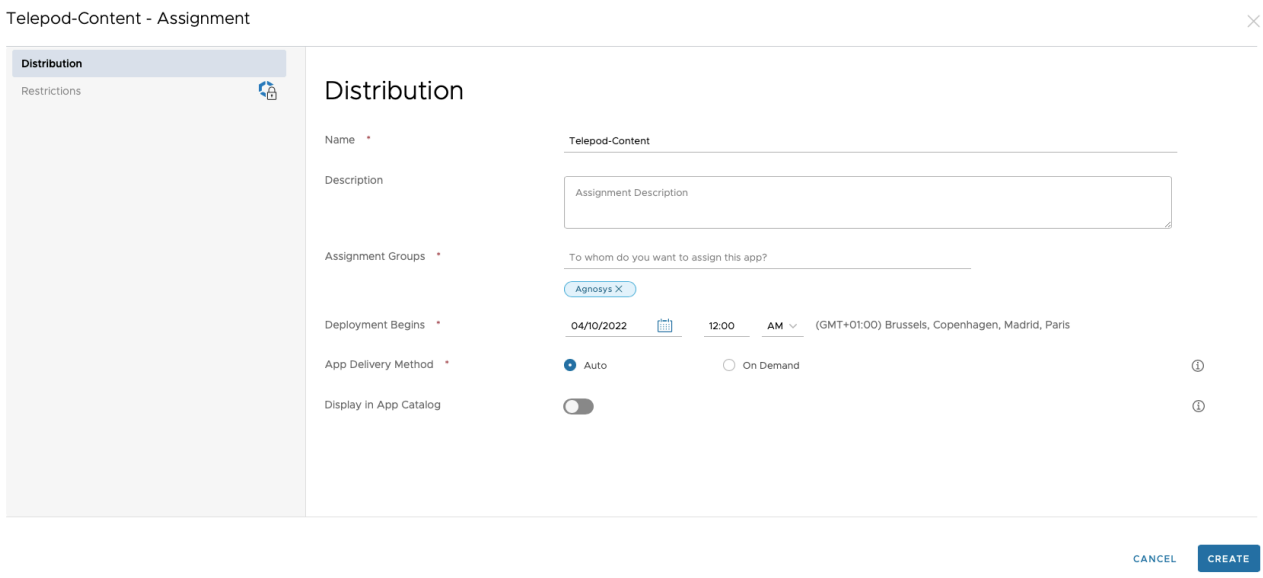


Select "Full Software Management".

Click on "Upload" and upload the associated property list file.

Click on "Continue".

In the Settings pane, click on "Save & Assign".



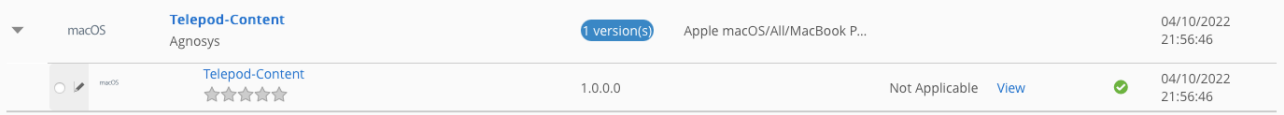
Complete the assignment form :
- Name : Telepod-Content
- Assignment Groups : select the Organization Group that encompasses the devices that must run Telepod
- App Delivery Method : **Auto**

- Display in App Catalog : **disabled**.

Click on "Create".

In the Assignment pane, click on "Save".

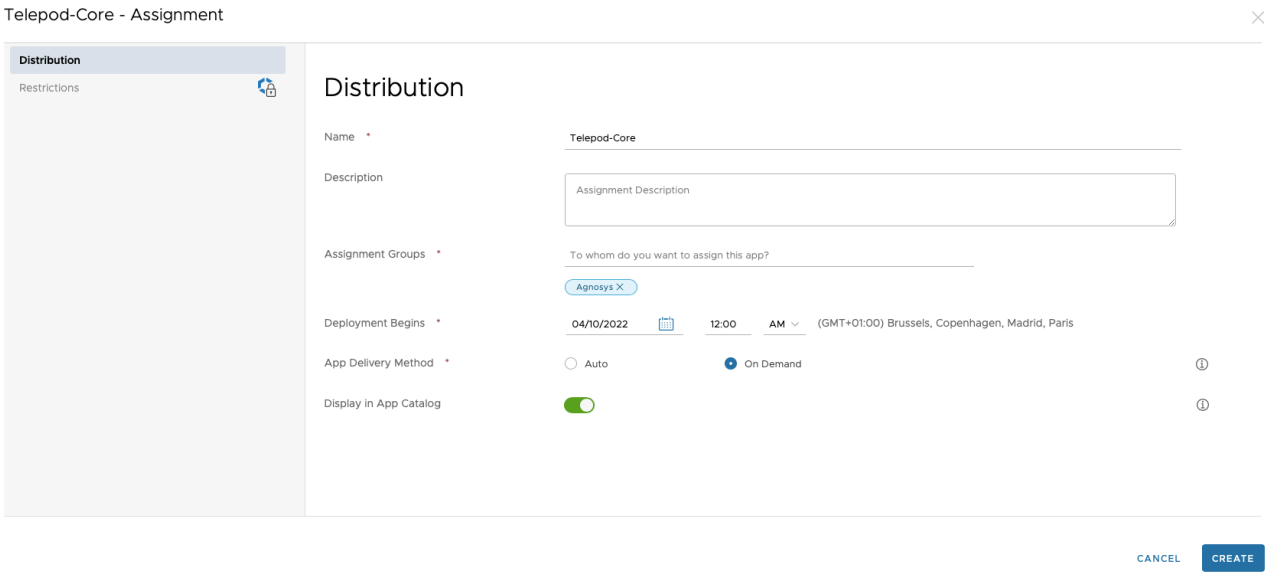
In the Preview Assigned Devices pane, click on "Publish".



Go to Resources > Apps > Native and check that the application is published and assigned.

Telepod-Core package

Reproduce the first same steps as for the Telepod-Content package until the assignment form :
- use Workspace ONE Admin Assistant to parse the Telepod-Core package
- add the Telepod-Core package as a native application
- deploy the application to the same devices using "Full Software Management".

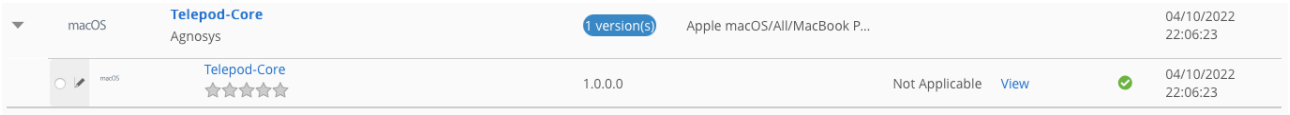


Complete the assignment form :
- Name : Telepod-Core
- Assignment Groups : select the Organization Group that encompasses the devices that must run Telepod
- App Delivery Method : **On Demand**
- Display in App Catalog : **enabled**.

Click on "Create".

In the Assignment pane, click on "Save".

In the Preview Assigned Devices pane, click on "Publish".



Go to Resources > Apps > Native and check that the application is published and assigned.

Telepod execution

Open the App Catalog.

Click on "Install" next to the "Telepod-Core" item.

The Telepod assistant opens automatically a few seconds after the Telepod-Core package is installed.

Workflows configuration

This section contains information that completes the Dictionary.

Automated Device Enrollment configuration

Telepod can automatically assign a device to a specific Automated Device Enrollment profile when this enrollment method is used, within the workflow types "Migration Back to my device", "Replacement", "Replacement en masse", "Setup", and "Setup en masse".

The selected profile may be customized to meet the specific requirements of a Telepod-driven enrollment.

This feature is currently supported only with Jamf Pro.

• **Jamf Pro**

The requirements are as follows:
- the device is enrolled using Automated Device Enrollment
- the version of Jamf Pro is 11.14 and later
- the use of Jamf Pro API is enabled.

First, in Jamf Pro, create and identify the PreStage Enrollment that the devices should use for enrollment.

Then, in the workflow configuration, fill in the dictionary named "AUTOMATED_DEVICE_ENROLLMENT".

In the PROFILE_SELECTION key, enter one of the following options :
- "name:" (exactly) followed by the Display Name of the PreStage Enrollment, or
- "id:" (exactly) followed by the ID of the PreStage Enrollment ; the ID is the integer visible in the address bar after id= when editing the profile.

Set the PROFILE_REVERT key to "true" to revert the profile assignment. This will reassign the device to the profile it had before the change, or to no profile if none was originally assigned.

Set the PROFILE_REVERT key to "false" to keep the newly assigned profile without reverting to the previous one.

Choosing the best workflow for an MDM Switching

To facilitate the transition between two MDMs, three methods are proposed, each with its own characteristics.

Workflow type	Migration Back to my device	Replacement	Migration
Device data			
Additional device required	Yes	Yes	No
Wired data flows	Device ▷ Pivot device ▷ Device	Current device ▷ New device	None
Wired data transfers performed	4 (2 backups and 2 restores)	2 (1 backup and 1 restore)	None
Resulting rapidity	☆	☆☆	☆☆☆
Device enrollment in the new MDM			
Using Automated Device Enrollment	Yes (from Setup Assistant)	Yes (from Setup Assistant)	No
Using Device Enrollment	No	Yes (from Web browser or MDM App)	Yes (from Web browser or MDM App)
Non removable enrollment	Available	Available	Not available
Device supervision			
Supervised status at end of migration	Yes	Yes	Yes (if the device is already supervised)
Supervision identity used	That of the new MDM	That of the new MDM	That of the previous MDM
Key points for choosing			
Advantages	• Workflow enabling the user to regain their device. • The removal of the remote management profile can be prevented using Automated Device Enrollment.	• All data stored on the current device is restored on the new device. • The removal of the remote management profile can be prevented using Automated Device Enrollment.	• Workflow enabling the user to regain their device. • Fastest workflow as no data transfer takes place.
Drawbacks	• Local data from apps ultimately not installed on the pivot device are not restored. • Workflow requiring the most user support from an IT technician when retaining personal data stored in non built-in and unmanaged apps is a concern.	New devices and/or device exchanges between users are required.	The removal of the remote management profile cannot be prevented because Automated Device Enrollment is not supported.

When required, the use of the additional device ensures that the supervision and enrollment information included in the backup is not applied to the device being setup.

In practice, the Migration Back to my device workflow requires that both the device and the pivot device support the latest version of iOS and iPadOS.

Data restored are those which can be backed up using an encrypted backup to a computer as designed by Apple for iOS and iPadOS.

Data from managed applications cannot be restored when configured by MDM so that their data cannot be backed up.

None of these workflows implies the recourse to iCloud.

By extension, a “**Replacement en masse**” workflow shares the same characteristics as a “Replacement” workflow, but allows the **bulk migration of devices using a single Mac host** running Telepod.

Cumulative database in XML format and CSV files

In the context of a workflow of type Replacement en masse, Setup en masse or Sorting, a cumulative database in XML format is available at this path :

/Library/Application Support/Telepod/Exports/Telepod-database.xml

This database is updated each time a device preparation is completed, successfully or not.

Prepared devices are sorted by UDID. For each device, the battery history records, for each collection date, the battery cycle count, the battery health (to be treated as a percentage) and the battery status, to help produce wear statistics.

The content of this cumulative database can be exported in whole or in part as CSV files when the workflow is stopped. Refer to the Telepod Dictionary for instructions on how to configure the EXPORTS Dictionary.

Device physical location

Telepod can display dynamically on which hub and on which port of this hub the selected device is physically connected.

When using non-manageable hubs or unsupported manageable hubs, a CSV file referencing the available slots in the USB tree must be created manually following these instructions.

A template for the CSV file is available : Telepod-Toolkit > telepod_library > locations.csv

First, build the USB tree bearing in mind that the architecture must then remain static. Consider the positioning of the components at definitive, from the USB port of the Mac host to the last hub connected in cascade. Subsequent changes may break your referencing. Then carefully validate that the constructed USB tree is fully functional by running a workflow that prepares as many iOS devices as possible.

After successful validation, apply labels to name the hubs and the ports, and to reference how all components are physically organized.

Once the labelling is completed, unplug all devices then open a Terminal Window and the CSV file.

Plug a single device to the first port of the first hub then type the following command :

```
cfgutil list
```

The answer will be a line similar to this one :

```
Type: iPad11,6 ECID: 0x1955391EA1402E UDID: 00008020-001955391EA1402E Location: 0x1100000 Name: iPad
```

Copy the value of the "Location" attribute.

In the CSV file, following an example, paste the value in the "Location" column, then add the name of the hub and the number of the port, which are two strings of your choice.

Unplug the device and repeat the process with the second port of the first hub, and so on down to the last port of the last hub.

Remove the example lines and make sure to export the file in the CSV format. Embed the CSV file in the Telepod Content and report its name, including the ".csv" extension, in the "LOCATIONS" key of the workflow.

Return to Service configuration

Handing a device from one user to the next is a common scenario in certain deployments like Education, Healthcare and Business. Available with iOS and iPadOS 17 and later, Return to Service allows an MDM to provide the device with all the information it needs to be erased and re-enrolled, on a Wi-Fi or wired network connexion.

Telepod supports Return to Service with FileWave, Jamf Pro, Mosyle Business, Mosyle Manager and VMWare Workspace ONE. During a Setup en masse workflow, when a device enrolled using Automated Device Enrollment or Device Enrollment is reconnected to the charging station, Telepod triggers a Return to service command.

The device keeps the name and the language and region settings it had before the refresh.

When the device is eligible to a "Return to Service", the following tasks that can be planned in the blueprint are ignored : Device renaming, Wi-Fi configuration profile, Device enrollment. Note that the enrollment is part of the Return to Service.

The other optional tasks planned in the workflow are executed once the device has been refreshed.

The chart below shows the types of enrollment supported by each MDM for Return to Service.

MDM Solution	Automated Device Enrollment	Device Enrollment
FileWave	✓	✗
Jamf Pro	✓	✗
Mosyle Business	✓	✓
Mosyle Manager	✓	✓
VMware Workspace ONE	✓	✗

• **FileWave**

Instead of a Device erase task, Telepod decides to trigger a Return to Service task based on several parameters :
- the workflow is of type "Setup en masse"
- the workflow does not include restoring a backup
- the device is installed with iOS or iPadOS 17 and later
- the device is enrolled using Automated Device Enrollment (based on the device inventory)
- an Activation Lock is not enabled on the device (based on the device inventory)
- an OS restore task determined by the workflow is not scheduled.

No check is implemented to validate this requirement :
- the version of FileWave is 15.1 and later.

To enable Return to Service, set the "SETTINGS > Refresh using Return to Service" key to "true".

Return to Service uses the Wi-Fi configuration profile defined by the RETURN_TO_SERVICE > WIFIPROFILEDATA key. Refer to the Telepod Dictionary to define the value expected by the MDM solution.

• **Jamf Pro**

Instead of a Device erase task, Telepod decides to trigger a Return to Service task based on several parameters :
- the workflow is of type "Setup en masse"
- the workflow does not include restoring a backup
- the version of Jamf Pro is 10.50 and later
- the use of Jamf Pro API is enabled
- the device is installed with iOS or iPadOS 17 and later
- the device is enrolled using Automated Device Enrollment (based on the device inventory)
- an Activation Lock is not enabled on the device (based on the device inventory)
- an OS restore task determined by the workflow is not scheduled.

To enable Return to Service, set the "SETTINGS > Refresh using Return to Service" key to "true".

Return to Service uses the Wi-Fi configuration profile defined by the RETURN_TO_SERVICE > WIFIPROFILEDATA key. Refer to the Telepod Dictionary to define the value expected by the MDM solution.

• **Mosyle Business and Mosyle Manager**

Instead of a Device erase task, Telepod decides to trigger a Return to Service task based on several parameters :
- the workflow is of type "Setup en masse"
- the workflow does not include restoring a backup
- the device is installed with iOS or iPadOS 17 and later
- the device is enrolled (Automated Device Enrollment or Device Enrollment)
- Find My is not enabled on the device (based on the device inventory)
- an OS restore task determined by the workflow is not scheduled.

To enable Return to Service, set the "SETTINGS > Refresh using Return to Service" key to "true".

Return to Service uses the Wi-Fi configuration profile defined in Management > iOS / iPadOS / watchOS > Management Profiles > Wifi Authentication > WiFi > Profile Name >
Return to Service : Set this Network as default to be sent with Erase commands. (iOS/iPadOS 17 and higher).

• **VMware Workspace ONE**

Instead of a Device erase task, Telepod decides to trigger a Return to Service task based on several parameters :
- the workflow is of type "Setup en masse"
- the workflow does not include restoring a backup
- the device is installed with iOS or iPadOS 17 and later
- the device is enrolled using Automated Device Enrollment (based on the device inventory)
- an Activation Lock is not enabled on the device (based on the device inventory)
- an OS restore task determined by the workflow is not scheduled.

To enable Return to Service, set the "SETTINGS > Refresh using Return to Service" key to "true".

Return to Service uses the Wi-Fi configuration profile defined by the RETURN_TO_SERVICE > WIFIPROFILEDATA key. Refer to the Telepod Dictionary to define the value expected by the MDM solution.

Integrating Telepod with Cambrionix units

Telepod can benefit from the use of Cambrionix units to report :
- the device physical location in the graphical interface
- the device preparation status via the USB ports LEDs.

This section outlines the key points for integrating Telepod with Cambrionix units. Please refer to Cambrionix documentation for details not specific to Telepod.

Cambrionix API installation

To install the Cambrionix API when it is detected as missing when Telepod is executed, configure the following keys with the indicated values :
- INTEGRATIONS > CAMBRIONIX_INTEGRATION — Boolean — true
- INTEGRATIONS > CAMBRIONIX_CONFIGURATION > INSTALL — String — enabled
- INTEGRATIONS > CAMBRIONIX_CONFIGURATION > API_URL — String — https://downloads.cambrionix.com/api/v1/software/cambrionix-hub-api/latest/macos/download (the alternative is to specify a download URL for a previous package).

The Cambrionix API is detected as missing when the file "/Library/Cambrionix/ApiService/bin/CambrionixApiService" does not exist.

The installation process only installs the "Cambrionix API Daemon" included in the package fetched at the specified URL.

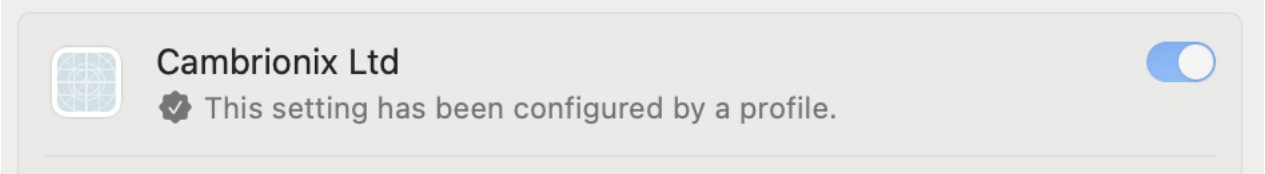
Please note that Telepod is not responsible for updating an existing version of the Cambrionix API Daemon and assumes that it is usable for the intended operations.

Background Item Management

With macOS 13 and later, a Background Item Management configuration profile must be deployed so that the system does not display a notification that Cambrionix has installed a Login item that can run in the background and that can be managed in System Settings.

Payload required : Background Item Management

- Rule Type : Label
- Rule Value : com.cambrionix.api



Once the configuration profile is deployed on a Mac host running Telepod, open System Settings > Login Items and check that the provisioned Login Items are enabled and cannot be disabled.

Units detection

In the context of a workflow of type Setup en masse or Sorting, the detected units are displayed before the devices list is displayed.

Device physical location

In the context of a workflow of type Setup en masse or Sorting, Telepod displays dynamically on which hub and on which port of this hub the selected device is physically connected. These informations are retrieved using API calls.

No additional configuration is required to achieve this result.

ThunderSync3-16 LEDs management

• Replacement en masse and Setup en masse workflow

The status of device operations is reported by the LEDs of the port to which it is connected.

Telepod takes over LED management when operations start on the first device and releases control when the workflow ends.

Green	Orange	Red	Meaning
Off	Off	Off	Device disconnected (status can be transient)
Flashing	Off	Off	Operations in progress
Flashing	Flashing	Off	Operations in progress, error detected (can be transient)
Steady-on	Off	Off	Operations completed
Steady-on	Flashing	Off	Operations completed, error(s) detected
Off	Off	Steady-on	Operations aborted (unrecoverable error encountered)

Apart from the time when Telepod is responsible for LEDs management, the default behaviour of the unit applies.

Green	Orange	Red	Meaning
Off	Off	Off	Device disconnected
Off	Steady-on	Off	Device connected

• Sorting workflow

The status of device operations is reported by the LEDs of the port to which it is connected.

Telepod takes over LED management when operations start on the first device and releases control when the workflow ends.

Green	Orange	Red	Meaning
Off	Off	Off	Device disconnected (status can be transient)
Flashing	Off	Off	Sorting in progress
Flashing	Flashing	Off	Sorting in progress, error detected (can be transient)
Steady-on	Off	Off	Sorting completed, battery status normal
Steady-on	Flashing	Off	Sorting completed, battery status warning
Steady-on	Off	Flashing	Sorting completed, battery status failure
Off	Off	Steady-on	Sorting aborted (unrecoverable error encountered)

Apart from the time when Telepod is responsible for LEDs management, the default behaviour of the unit applies.

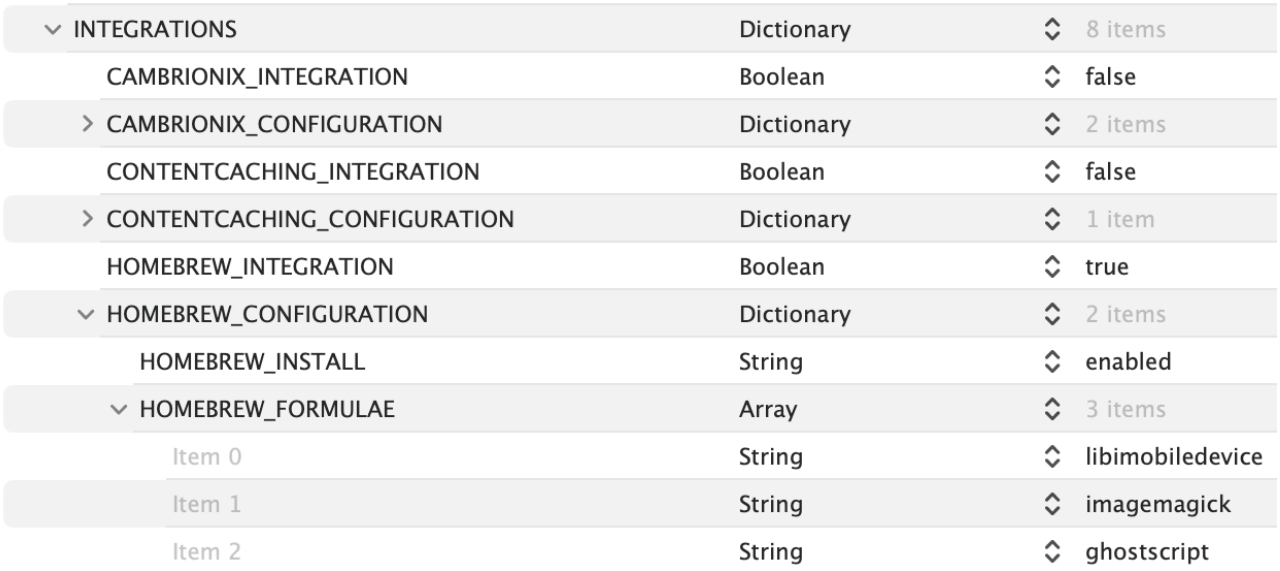
Green	Orange	Red	Meaning
Off	Off	Off	Device disconnected
Off	Steady-on	Off	Device connected

Implementing Digital signage

Digital signage enables customized text to be inlaid into wallpapers installed by Telepod. This capability is supported with Setup and Setup en masse workflows and requires very precise configurations, as detailed in this chapter. The following instructions apply for both workflows unless otherwise stated.

Software dependencies

Digital signage requires the installation of two Homebrew formulae named "imagemagick" and "ghostscript".



In the main settings, check the following configurations :
- HOMEBREW_INTEGRATION : "true"
- HOMEBREW_INSTALL : "enabled"
- HOMEBREW_FORMULAE : includes "imagemagick" and "ghostscript" in this order (libimobiledevice is required for battery diagnostics).

Wallpapers and fonts

Find the pictures to be used for the home screen and the lock screen. The same picture can be used for both screens. A picture in landscape mode will be cropped to portrait mode and the final picture will have a ratio of 2:3. Therefore consider that the important part of a picture is its center.

The fonts to be used for the texts must be installed on the Mac host running Telepod. The same font can be used for both screens. Any font available in the Font Book application should be usable by Digital signage. Please note that Telepod is not responsible for font installation.

Overlay values

When configuring Digital signage, an Overlay value must be entered for each configured wallpaper. This value contains three informations :
- font : exact name of a font available on the Mac host running Telepod
- fill : color of the text in RGB Decimal Code
- max-width : maximum number of points in the image width that can be used to display the entire sample text.

The Telepod Toolkit includes a tool that constructs this value on the basis of your experiments.

Open the Telepod Toolkit then the telepod_library subfolder.

Open the script named "telepod_digital_signage_helper.sh" with a Text Editor like Sublime Text.

Go to this section :

```
# Parameters (see the instructions)

DS_PICTURE_NAME="/Users/ladmin/Desktop/luxury_1.jpg"
DS_FONT="Snell-Roundhand"
DS_FILL="rgb(255,255,255)"
DS_MAX_WIDTH=1300
```

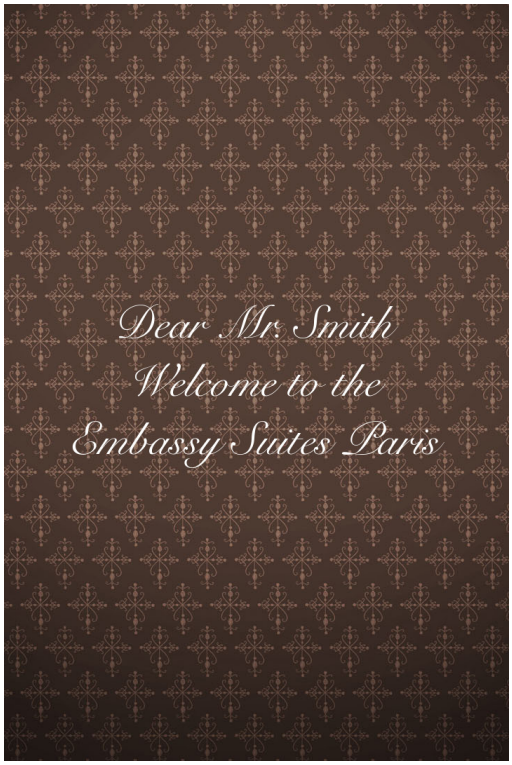
First focus on the DS_PICTURE_NAME variable. To easily obtain the pathname to a picture, right-click on the this picture, then hold down the Option key to reveal the "Copy (item name) as Pathname" action and select it. In the script, select the string **between** the two double quotes and go to Edit > Paste.

Go to File > Save to save the script with the edited pathname.

Open the Terminal utility located in /Applications/Utilities and type the command "bash" followed by a space. Then drag and drop the script inside the window to build the complete command similar to this one.

```
ladmin@MacBook-Air ~ % bash /Users/ladmin/Desktop/Telepod-Toolkit/
telepod_library/telepod_digital_signage_helper.sh
```

The script will first check that Homebrew and the required dependencies are installed. If that is not the case, follow the displayed instructions and enter your password when prompted. After a few operations, the picture with the text inlay is opened.



This is where the fine-tuning begins.

In the Terminal window, scroll up to return to the section entitled "Exact names of fonts available on this Mac". Identify the exact name to be used, that is expected to match the font chosen in the Font Book application. Copy the name, go back to the script, select for the DS_FONT variable the string **between** the two double quotes and go to Edit > Paste.

Go to File > Save to save the script with the edited pathname and font name.

Return to the Terminal window and type `!!` (2 exclamations marks). The previous command will be replayed and the picture with the text inlay and the new font is opened.

In the same way, edit and test the values for the DS_FILL and DS_MAX_WIDTH variables.

To find the color of the text in RGB Decimal Code, you can refer to this site :
https://www.rapidtables.com/web/color/RGB_Color.html

To find the maximum number of points in the image width that can be used to display the entire sample text, you need to proceed by successive tests as the value depends on the picture and the font chosen. Remember to leave a small margin between the text and the edge of the image. Note that the sample text used to determine this value is of no importance whatsoever, but is representative of the use of the Digital signage.

Once you are satisfied with a combination of picture, font and color, look at the last two lines of the output in the Terminal window :

```
Use the following value for the OVERLAY key :
font:Snell-Roundhand|fill:rgb(255,255,255)|max-width:1300
```

The last line here in bold is the one you will use as the Overlay value when configuring Digital signage. Copy it in a safe place with a note of its use case, you will need it for the next steps.

If you need another Overlay value because you are going to use different pictures, fonts or colors for the home screen and the lock screen, it is recommended to define it now, so you will have all the Overlay values ready to be used.

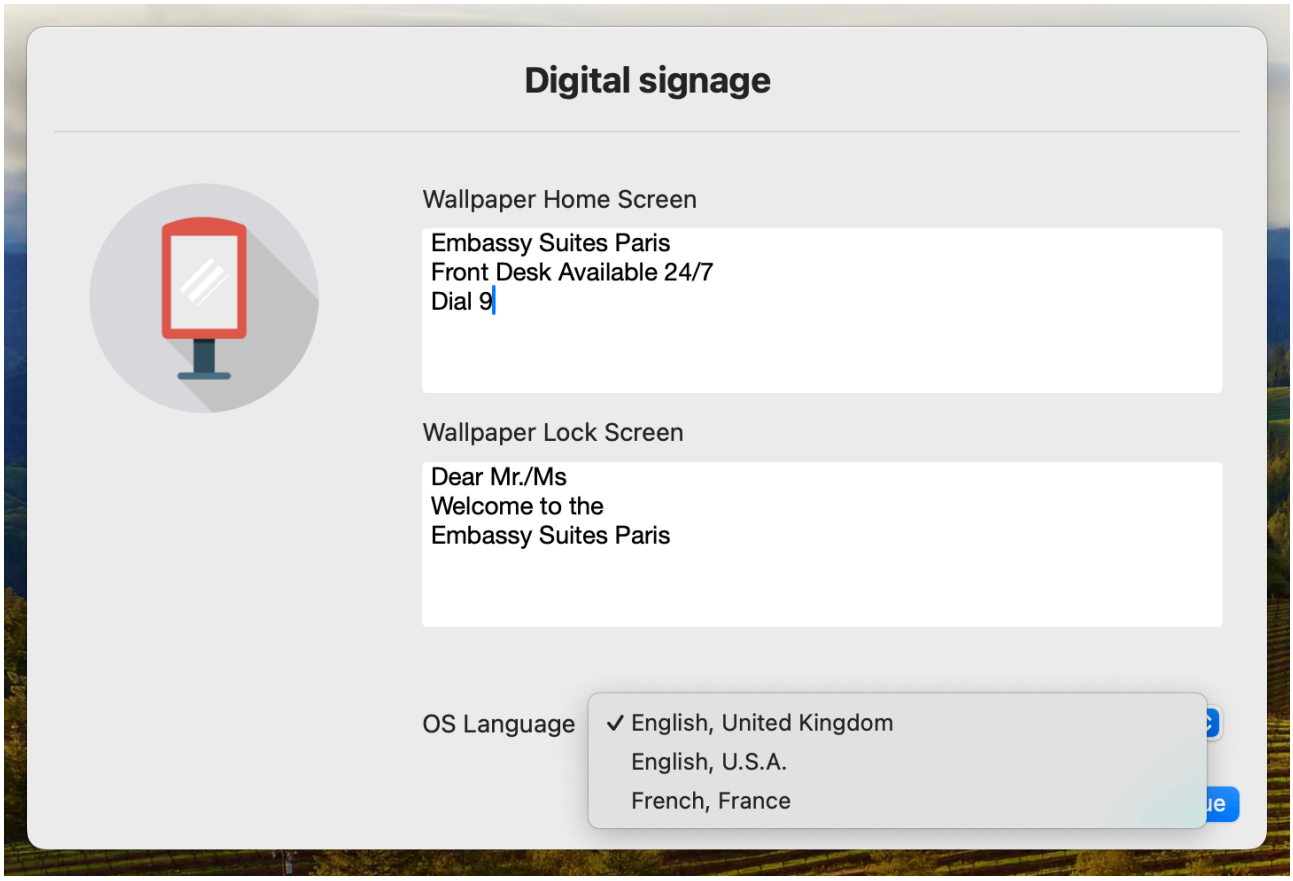
Configuring digital signage for a Setup workflow

This section only applies to a Setup workflow.

DIGITAL_SIGNAGE	Dictionary	2 items
FIELDS	Array	2 items
Item 0	Dictionary	5 items
TITLE	String	Wallpaper Home Screen
TYPE	String	textarea
PLACEHOLDER	String	Embassy Suites Paris\rFront Desk Available 24/7\rDial 9
LOCATION	String	HOME_SCREEN
OVERLAY	String	font:Snell-Roundhand|fill:rgb(255,255,255)|max-width:1300
Item 1	Dictionary	5 items
TITLE	String	Wallpaper Lock Screen
TYPE	String	textarea
PLACEHOLDER	String	Dear Mr./Ms\rWelcome to the\rEmbassy Suites Paris
LOCATION	String	LOCK_SCREEN
OVERLAY	String	font:Snell-Roundhand|fill:rgb(255,255,255)|max-width:1300
LANGUAGES	Array	3 items
Item 0	Dictionary	2 items
LANGUAGE_DISPLAYED	String	English, United Kingdom
LANGUAGE_LOCALE	String	language:en,locale:en_GB
Item 1	Dictionary	2 items
LANGUAGE_DISPLAYED	String	English, U.S.A.
LANGUAGE_LOCALE	String	language:en,locale:en_US
Item 2	Dictionary	2 items
LANGUAGE_DISPLAYED	String	French, France
LANGUAGE_LOCALE	String	language:fr,locale:fr_FR

This is the Digital signage template for this type of workflow. To start, be sure to remove the "disabled-" prefix before "DIGITAL_SIGNAGE" to enable the capability.

This template triggers the display of the following Digital signage pane.



In the FIELDS Array, Item 0 configures the Home Screen and Item 1 configures the Lock Screen.

The only changes to make in each item are the following :
- replace the PLACEHOLDER value with the text to be displayed by default ; note that \r (backslash followed by r) is used to define a new line in the text inlay
- replace the OVERLAY value with the previously defined one.

The TYPE and LOCATION values must not be changed.

The TITLE value can be edited for a translated string if necessary.

In the LANGUAGES Array, each item defines a Language and Locale combination available in the menu. The LANGUAGE_DISPLAYED value is at your choice, which is not the case for the corresponding LANGUAGE_LOCALE value, e.g. "language:fr,locale:fr_FR".

The recommended way to define a language with a locale is the following :
- connect an iOS device to a Mac
- open a Terminal window
- type the command : `cfgutil get supportedLanguages supportedLocales`

Grab the supported languages and locales displayed to build the combinations that appear to be the most common, bearing in mind that you will not support all the possible combinations.

WALLPAPER	Dictionary	2 items
HOME_SCREEN	Dictionary	1 item
IMAGE	String	home_screen.jpg
LOCK_SCREEN	Dictionary	2 items
IMAGE	String	lock_screen.jpg
TEXT	String	

Below the DIGITAL_SIGNAGE Dictionary, find the WALLPAPER Dictionary. Replace the HOME_SCREEN > IMAGE value with the name of the picture to be used for the home screen and the LOCK_SCREEN > IMAGE value with the name of the picture to be used for the lock screen. Check that the pictures referenced here are the ones used to define the Overlay values and that they are part of the Telepod Content.

This concludes the Digital signage configuration for a Setup workflow.

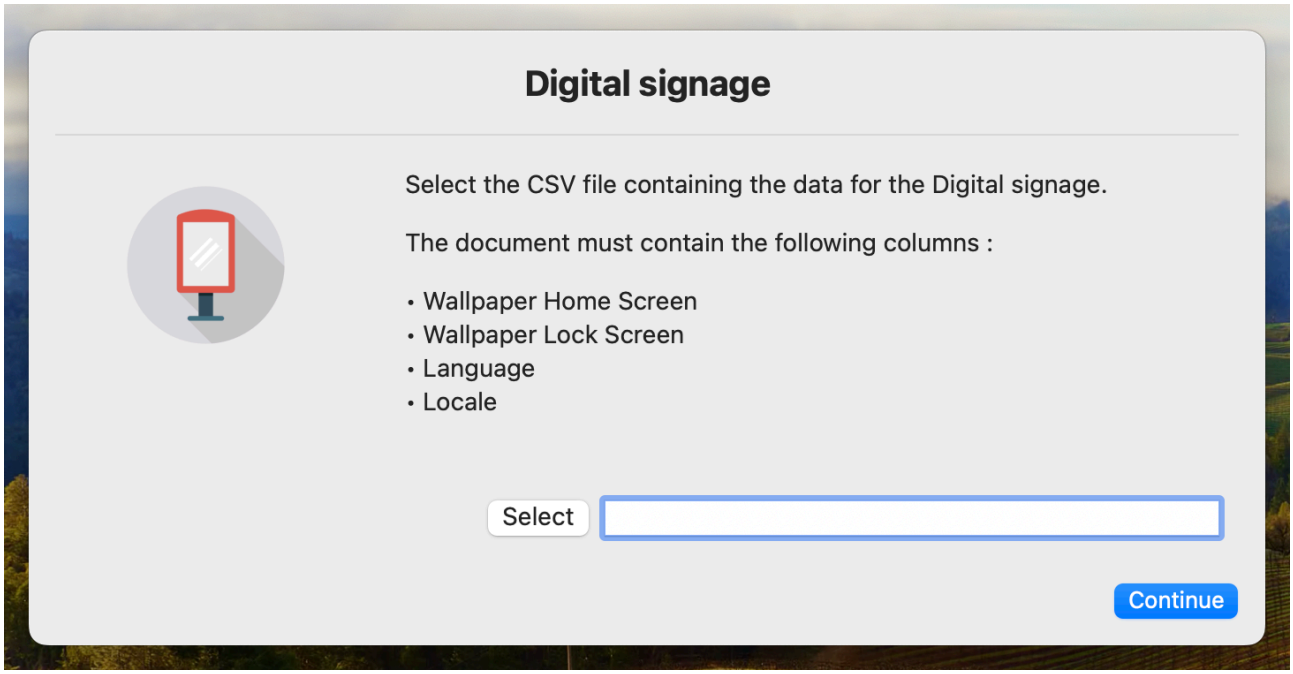
Configuring digital signage for a Setup en masse workflow

This section only applies to a Setup en masse workflow.

DIGITAL_SIGNAGE	Dictionary	1 item
COLUMNS	Array	2 items
Item 0	Dictionary	3 items
TITLE	String	Wallpaper Home Screen
LOCATION	String	HOME_SCREEN
OVERLAY	String	font:Snell-Roundhand|fill:rgb(255,255,255)|max-width:1300
Item 1	Dictionary	3 items
TITLE	String	Wallpaper Lock Screen
LOCATION	String	LOCK_SCREEN
OVERLAY	String	font:Snell-Roundhand|fill:rgb(255,255,255)|max-width:1300

This is the Digital signage template for this type of workflow. To start, be sure to remove the "disabled-" prefix before "DIGITAL_SIGNAGE" to enable the capability.

This template triggers the display of the following Digital signage pane.



In the COLUMNS Array, Item 0 configures the Home Screen and Item 1 configures the Lock Screen. The only change to make in each item is the remplacement of the OVERLAY value with the previously defined one.

The TITLE values must match the names of the columns in the CSV file selected.

The Telepod Toolkit includes templates for the CSV file expected in CSV, Excel and Numbers formats.

Open the Telepod Toolkit then the telepod_library subfolder. Open the file named "digital_signage.numbers" or "digital_signage.xslx" according to your preferred spreadsheet application.

Wallpaper Home Screen	Wallpaper Lock Screen	Language	Locale
Embassy Suites Paris\rFront Desk Available 24/7\rDial 9	Dear Mr. Smith\rWelcome to the\rEmbassy Suites Paris	en	en_GB
Embassy Suites Paris\rFront Desk Available 24/7\rDial 9	Dear Mr. Jones\rWelcome to the\rEmbassy Suites Paris	en	en_US
Embassy Suites Paris\rFront Desk Available 24/7\rDial 9	Dear Ms Martin\rWelcome to the\rEmbassy Suites Paris	fr	fr_FR
Embassy Suites Paris\rFront Desk Available 24/7\rDial 9	Dear Ms Rossi\rWelcome to the\rEmbassy Suites Paris	it	it_IT

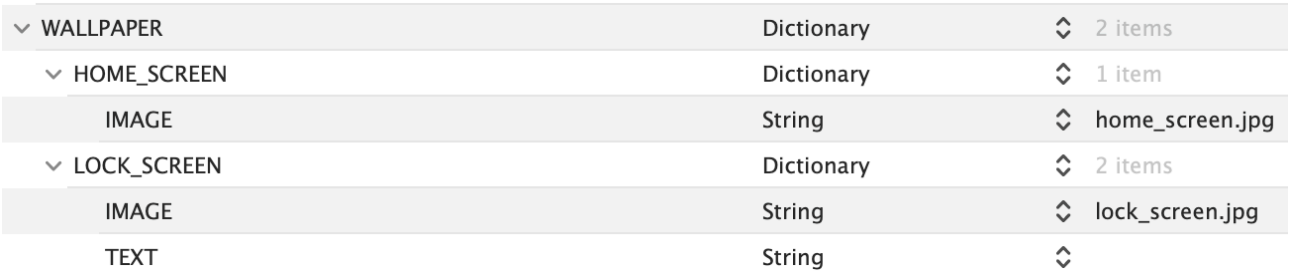
Observe that the names of the columns match those indicated in the Digital signage pane. Note that \r (backslash followed by r) is used to define a new line in the text inlay.

The recommended way to define possible languages and locales is the following :
- connect an iOS device to a Mac
- open a Terminal window
- type the command : `cfgutil get supportedLanguages supportedLocales`

Once the file is completed, it must be exported in CSV format (the supported separators are the comma and the semicolon).

When exporting the file with Excel, select one of these file formats :
- Comma Separated Values (.csv)
- MS-DOS Comma Separated (.csv).

Do not use the file format CSV UTF-8 (Comma delimited) (.csv) which adds a BOM that breaks the CSV file parsing.



Below the DIGITAL_SIGNAGE Dictionary, find the WALLPAPER Dictionary. Replace the HOME_SCREEN > IMAGE value with the name of the picture to be used for the home screen and the LOCK_SCREEN > IMAGE value with the name of the picture to be used for the lock screen. Check that the pictures referenced here are the ones used to define the Overlay values and that they are part of the Telepod Content.

This concludes the Digital signage configuration for a Setup en masse workflow.

Digital signage operations

For a Setup workflow, the Digital signage is applied during the "Wallpaper" task on the selected device.

For a Setup en masse workflow, the Digital signage modifies the functioning of the Telepod task manager named EMERAC.

EMERAC first determines the number of devices required to meet Digital signage needs based on the CSV file uploaded, then attempts to map each device required to a connected device. If the number of connected devices is less than the number of required devices, Telepod indicates the number of "Awaited devices", so that the Telepod user knows how many additional devices to connect. Inversely, if the number of connected devices is greater than the number of required devices, Telepod indicates the number of "Ignored devices", so that the Telepod user knows how many connected devices will remain untouched during the workflow.

Localizing Telepod

Telepod offers two methods to localize the strings displayed during a workflow, a basic one to quickly localize a couple of key strings in the configuration files and an advanced one to fully localize all strings.

Localization of the configuration files for one language

Once the Telepod configuration file is built with the main settings and the workflows, localize the strings in the UIHELPER and INTEGRATIONS sections.

As indicated in the Telepod Dictionary, use \r to create a line break and \r\r to create a line break followed by an empty line, except in the UIHELPER_MAIN_TEXT_HELP key, where exactly two spaces followed by \n create a line break, and \n\n creates a line break followed by an empty line.

Take care of the variables used. Variables must be written exactly as indicated in the placeholders, keeping the starting and leading columns (:) otherwise their substitutions by expected values will fail.

The strings used to declare a menu in the SETTINGS_PANE > LIST array offer localizable texts :
- TITLE, BUBBLE_TITLE, BUBBLE_TEXT
- VALUE_DISPLAYED, VALUE_STORED.

Localization of the configuration files for multiple languages

The following keys can be localized for multiple languages :
- UIHELPER_MAIN_TITLE_WELCOME
- UIHELPER_MAIN_TEXT_WELCOME
- UIHELPER_MAIN_TEXT_HELP
- UIHELPER_BUTTON_LABEL_HELP
- UIHELPER_MAIN_TITLE_INTRO
- UIHELPER_MAIN_TEXT_INTRO
- UIHELPER_MAIN_TITLE_EULA
- UIHELPER_MAIN_TEXT_EULA
- UIHELPER_BUTTON_LABEL_EULA
- UIHELPER_TITLE_EULA_FORM
- UIHELPER_SUBTITLE_EULA_FORM
- UIHELPER_MAIN_TITLE_SETTINGS
- UIHELPER_MAIN_TEXT_SETTINGS
- UIHELPER_MAIN_TITLE_LANDING
- UIHELPER_MAIN_TEXT_LANDING

1. Identify the language codes to use in the configuration file(s) :

    - in the Language & Region System Setting (Preference), set the Preferred languages

    - open a Terminal Window

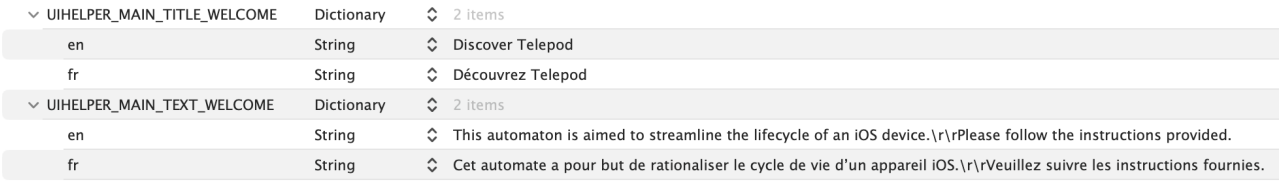
- type the following command :

```
defaults read .GlobalPreferences.plist AppleLanguages
```

- read the output for a user which preferred languages are French then English :

```
(
        "fr-FR",
        "en-FR"
)
```

2. Convert the Strings to Dictionaries and add one entry for each language supported.



For each entry of the Dictionary, the key name is one of the codes identified at step 1, the key type is a string and the key value is the text to display.

When Telepod is executed, the previous command is used to define the preferred languages, read from top to bottom. Each time a translation is supported, a localizable string is searched according to the order of the preferred languages. If no string is available in the preferred languages, the fallback is firstly the string in English (en), secondly the first string found in the Dictionary, and thirdly the built-in string in English.

Advanced localization

Once familiar with the basic localization, you can go with the advanced localization. This localization is based on building a custom PO file from a template POT file.

The localization is aimed firstly to translate the built-in strings of Telepod in English to another language, but can also be diverted to just customize those strings in English.

The POT file is provided in the telepod_library subfolder of the Telepod Toolkit folder. An example of a PO file for French language is available at the same place.

To create a new PO file for your language with the POedit application, please follow these steps.

1. Download Poedit : https://poedit.net/download

2. Open Poedit

3. File > New From POT/PO File...

4. Select Telepod Toolkit > telepod_library > telepod.pot > Open

5. Language of the translation > select the targeted language (e.g. "French")

6. Translate offered strings

In the translations, use \n to create a line break, and \n\n to create a line break followed by an empty line. Poedit automatically manages the \n when inserting a carriage return.

Take care of the variables used. Variables must be written exactly as indicated in the placeholders, keeping the starting and leading columns (:) otherwise their substitutions by expected values will fail.

If a translation is blank in the PO file, the fallback is the built-in string in English.

7. Identify the language code to use in the PO filename :

- in the Language & Region System Setting (Preference), set the Preferred languages

- open a Terminal Window

- type the following command :

```
defaults read .GlobalPreferences.plist AppleLanguages
```

- read the output for a user which preferred languages are French then English :

```
(
      "fr-FR",
      "en-FR"
)
```

8. File > Save > Save As : name the file "telepod_**languagecode**.po" (e.g. "telepod_**fr**.po")

9. Add the PO file to the Telepod Content (MO files are not supported, see POedit Preferences to stop their compilation)

10. To update an existing PO file with the strings of an updated telepod.pot file : Translation > Update from POT File

When Telepod is executed, the previous command is used to define which PO file must be invoked. The languages are read from top to bottom. As a PO file matches the language read, it is cached for the length of the workflow and the evaluation stops. If the language read is English and no PO file is available for English, the built-in strings in English are displayed.

Updating Telepod

To safely update your Telepod implementation with the latest version of the product, please follow these instructions carefully.

The components to be updated are respectively :
- Telepod Toolkit
- Telepod configuration file(s)
- Custom configuration profile(s)
- Telepod Content package
- Telepod Core package.

Telepod Toolkit

First of all, backup your current Telepod-Toolkit folder. It contains ressources that must be preserved during the update.

1. Rename your current Telepod-Toolkit folder, adding a suffix like "_previous"

2. Download and install the updated version of Telepod Toolkit

3. Place the updated Telepod-Toolkit folder next to the previous Telepod-Toolkit folder

4. Copy from the previous folder the **.plist files** stored in telepod_configs > configs_plists to the updated folder in telepod_configs > configs_plists. Be sure to keep the updated templates (the file named "config_1.plist" and the folder named "templates").

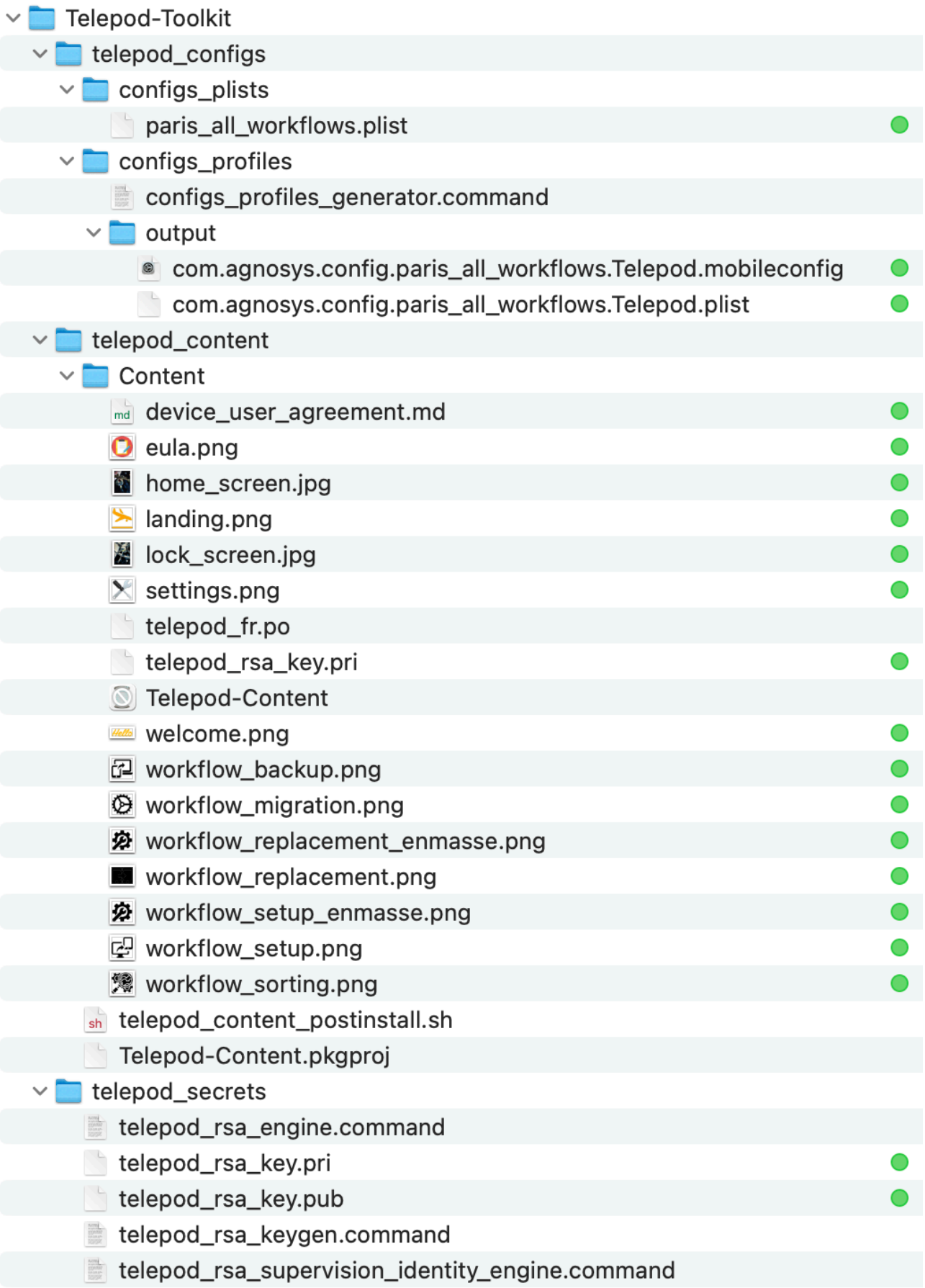
5. Copy from the previous folder the **.mobileconfig and .plist files** stored in telepod_configs > configs_profiles > output to the updated folder in telepod_configs > configs_profiles > output

6. Copy from the previous folder **the content of the folder** telepod_content > Content except **Telepod-Content.app and original .po files** to the updated folder in telepod_content > Content

7. Copy from the previous folder **the following 2 files** stored in telepod_secrets to the updated folder in telepod_secrets :

    - telepod_rsa_key.pri
    - telepod_rsa_key.pub

To summarize, the figure below shows the copied resources with green dots.


Telepod-Toolkit
telepod_configs
configs_plists
paris_all_workflows.plist
configs_profiles
configs_profiles_generator.command
output
com.agnosys.config.paris_all_workflows.Telepod.mobileconfig
com.agnosys.config.paris_all_workflows.Telepod.plist
telepod_content
Content
device_user_agreement.md
eula.png
home_screen.jpg
landing.png
lock_screen.jpg
settings.png
telepod_fr.po
telepod_rsa_key.pri
Telepod-Content
welcome.png
workflow_backup.png
workflow_migration.png
workflow_replacement_enmasse.png
workflow_replacement.png
workflow_setup_enmasse.png
workflow_setup.png
workflow_sorting.png
telepod_content_postinstall.sh
Telepod-Content.pkgproj
telepod_secrets
telepod_rsa_engine.command
telepod_rsa_key.pri
telepod_rsa_key.pub
telepod_rsa_keygen.command
telepod_rsa_supervision_identity_engine.command

Telepod configuration file(s)

Complete your current .plist file(s) to implement as desired new capabilities of Telepod, helping you with the updated Telepod Dictionary and the updated config_1.plist file. Do not hesitate to contact Telepod support if you need any clarifications.

Warning : Ensure that your Telepod configuration file(s) contain(s) your current Telepod license, as it may have been updated directly in the MDM solution, but not in the Telepod configuration file(s).

Even if your MDM solution offers an interface for directly modifying, and not just reading, the keys of the deployed Custom configuration profile(s), it is recommended to update the Telepod configuration file(s) using your preferred Property List editor to ensure no structural errors are introduced accidentally. The only key supported for direct modification is the license code.

Custom configuration profile(s)

1. Refer in this documentation to the section entitled "Telepod configuration files to Custom configuration profiles conversion" to convert your updated Telepod configuration file(s) to Custom configuration profile(s), if applicable. This one / these ones will reuse the same identifier(s) as the previous Custom configuration profile(s), thanks to the content of the output folder copied at the expected location.

2. Refer in this documentation to the section entitled "Custom configuration profile" included in each chapter entitled "Provisioning *MDM",* and consult the MDM documentation if necessary, to distribute the updated Custom configuration profile(s), replacing the previous one(s).

Telepod Content package

As the private key contained in the file "telepod_rsa_key.pri" is static and if you didn't update the other resources, no action is necessary.

If you implemented an advanced localization, you may have to revise your PO files after importing the updated POT file provided. Otherwise, built-in strings in English may be unexpectedly displayed.

If you updated the other resources :
- refer to this documentation to build an updated Telepod-Content package
- refer to this documentation and the MDM documentation to deploy the updated package.

Telepod Core package

1. Download the updated version of Telepod Core.

2. Refer to this documentation and the MDM documentation to deploy the updated package.

Troubleshooting

When using the commands described below, pay attention to use "**straight**" double quotes and not "curly" double quotes often generated automatically by word processing applications.

Enable the logging manually

Open the Terminal utility located in /Applications/Utilities.

Two level of logging can be enabled, depending of the debug flag created.

To enable a standard logging, type :
`sudo touch "/Library/Application Support/Telepod/debug"`

To enable a verbose logging, type :
`sudo touch "/Library/Application Support/Telepod/debugverbose"`

Enter your password.

Logs are written in /private/var/log.

Warning : Do not forget to delete the Telepod logs and the debug flag created once the log analysis is completed.

Enable the logging with Custom configuration profile

Two level of logging can be enabled, depending of the value entered for the DEBUGMODE.

To enable a standard logging, set the DEBUGMODE key to "debug".

To enable a verbose logging, set the DEBUGMODE key to "debugverbose".

Logs are written in /private/var/log.

Warning : Do not forget to disable the debug logging then delete the Telepod logs once the log analysis is completed.

Note that this setting is ignored if the logging has been already enabled by the manual creation of a debug flag.

Display the logs from the Console utility

Open the Console utility located in /Applications/Utilities.

Select Reports > Log Reports > a log file whose name begins with "Telepod-"

Display the logs from the Terminal utility

Select Finder > Go > Go to Folder > /private/var/log

Open the Terminal utility located in /Applications/Utilities.

Type : `sudo cat`

Type a space then drag and drop a log file whose name begins with "Telepod-"

Enter your password.

In the context of a request for support, please attach a **verbose** log to your message.

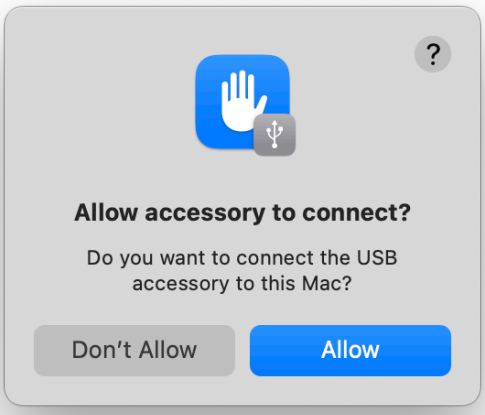
Terminate the execution of a running workflow

To terminate the execution of a running workflow :
- open a Terminal Window as an administrator account
- type the following commands :

```
sudo launchctl bootout system/com.agnosys.telepod_supervisor
sudo launchctl bootout system/com.agnosys.telepod
```

Alternatives to terminate the execution of a running workflow :
- log out and leave the Mac 10 seconds on the login window
- restart or shutdown the Mac.

Allow accessories to connect



If the Mac host is a laptop with Apple silicon running macOS 13 and later, new USB devices that are connected must be approved. If you choose "Allow", the device allows both power and data transmission. If you choose "Don't Allow", the device can still charge, but no data is transmitted.

To suppress this alert when using the Telepod, open System Settings > Privacy & Security and in the Security section, select in "Allow accessories to connect" the option "Always".

The alternative to this manual configuration is to provision the Mac host with a configuration profile of type restrictions that includes the key "Allow USB restricted mode" set to "false".

Reset the backup password of a device

Encrypted backups can include information that unencrypted backups don't like saved passwords, Wi-Fi settings, Website history, Health data or Call history. Encrypted backups don't include Face ID, Touch ID, or device passcode data

The password used to encrypt a backup made locally on a computer is most of the time defined when the device is backed up with the Finder or iTunes. The password is stored on the device and is not dependant of the computer used to set it up. A Mac may have a copy of it in the Login Keychain of the user who defined it, although if is not mandatory.

Forgetting this password does not prevent to backup the device. It prevents the backup to be restored on the same device or another device, making it unusable.

If the device is running iOS 11 or later, when this password is lost, it can be reset on the device itself. Go to Settings > General > Transfer or Reset [Device] > Reset > Reset All Settings. This won't affect the user data or passwords, but it will reset settings like display brightness, Home Screen layout, and wallpaper.

Then, a Telepod workflow can set up a new backup password, either read from the configuration file or entered interactively. Please refer to the Telepod Dictionary to know how to use the BACKUP_PASSWORD key for both scenarios.

Device identification

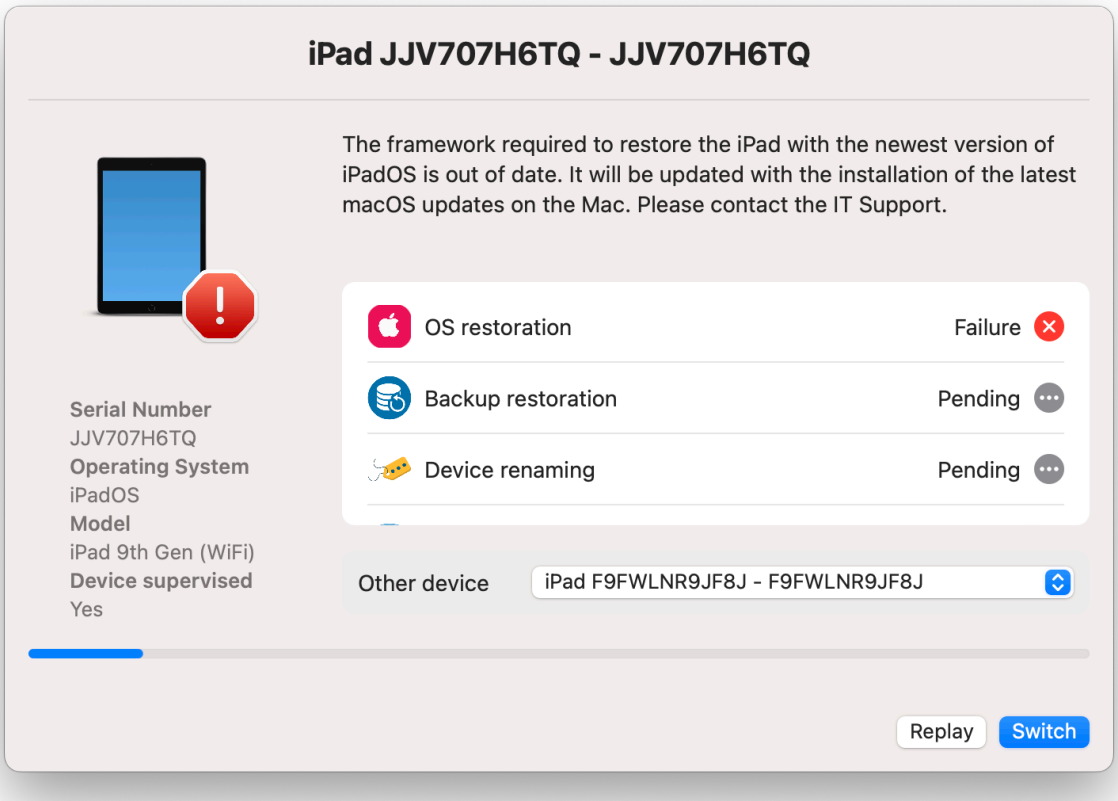
Telepod tries to convert the device type to the device model based on the following project : https://gist.githubusercontent.com/adamawolf/3048717/raw

Telepod tries to display the Apple picture of the device based on the genuine MobileDevices[...].bundle files which are searched by default in /System/Library/Templates/Data/System/Library/CoreServices/CoreTypes.bundle/Contents/Library with a fallback to /System/Library/CoreServices/CoreTypes.bundle/Contents/Library.

To extend the pictures available on a Mac host which may not run the latest version of macOS :
- embed the most recent versions of these bundles in the Telepod Content
- set the MOBILEDEVICES_BUNDLES key to the full path of their location (e.g. /Library/Application Support/Telepod/Content).

If the device model or the device picture is not displayed correctly, please send a message to telepod.support@agnosys.fr with these informations :
- device type displayed (e.g. iPad13,19) instead of expected device name (e.g. iPad 10th Gen)
- device color or finish (e.g. Space Gray)
- network connectivity (e.g. Wi-Fi or Wi-Fi + Cellular).

MobileDevice framework out of date

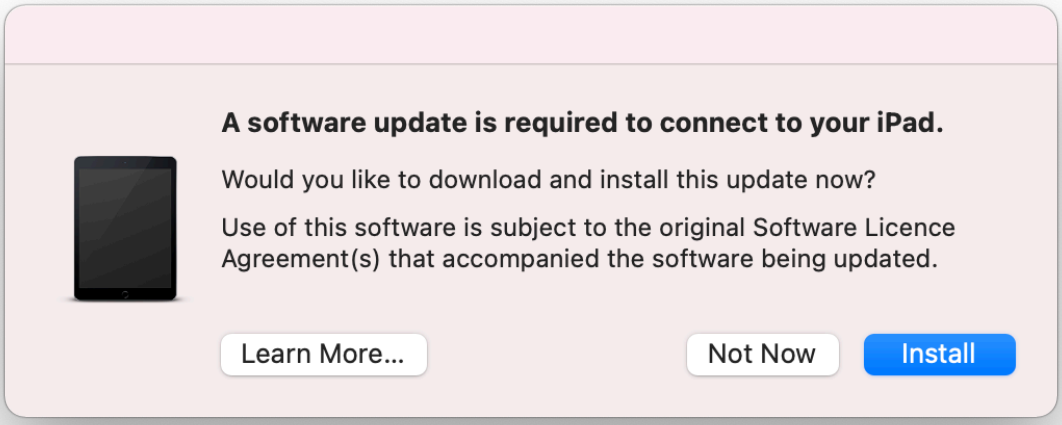


This message appears when macOS must download and install an update of the MobileDevice framework to restore a brand-new version of iOS or iPadOS on a connected device.

There are two ways to update the framework : using a device or using Xcode.

• **Using a device**

Manually update a device to the latest available version of iOS or iPadOS, then connect this device to the Mac host.

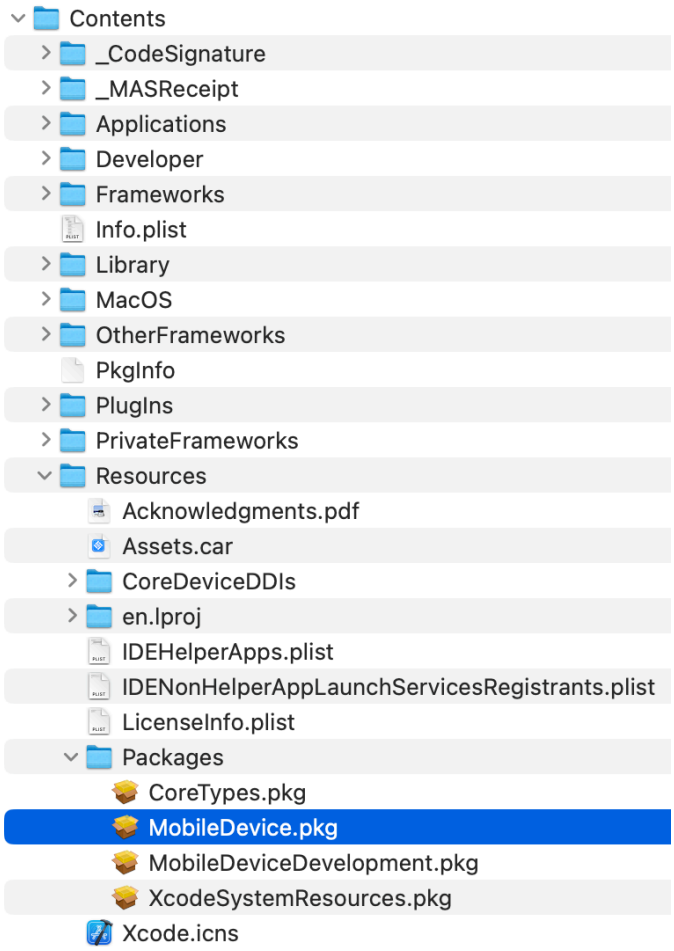


Proceed to the installation so the MobileDevice framework is updated.

• **Using Xcode**

Update a Mac to the latest available version of macOS then install or update Xcode to its latest available version.

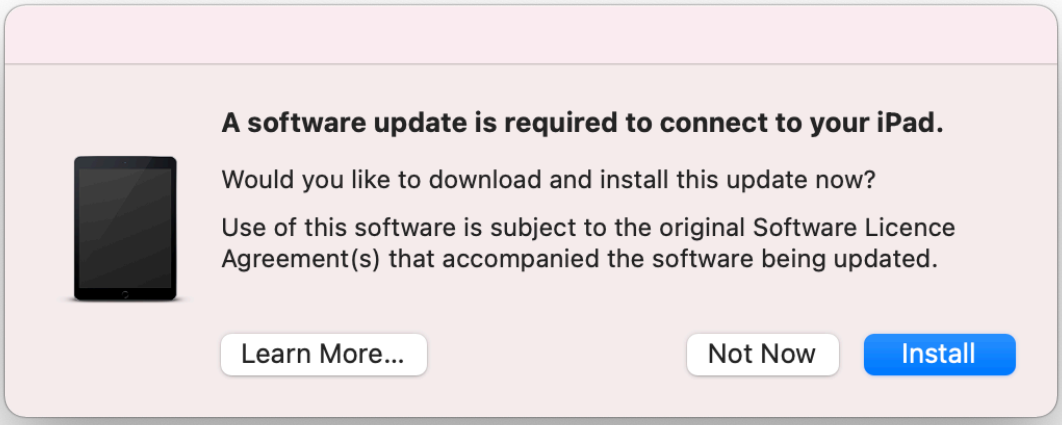
Right-click on the Xcode application then select Show Package Contents.



Open Contents > Resources > Packages then identify the package named MobileDevice.pkg.

Deploy this package on all Mac hosts running Telepod.

Required Software Update



This message appears when macOS must download and install an update for the Mac to communicate with the connected device. Without the required update, Telepod cannot detect the connected device and considers that no device is connected.

The software to be installed updates macOS and does not change the Operating System version of the connected device. Once the update is installed, the communication between the Mac and the device can be established and the Telepod workflow can proceed.

Location of downloaded OS Firmwares

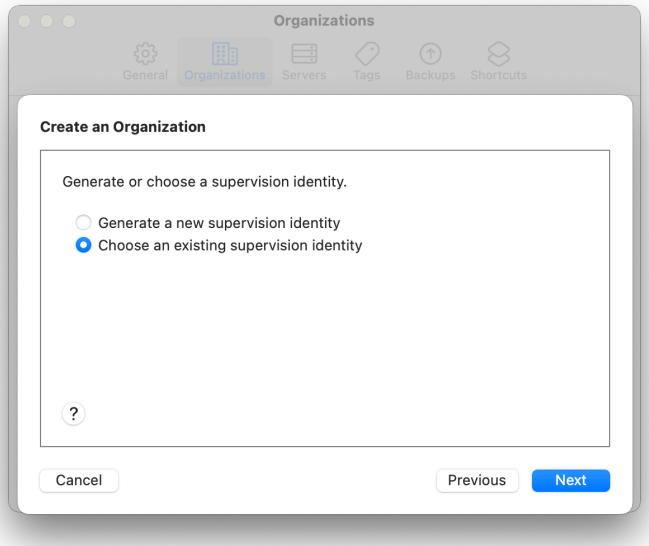
The OS Firmwares downloaded by Telepod to upgrade devices are stored in the following path :

```
/private/var/root/Library/Group Containers/
K36BKF7T3D.group.com.apple.configurator/Library/Caches/Firmware
```

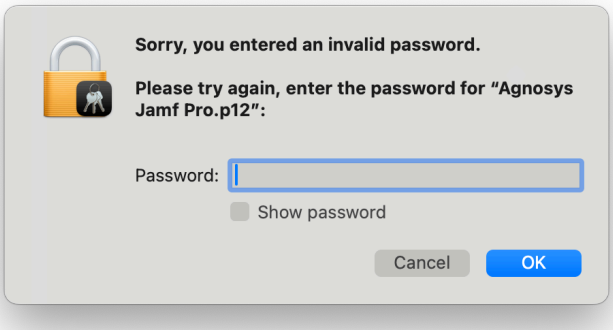
Please note that **they are not stored** in the Library of the user from whose session Telepod is running.

Jamf Pro - Error when importing Jamf Pro Supervision identity into Keychain

This section only applies if the management solution is Jamf Pro.



When creating an Organization in Apple Configurator, the option to use an existing Supervision identity is offered. This must then be selected from a list of identities stored in the keychain.



When importing a Jamf Pro Supervision identity into the Keychain so that Apple Configurator can offer it, a message may continue to appear indicating that the password entered is incorrect, when in fact it is.

To overcome this problem, execute the script titled "telepod_supervision_identity_jamf_pro_converter.command" provided in the subfolder "telepod_library" of the Telepod Toolkit. To easily obtain the "pathname to Jamf Pro Supervision Identity", right-click on the PKCS#12 (P12) file exported from Jamf Pro, then hold down the Option key to reveal the "Copy (item name) as Pathname" action and select it. Then position the cursor where the pathname is awaited and go to Edit > Paste. Once the pathname is displayed, press the Return key. Follow the displayed instructions. When you are asked to enter an "Export password", choose any of your choice. The Keystore written to /Users/Shared/keystore.p12 can be imported into the macOS Keychain using the chosen password.

Once imported in the Keychain, the Supervision identity can be selected in Apple Configurator.

Jamf Pro - Error Code 4001 when enrolling a device using Device Enrollment

This section only applies if the management solution is Jamf Pro.

The error code 4001 appears in the device’s setup log as follows :

```
cfgutil: error: Profile Installation Failed
(Domain: MCInstallationErrorDomain Code: 4001)
```

This error occurs when a device previously enrolled through Automated Device Enrollment is attempted to be enrolled again using Device Enrollment by Telepod, a scenario likely to happen only during testing.

To overcome this problem, delete the device from Jamf Pro before running the workflow.

Microsoft Intune - Solve a non-reinstallation issue

This section only applies if the management solution is Microsoft Intune.

To help the MDM determine that the Telepod-Core package and/or the Telepod-Content package have been successfully installed so these last are not reinstalled in loop at each sync, Telepod includes two detection apps :
- /Library/Application Support/Telepod/Core/Telepod-Core.app
- /Library/Application Support/Telepod/Content/Telepod-Content.app.

The side effect of their presence is that they may prevent a reinstallation of these packages.

To solve this issue, open the Terminal utility located in /Applications/Utilities, type one of the following command depending of the package to be reinstalled and enter your password when prompted.

```
sudo rm -Rf "/Library/Application Support/Telepod/Core/Telepod-Core.app"
```

```
sudo rm -Rf "/Library/Application Support/Telepod/Content/Telepod-Content.app"
```

Then trigger an MDM sync to reinstall the targeted package(s).

Support

Paid support included in Telepod offers

Send your support request to telepod.support@agnosys.fr

Support is delivered by email in English and French.

Support is opened Monday to Friday 10:00-17:00 Time Zone Europe/Paris.

The first callback is targeted to be done within 4 hours after the reception of the support request.

Free community support

Join our Slack channel at https://macadmins.slack.com/archives/C03V4MQRRV0

The free support is offered as time permits for basic cases, bug report studies and feature request discussions.

The community is encouraged to help the other adopters and share its findings.

Telepod announcements and public release notes, which are a summary of the release notes, are published in the Slack channel.

Release notes

The release notes are available in the Dropbox folder where the software is available for download. They contain a detailed log of the changes introduced with the different released versions and the one in development.