MacOnboardingMate

Integration Guide

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

Introduction

MacOnboardingMate (MOM) is a wizard designed to streamline Mac onboarding into a Mobile Device Management (MDM) solution or to orchestrate its migration between MDMs, all under the remote supervision of IT support.

MOM provisioning over the Setup Assistant or Login Window allows a Mac to be onboarded even before the user's first session is opened. Key integrations with Installomator and Homebrew ensure that the latest software versions are installed during onboarding, while mSCP helps IT support improve security posture and assess a Mac's compliance score before it is assigned to a user. Slack and Teams integrations provide real-time visibility during workflows.

A MOM Setup license allows a Mac to be onboarded either from an existing user session or the Setup Assistant. In the first scenario, the Mac is already in production and enrolled in the MDM using Device Enrollment or Automated Device Enrollment. In the second, the Mac is new or reset and enrolled using Automated Device Enrollment.

A MOM Switch license enables a Mac to be migrated from an active user session and enrolled in a new MDM using Device Enrollment or Automated Device Enrollment. This critical process is central to any MDM migration project, requiring migrated devices to retain their Automated Device Enrollment configuration when applicable. The MOM Switch license also includes all the features of the MOM Setup license.

MOM operates in two execution modes to run these workflows. The Launcher mode is used when MOM is run manually outside of an MDM. In contrast, AutoLauncher is used when MOM runs from an MDM, either automatically or manually via Self Service. For example, when a Mac is migrated between MDMs, MOM is executed from the original MDM using the AutoLauncher mode.

MOM is multilingual, currently localized in English and French, with translations easily built from a template to support users' preferred languages. MOM is a turnkey solution requiring no scripting knowledge for implementation or upgrades. If needed, MOM can be extended with custom scripts executed at key workflow stages.

References

Before reading this documentation, please consult the following references.

• Introduction

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

• Management solutions support

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

• Capabilities

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

• Offers and pricing

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

Terminology

Provisioning “Over the Setup Assistant” : the onboarding occurs during the Setup Assistant, with MOM overlaying its interface.

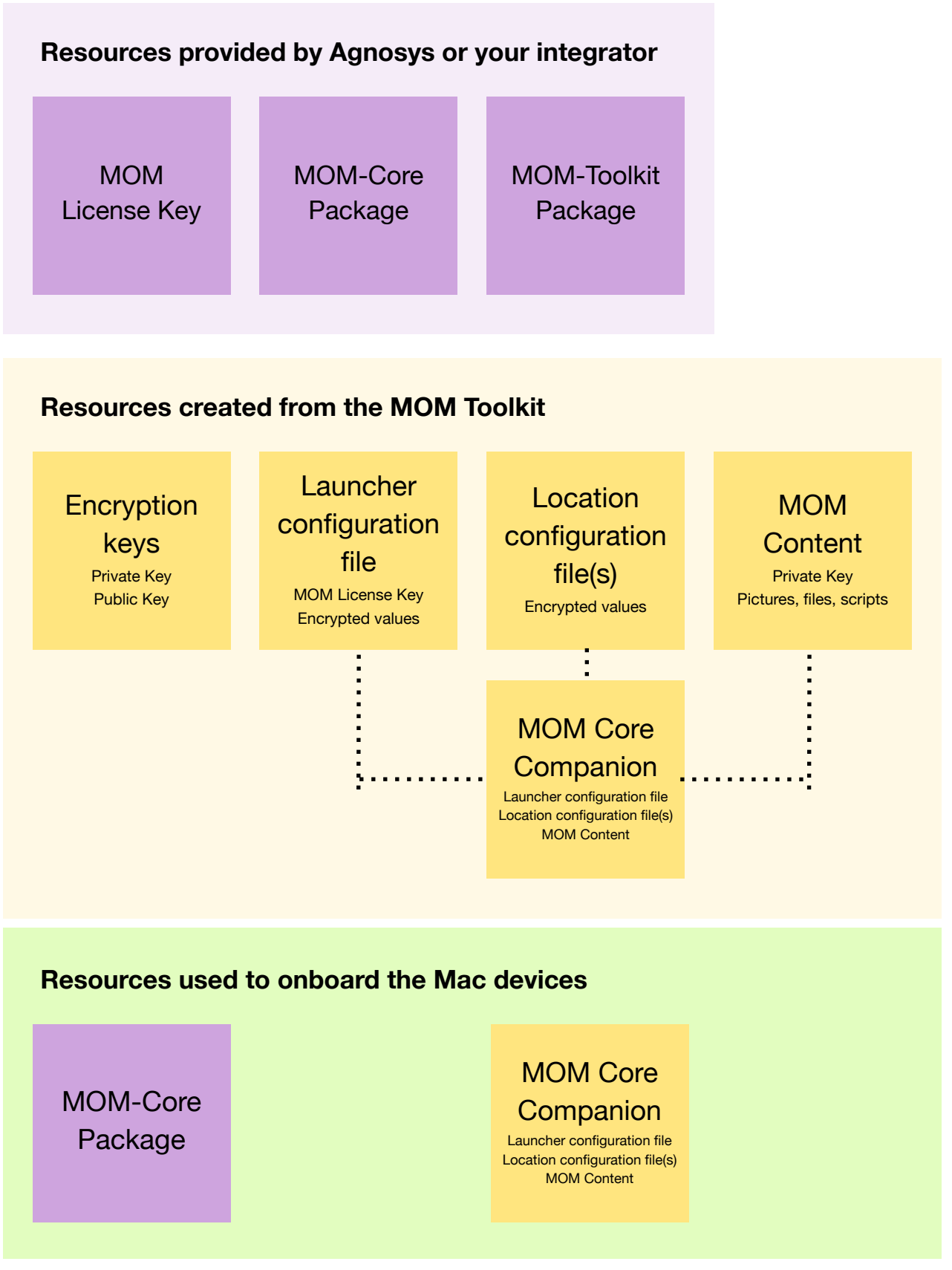
Provisioning “Over the Login Window” : the onboarding occurs during the Login Window, with MOM overlaying its interface.

Provisioning “Over the Desktop” : the onboarding occurs over the Desktop of the first logged-in user.

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

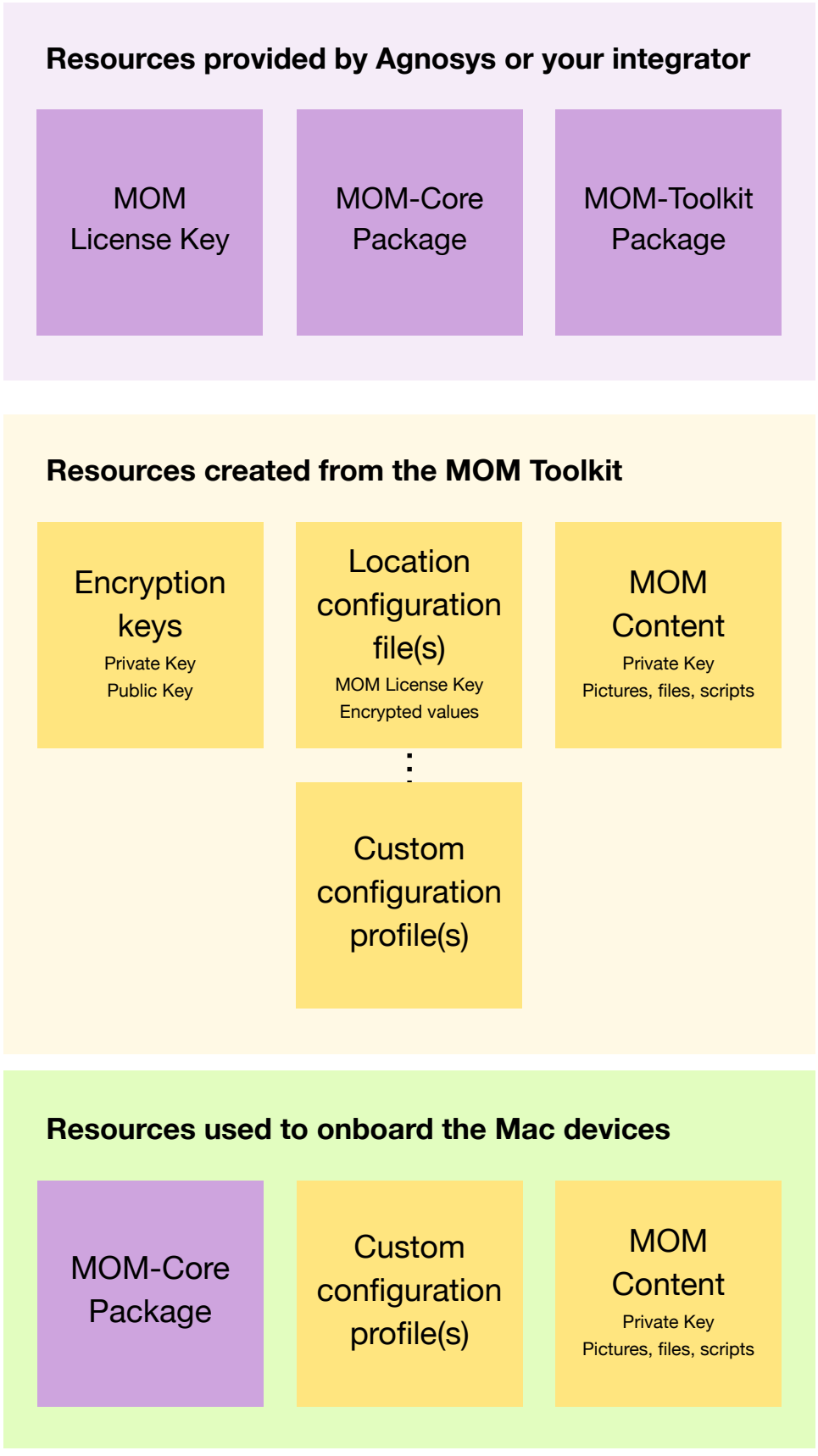
Synopsis

Implementing Launcher mode



Step	Chapter in this document
Get a MacOnboardingMate License Key	Software requirements
Download the MOM-Core Package	
Download the MOM-Toolkit Package	
Install the Packages app	
Install a Property List editor	
Install the MOM-Toolkit	MOM Toolkit installation
Create the encryption keys	Encryption keys creation
Customize the Launcher configuration file	Launcher configuration file edition
Customize the Location configuration file	Location configuration files edition
Create other Location configuration files if necessary	
Build (and sign) the MOM-Content package	MOM Content building
Embed the resources in the MOM-Core-Companion disk image	MOM Core Companion building
Provision the MDM with required configuration profiles	Configuration profiles requirements
Onboard your first Mac	Onboarding a Mac using MOM in Launcher mode
Enable logging and display logs	Troubleshooting
Reset the safeguards	

Implementing AutoLauncher mode



Step	Chapter in this document
Get a MacOnboardingMate License Key	Software requirements
Download the MOM-Core Package	
Download the MOM-Toolkit Package	
Install the Packages app	
Install a Property List editor	
Install the MOM-Toolkit	MOM Toolkit installation
Create the encryption keys	Encryption keys creation
Customize the Location configuration file	Location configuration files edition
Create other Location configuration files if necessary	
Convert Location configuration files to Custom configuration profiles	
Build (and sign) the MOM-Content package	MOM Content building
Provision the MDM with required configuration profiles	Configuration profiles requirements
Provision the MDM for AutoLauncher mode	Provisioning *MDM* for AutoLauncher mode
Onboard your first Mac	Onboarding a Mac using MOM in AutoLauncher mode
Enable logging and display logs	Troubleshooting
Reset the safeguards	

Known issues and limitations

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

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

Kandji

Provisioning over the Setup Assistant is not supported because this MDM does not offer to install packages aka Custom Apps until the Setup Assistant is completed.

However, provisioning over the Login Window or Desktop are available.

Homebrew integration

Homebrew integration is not supported in the context of provisioning over the Setup Assistant or Login Window when no end user account creation is planned, as Homebrew cannot be installed under the root (System Administrator) user.

In the context of provisioning over the Setup Assistant or Login Window when an end user account creation is planned, Homebrew installation is performed under this account before the user logs in. In the context of provisioning over the Desktop, Homebrew installation is performed under the logged-in account.

Software requirements

macOS

MacOnboardingMate requires macOS 10.13.4 and later.

MacOnboardingMate packages

Download (only) the following packages from this URL :

https://www.dropbox.com/sh/fucxpyi7uuahjaj/AAA8bwRDlu5zYmgxnHZGyieTa?dl=0

- MOM-Core-*version*.pkg

- MOM-Toolkit-*version*.pkg

Warning : Do not install MOM-Core on your computer.

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

MacOnboardingMate 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

If the MDM solution is VMware Workspace ONE, this documentation refers to "Sublime Text" available at this address for the opening of a Plist file :

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

VMware Workspace ONE Admin Assistant

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

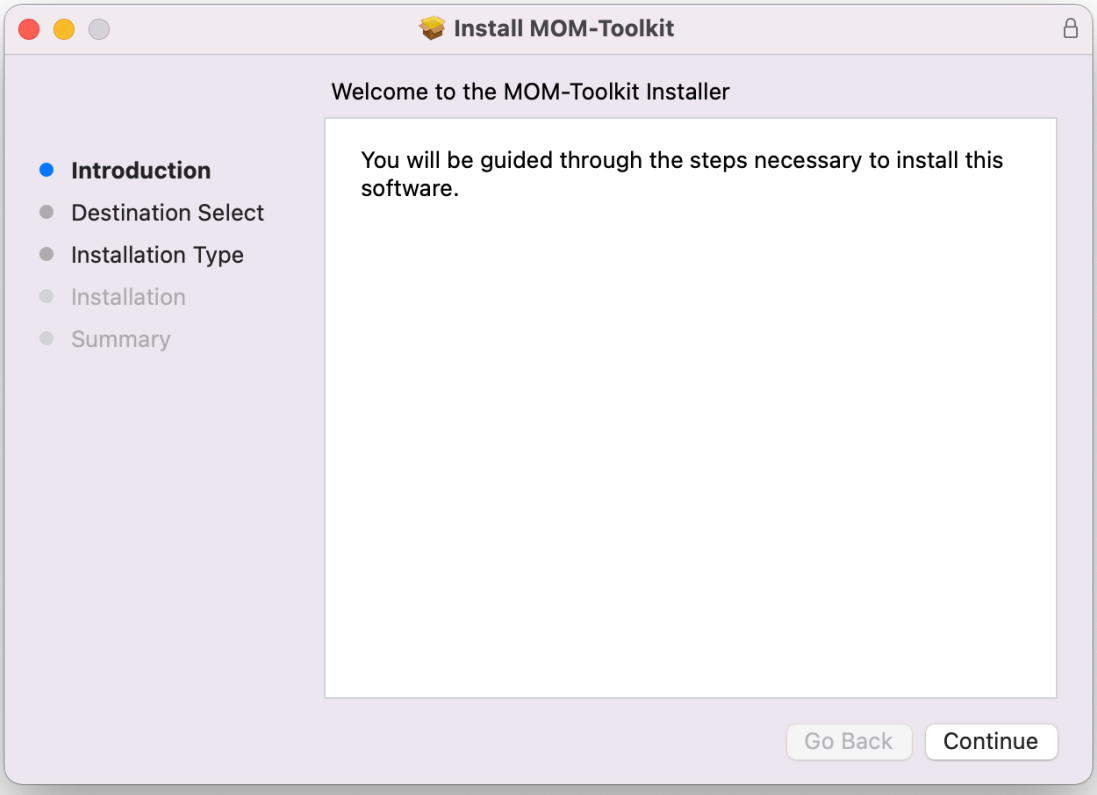
Workspace ONE Admin Assistant
https://getwsone.com/AdminAssistant/VMwareWorkspaceONEAdminAssistant.dmg

Automated Device Enrollment

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

MOM Toolkit installation

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



Enter your administrator password when prompted.

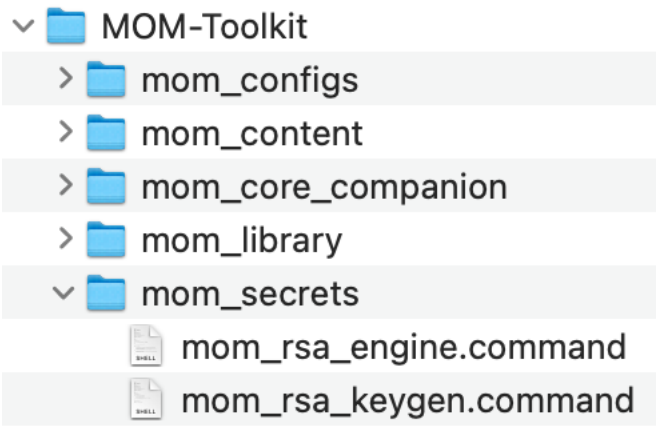
The "MOM-Toolkit" folder is created in /Users/Shared. It contains the following subfolders :
- mom_configs
- mom_content
- mom_core_companion
- mom_library
- mom_secrets

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

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

Encryption keys creation

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

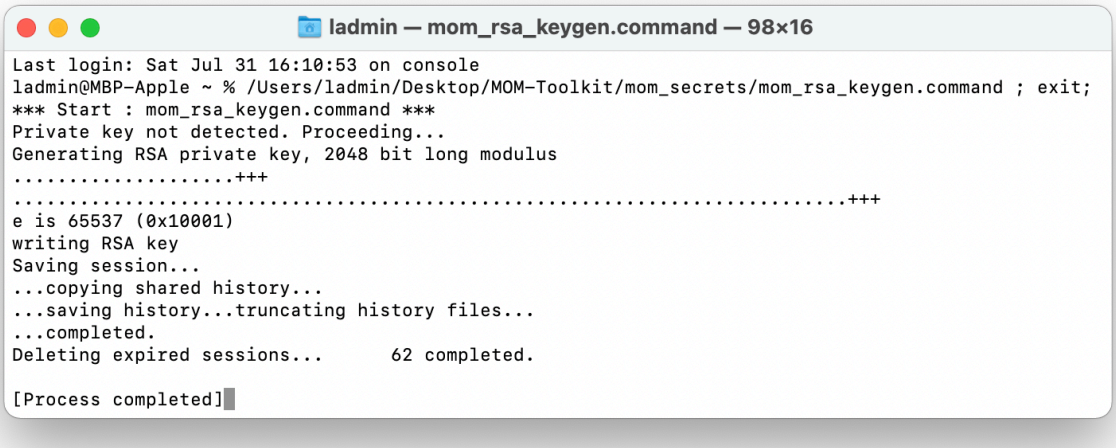


Open the "MOM-Toolkit" folder.

Open the "mom_secrets" subfolder.

Execute the "mom_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 MacOnboardingMate integration lifetime.



The private / public key pair is created at the following path :
MOM-Toolkit > mom_secrets > mom_rsa_key.pri and mom_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 MOM-Content package (Launcher and AutoLauncher modes)
- generate a new MOM-Core-Companion disk image (Launcher mode only).

The private key is automatically copied at the following path :
MOM-Toolkit > mom_content > Content > mom_rsa_key.pri

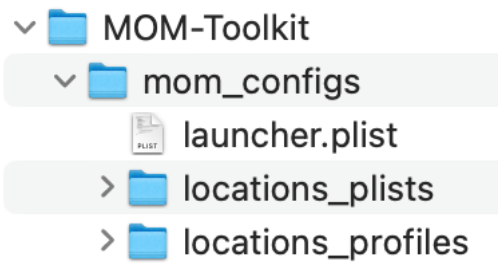
If you delete the private key at this path, execute the script again. It will copy again the existing private key.

Launcher configuration file edition

This section only applies to Launcher mode.

The Launcher configuration file is eventually embedded in the MOM-Core-Companion disk image.

Access to the configuration file template

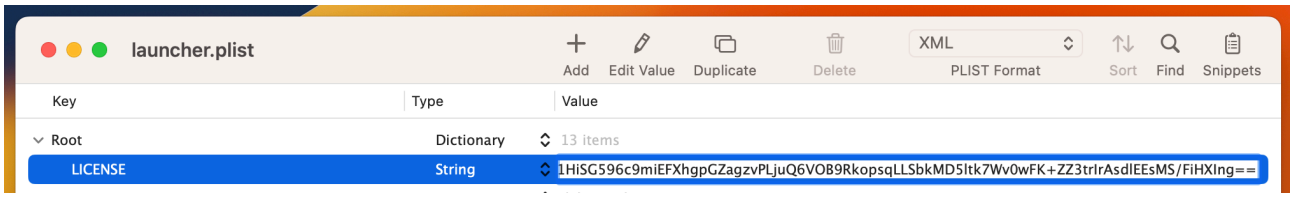


Open the "MOM-Toolkit" folder.

Open the "mom_configs" subfolder.

Open the "launcher.plist" property list with you favorite editor.

License key



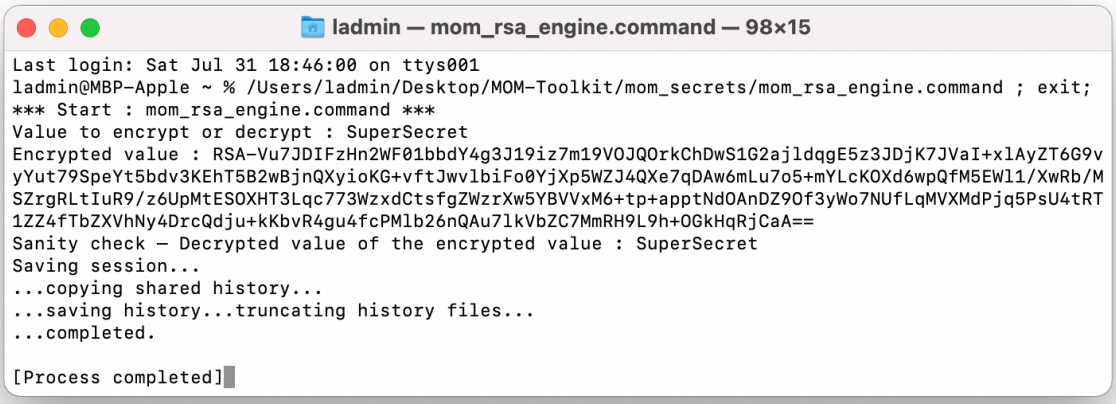
Paste the MOM Setup or MOM Switch license key in the LICENSE key.

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

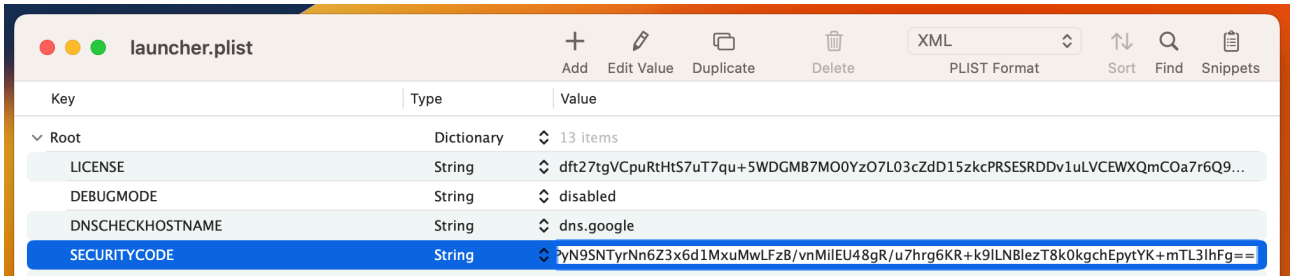
Security code

The security code is an encrypted version of the password used to protect the MOM-Core-Companion disk image from an unauthorized access.

To generate the security code, follow these instructions :
- open the "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_rsa_engine" script (double-click on the .command file)
- enter the complex password of your choice



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



Paste the encrypted password in the SECURITYCODE key.

Reference for configuration file keys

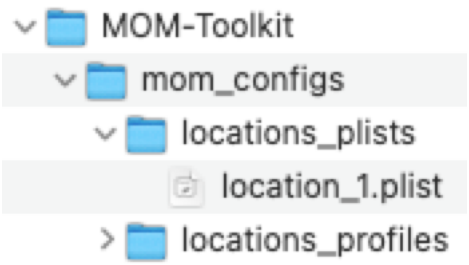
Please open the MOM Dictionary, whose filename is "3. MOM_Dictionary.pdf", and consult the sheet titled "launcher.plist" to learn how to customize the other keys.

Location configuration files edition

At least one Location configuration file is required.

In the context of Launcher mode, the Location configuration file(s) :
- is/are referenced in the Launcher configuration file
- is/are eventually embedded in the MOM-Core-Companion disk image.

Access to the configuration file template



Open the "MOM-Toolkit" folder.

Open the "mom_configs" subfolder.

Open the "locations_plists" subfolder.

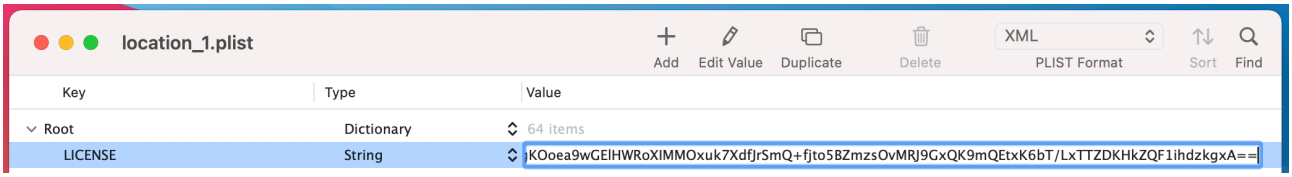
Open the "location_1.plist" property list with you favorite editor.

Reference for configuration file keys

Please open the MOM Dictionary, whose filename is "3. MOM_Dictionary.pdf", and consult the sheet titled "location1_plist" to learn how to customize the keys.

At the end of the table are listed the keys that are used only in the context of a migration that requires a MOM Switch license.

License key



This section only applies to AutoLauncher mode.

Paste the MOM Setup or MOM Switch license key in the LICENSE key.

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

Password complexity

If a local account password policy has been defined to meet your organization's requirements, please pay attention to the following point.

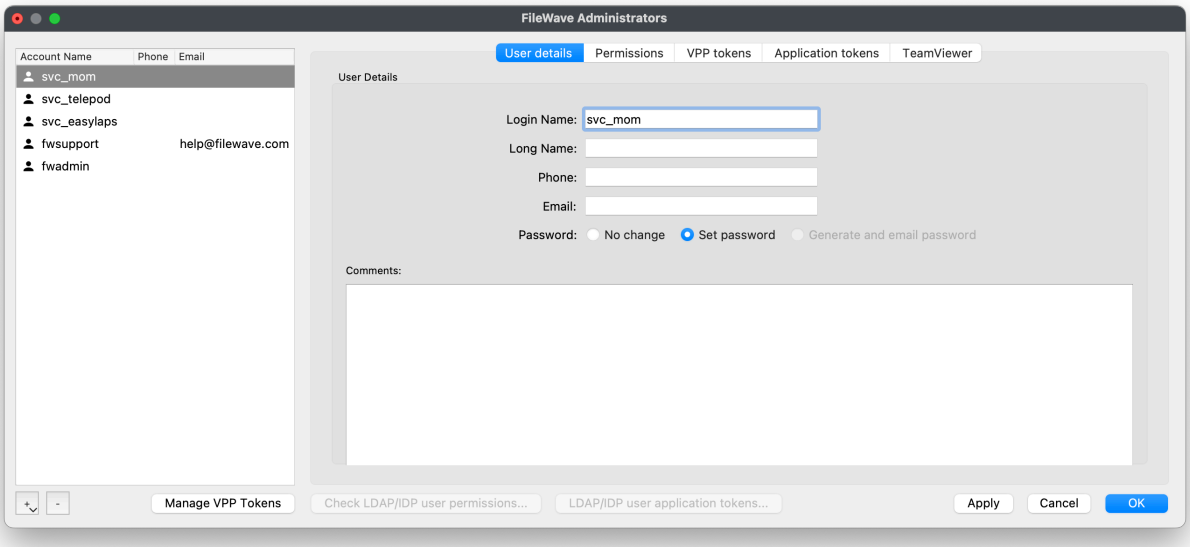
MOM creates the management account defined in the configuration file if it is detected as missing at the time the workflow is executed. In this context, the password of the management account is the password defined in the MGTACCOUNTPASSWORD key. **This password must therefore comply with the local account password policy.** In case this compliance is not respected, the management account creation will fail and be skipped.

FileWave : APIAUTHENTICATIONSTRING key

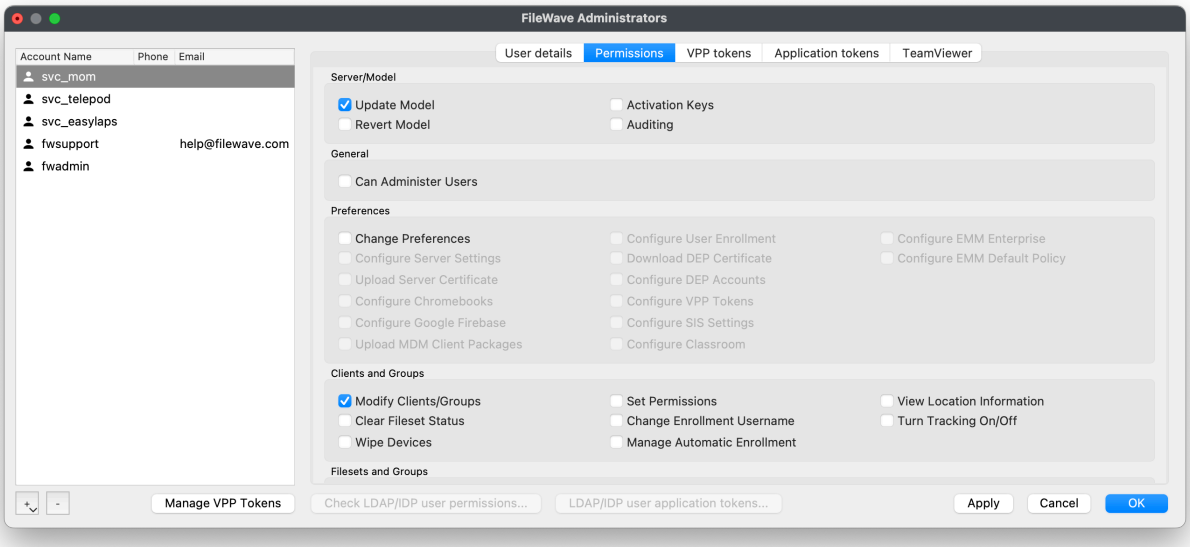
This section only applies if the management solution is FileWave.

First create a new administrator that will be used by MacOnboardingMate 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.



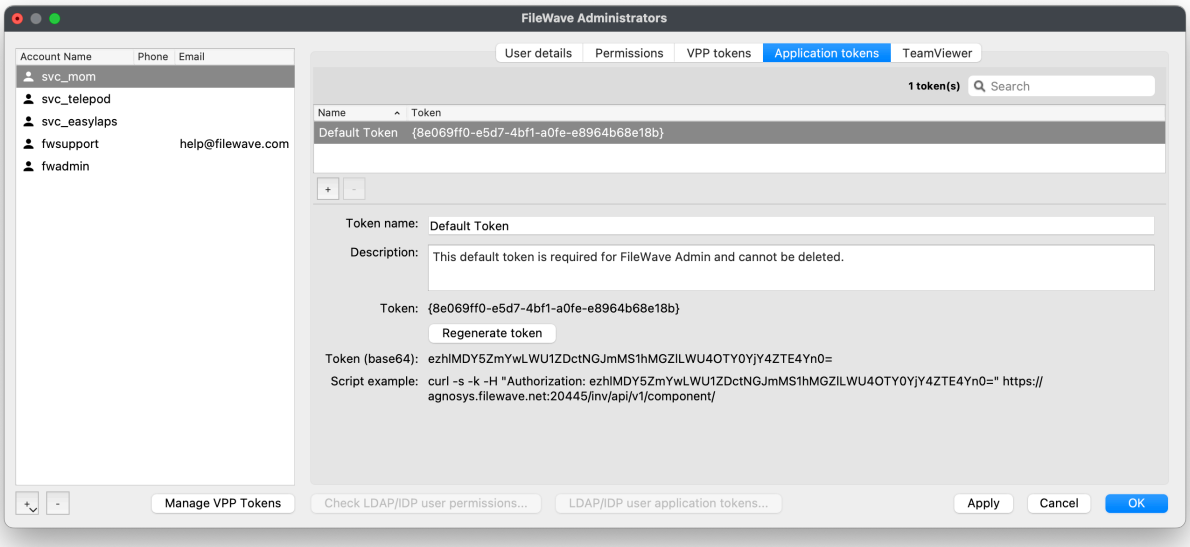
Select "Permissions".

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

To allow MOM to make an API call to remotely unenroll a device which Remote Management Profile is locked (option for Automated Device Enrollment), the account 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 MOM is deployed. However, MOM 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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).

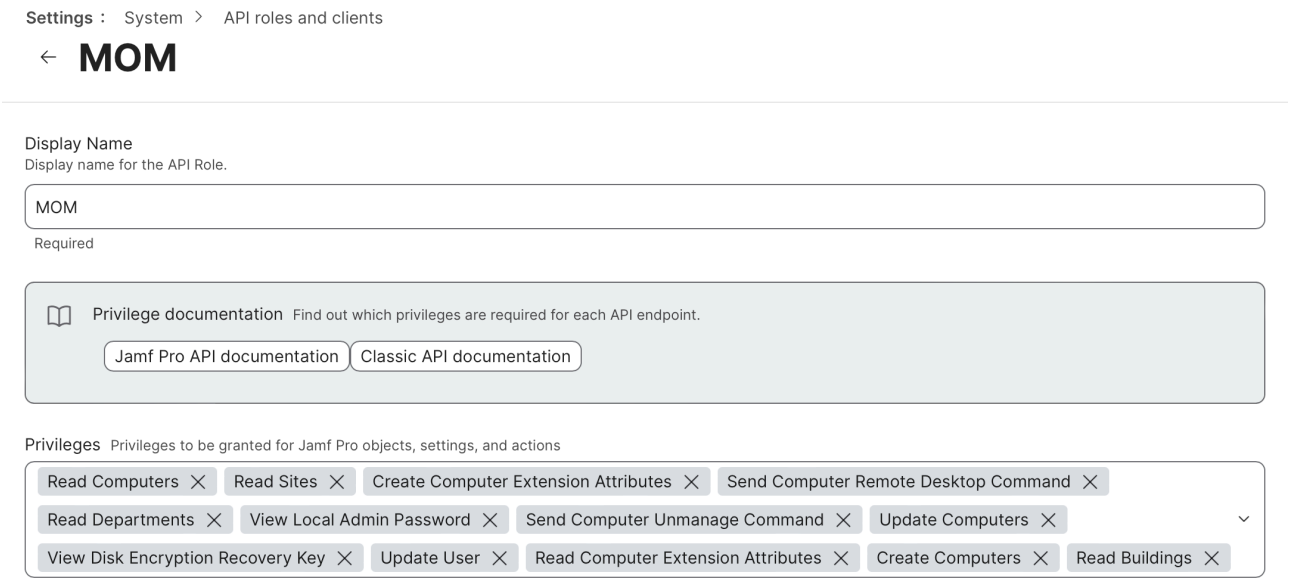
The key will be used by MacOnboardingMate to make API calls.

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 "MOM".

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

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

- Read Computers

- Update Computers

- Update User

- Assign Users to Computers
  (**not proven** to be required)

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

To allow MOM to make an API call to remotely enable Remote Desktop after the service has been configured using the REMOTEMANAGEMENT key, the Role must have these supplemental privileges :

- Create Computers

- Send Computer Remote Desktop Command

To allow MOM to make an API call to remotely unenroll a device which Remote Management Profile is locked (option for Automated Device Enrollment), the Role must have these supplemental privileges :

- Create Computers

- Send Computer Unmanage Command

All computer attributes specified in the configuration file for both the contexts of an onboarding or a migration should be created manually before MOM is deployed. However, MOM can create these attributes when detected as missing if the Role has these supplemental privilege :

- Create Computer Extension Attributes

To allow MOM 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

MOM Switch only — To allow MOM to make an API call to retrieve the current FileVault Personal Recovery Key (PRK) of a device to facilitate its reissuance during a migration, the Role must have this supplemental privilege :

- View Disk Encryption Recovery Key

MOM Switch only — To allow MOM to make an API call to collect the current management account password managed by the native Jamf Pro LAPS solution and make it available to EasyLAPS via the EasyLAPS Gateway, the Role must have this supplemental privilege :

- View Local Admin Password

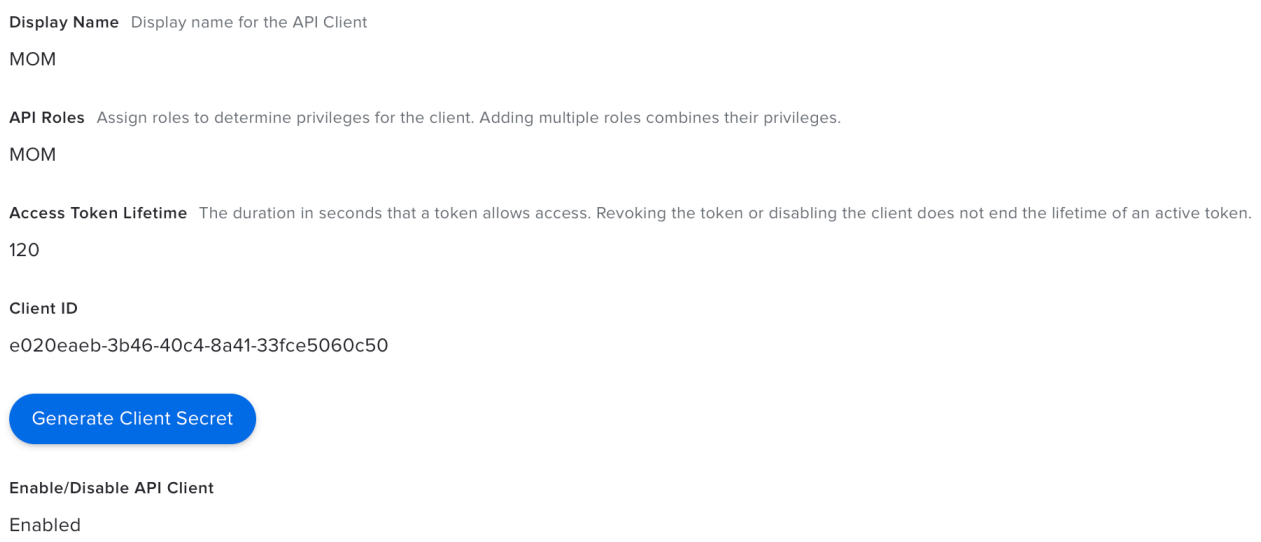
Click on "Save".

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

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

Enter a name like "MOM", select the MOM 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate to make API calls.

This account requires the following set of privileges :

- Jamf Pro Server Objects
    - Computer Extension Attributes : Read
      (**not required** if Jamf Pro API is enabled)
    - Computers : Read - Update
    - Users : Update
- Jamf Pro Server Actions
    - Assign Users to Computers
      (**not proven** to be required)

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

To allow MOM to make an API call to remotely enable Remote Desktop after the service has been configured using the REMOTEMANAGEMENT key, the account must have these supplemental privileges :

- Jamf Pro Server Objects
    - Computers : Create
- Jamf Pro Server Actions
    - Send Computer Remote Desktop Command

To allow MOM to make an API call to remotely unenroll a device which Remote Management Profile is locked (option for Automated Device Enrollment), the account must have these supplemental privileges :

- Jamf Pro Server Objects
    - Computers : Create
- Jamf Pro Server Actions
    - Send Computer Unmanage Command

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

- Jamf Pro Server Objects
    - Computer Extension Attributes : Create

To allow MOM 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

MOM Switch only — To allow MOM to make an API call to retrieve the current FileVault Personal Recovery Key (PRK) of a device to facilitate its reissuance during a migration, the account must have this supplemental privilege :

- Jamf Pro Server Actions
    - View Disk Encryption Recovery Key

MOM Switch only — To allow MOM to make an API call to collect the current management account password managed by the native Jamf Pro LAPS solution and make it available to EasyLAPS via the EasyLAPS Gateway, the account must have this supplemental privilege :

- Jamf Pro Server Actions
    - View Local Admin Password

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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate to make API calls.

Go to School > Settings > API. Click on "Add API Key" and enter "MacOnboardingMate" 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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.

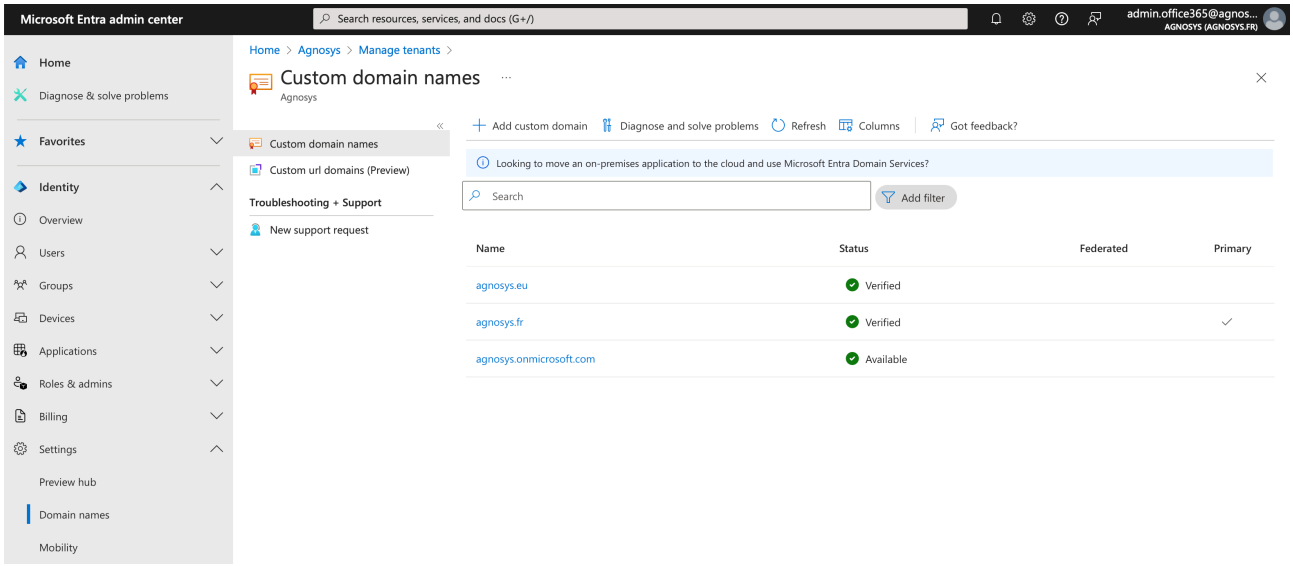
Microsoft Intune : APIAUTHENTICATIONSTRING key

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

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

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

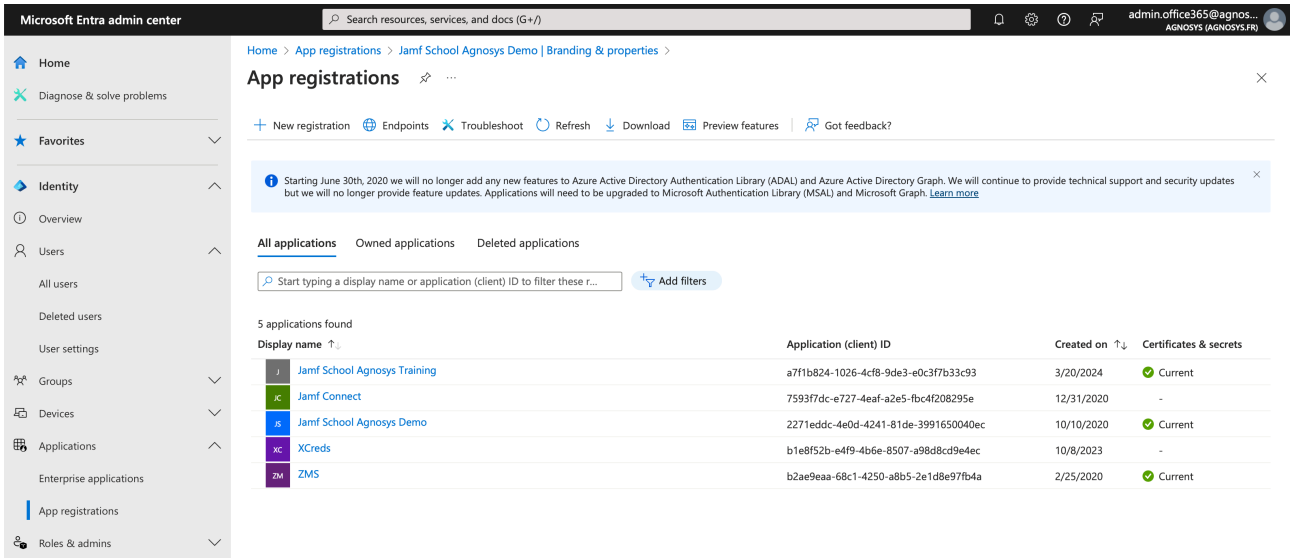
Connect to Microsoft Entra admin center.



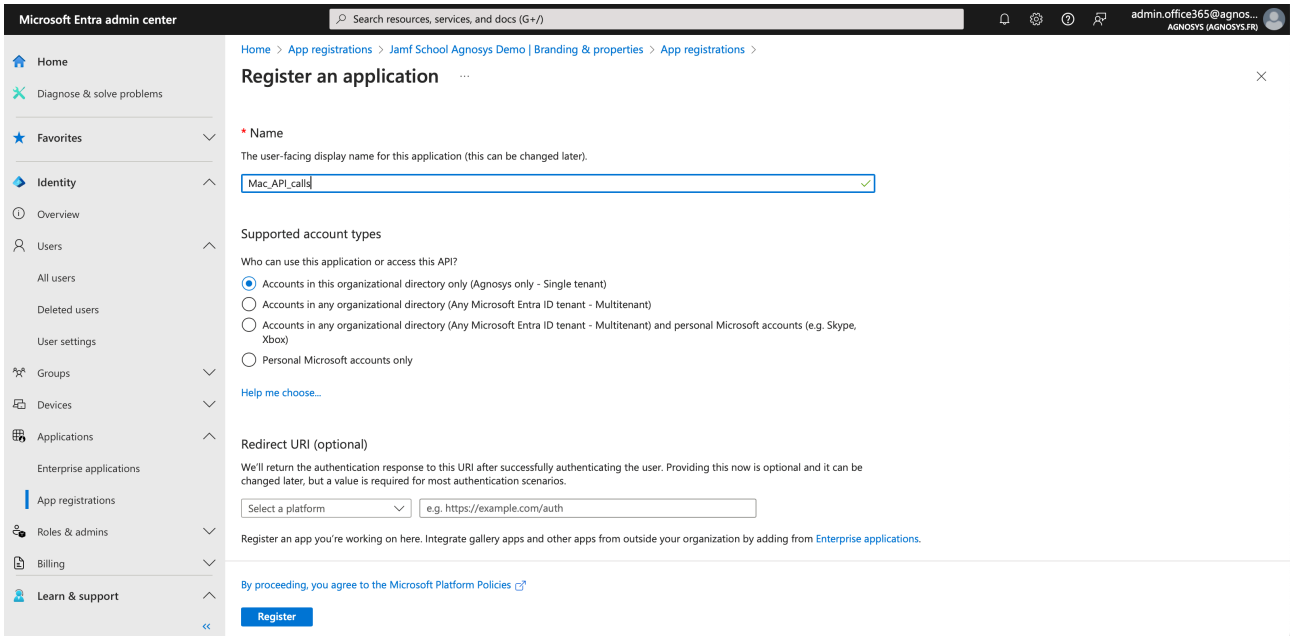
Go to Identity > Settings > Domain names.

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

Go to Identity > Applications > App registrations.



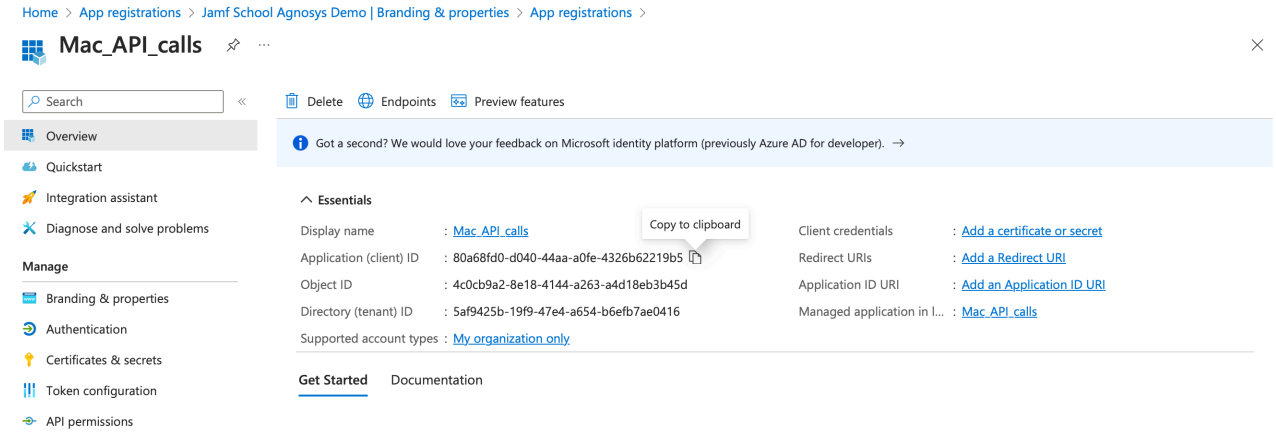
Click on "All applications", then on "New registration".



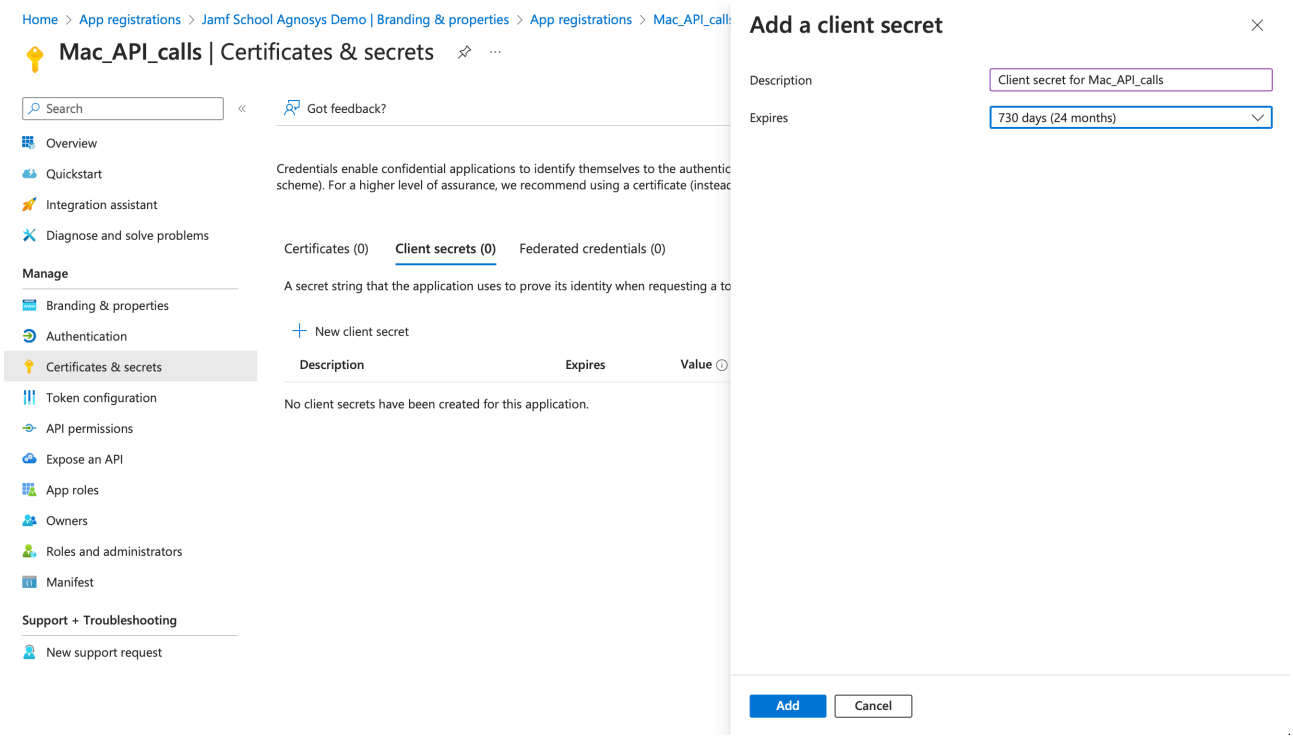
Enter a name for the application.

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

Click on "Register".



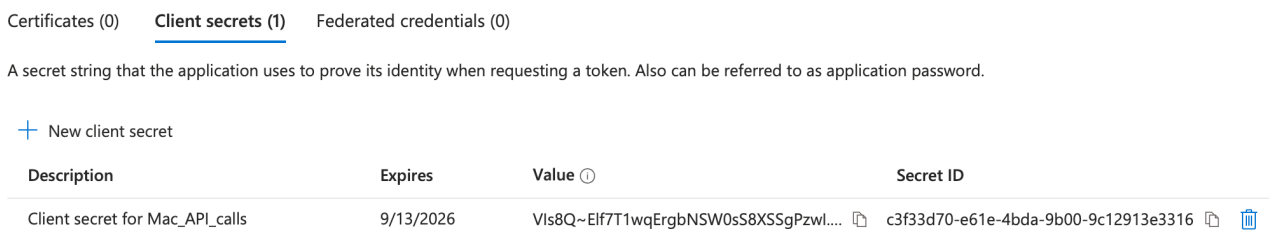
Copy / paste the Application (client) ID in the text document.



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

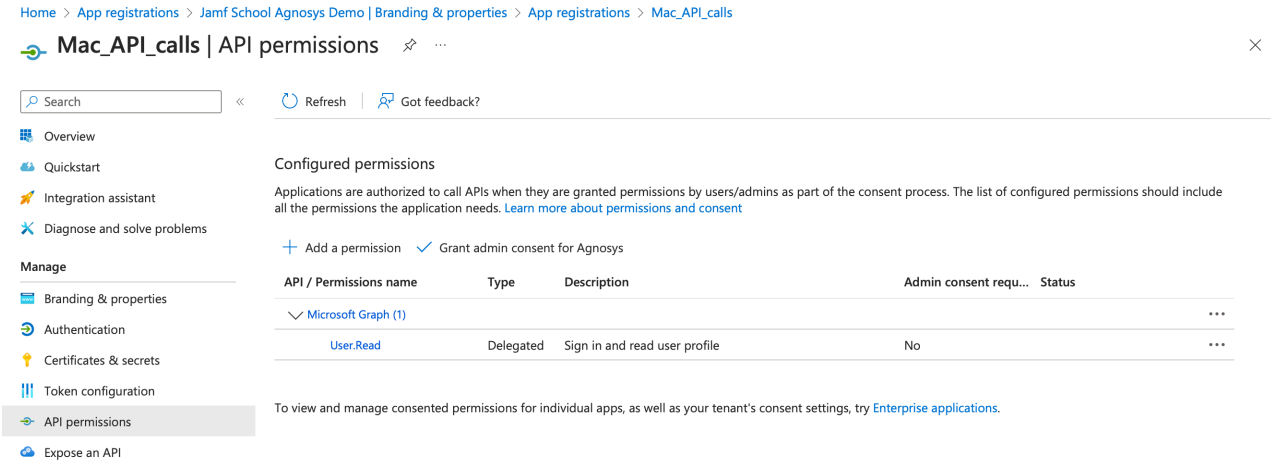
Enter a description and select a life time.

Click on "Add".

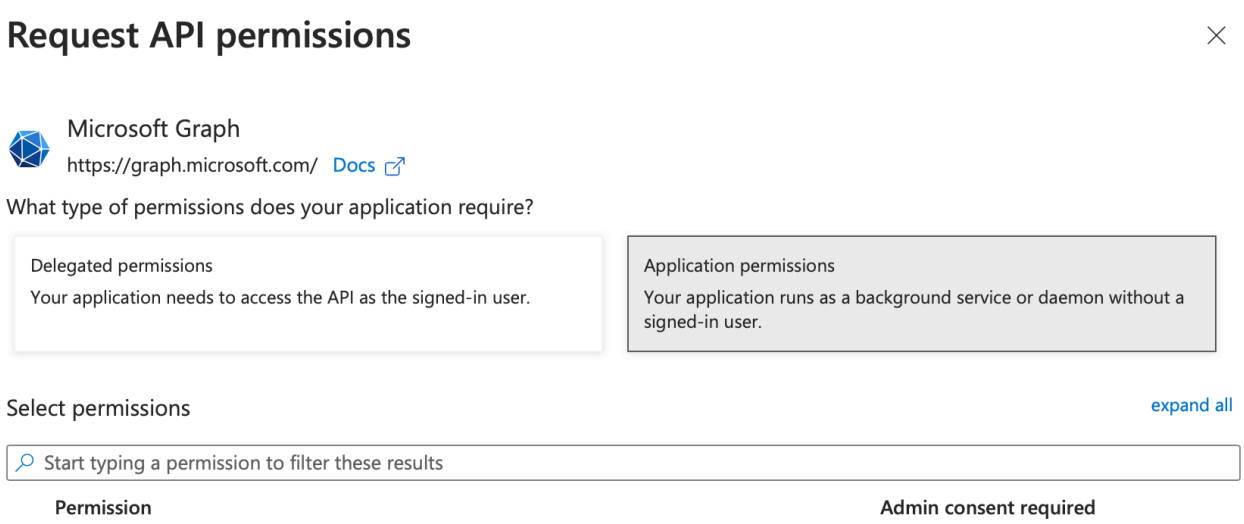


You will see this information **only once**.

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)".

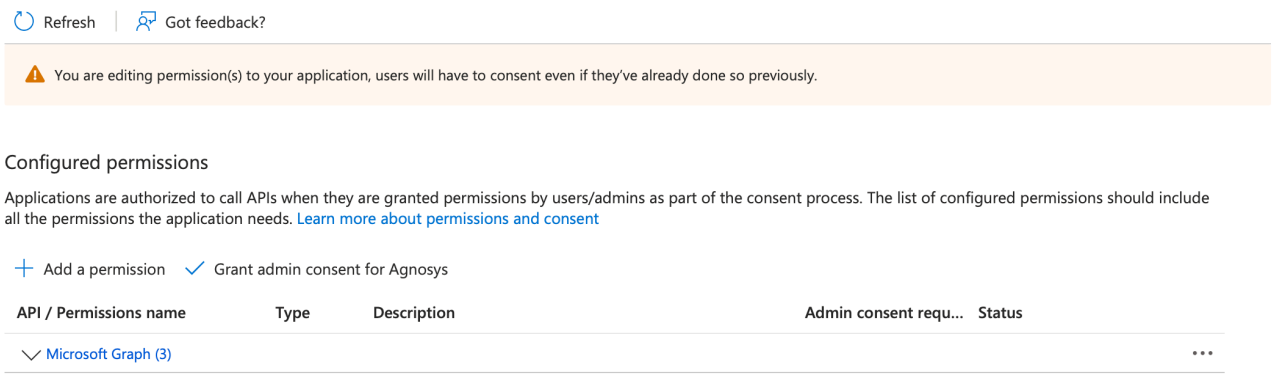


Click on "**Application permissions**".

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

If you want to authorize MOM to make an API call to remotely unenroll a device which Remote Management Profile is locked (option for Automated Device Enrollment), 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate 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 : MacOnboardingMate
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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate 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 : MOM Role
- Organization > Integrations :
    - API Integration : View - Create

All other privileges should be disabled.

Click on "Save". Back to the "Role Selector", click on "MOM Role". Check that the new administrator account is limited to the "MOM 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 "MOM 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate 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 : MOM Role
- My School > Integrations :
    - API Integration : View - Update

All other privileges should be disabled.

Click on "Save". Back to the "Role Selector", click on "MOM Role". Check that the new administrator account is limited to the "MOM 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate to make API calls.

Go to Account > API. Click on "Add API Key" and enter "MacOnboardingMate" 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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 MacOnboardingMate to make API calls.

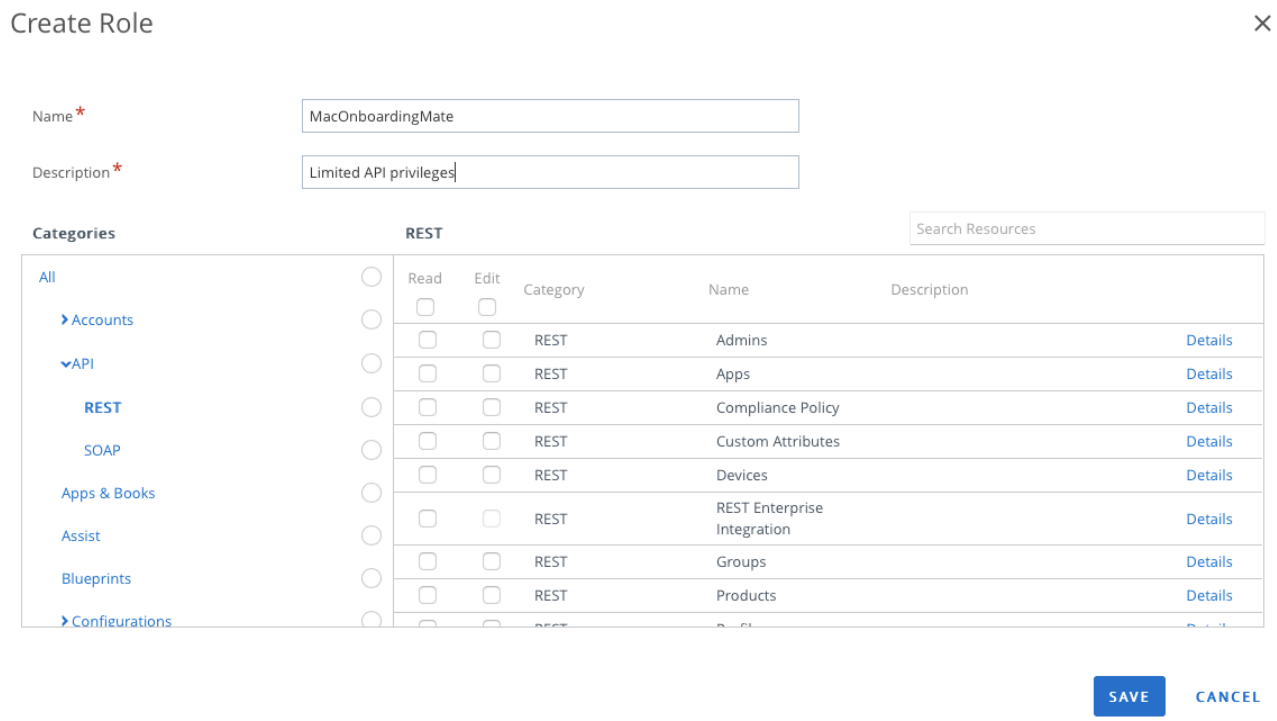
Create a new text document with 4 lines :
- Token URL :
- Client ID :
- Client Secret :

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 "MacOnboardingMate" and a description, then in the "Categories" sidebar, select All > API > REST.

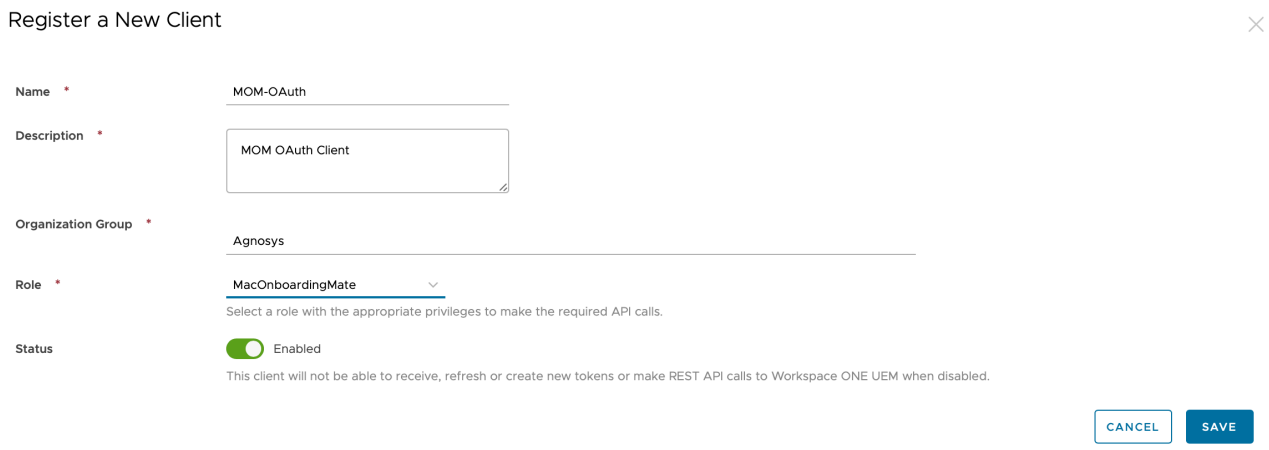
The role requires the following set of privileges :

- 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

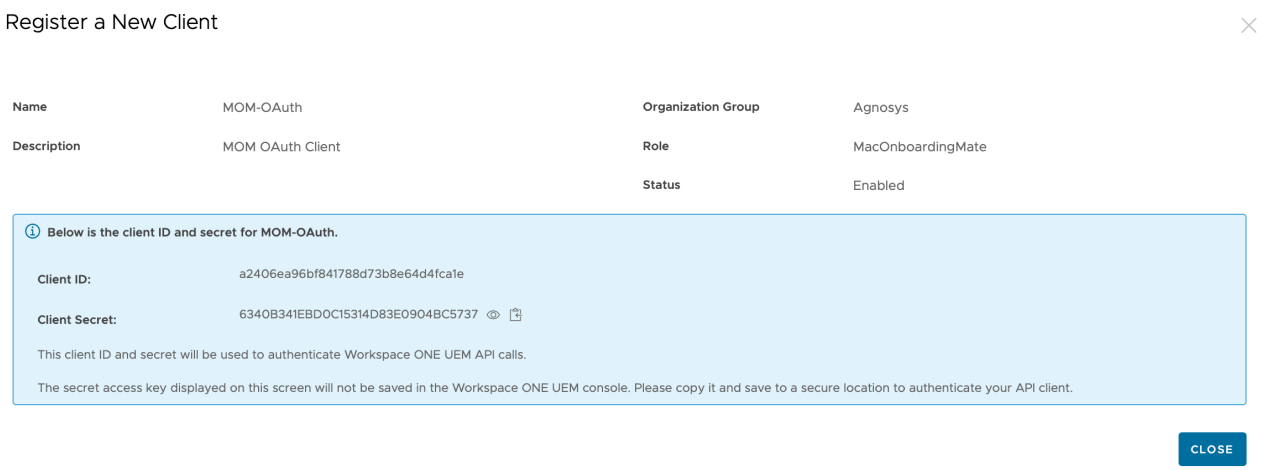
Click on "Save".

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 MacOnboardingMate then select the "MacOnboardingMate" 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 "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_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

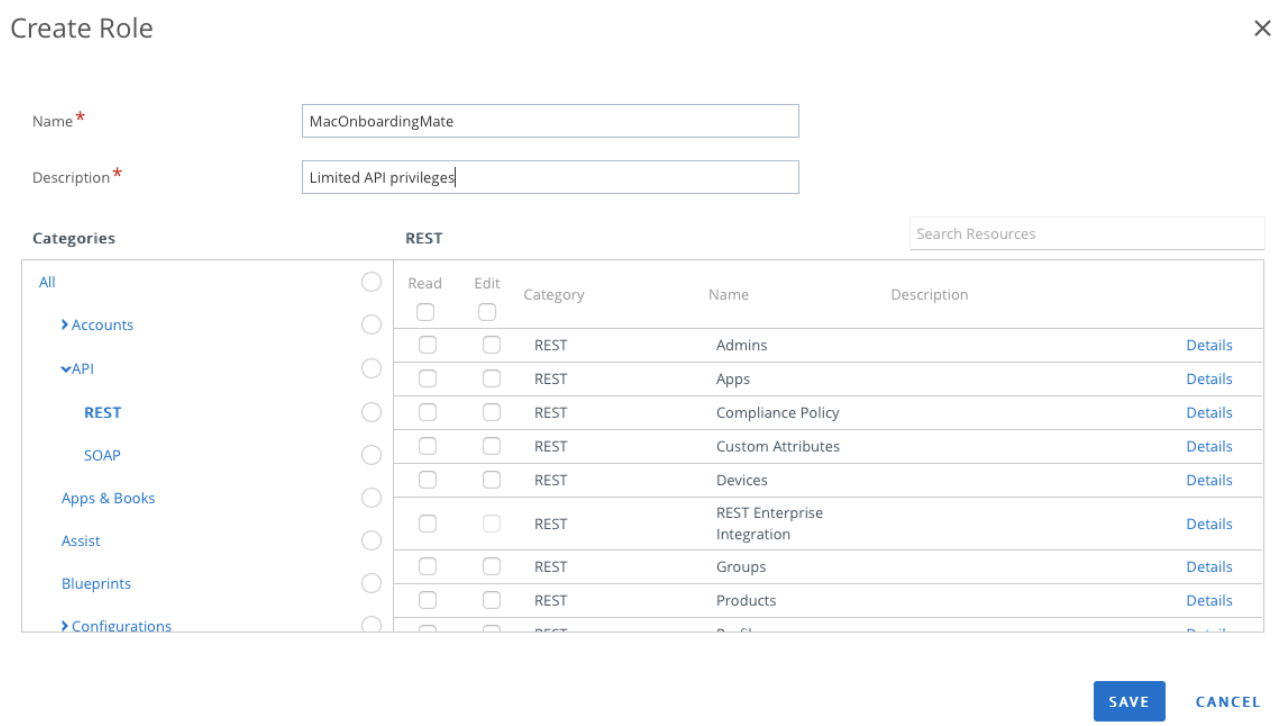
This section only applies if the management solution is VMware Workspace ONE and the authentication mechanism is Basic (not recommended).

The key will be used by MacOnboardingMate 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 "MacOnboardingMate" 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

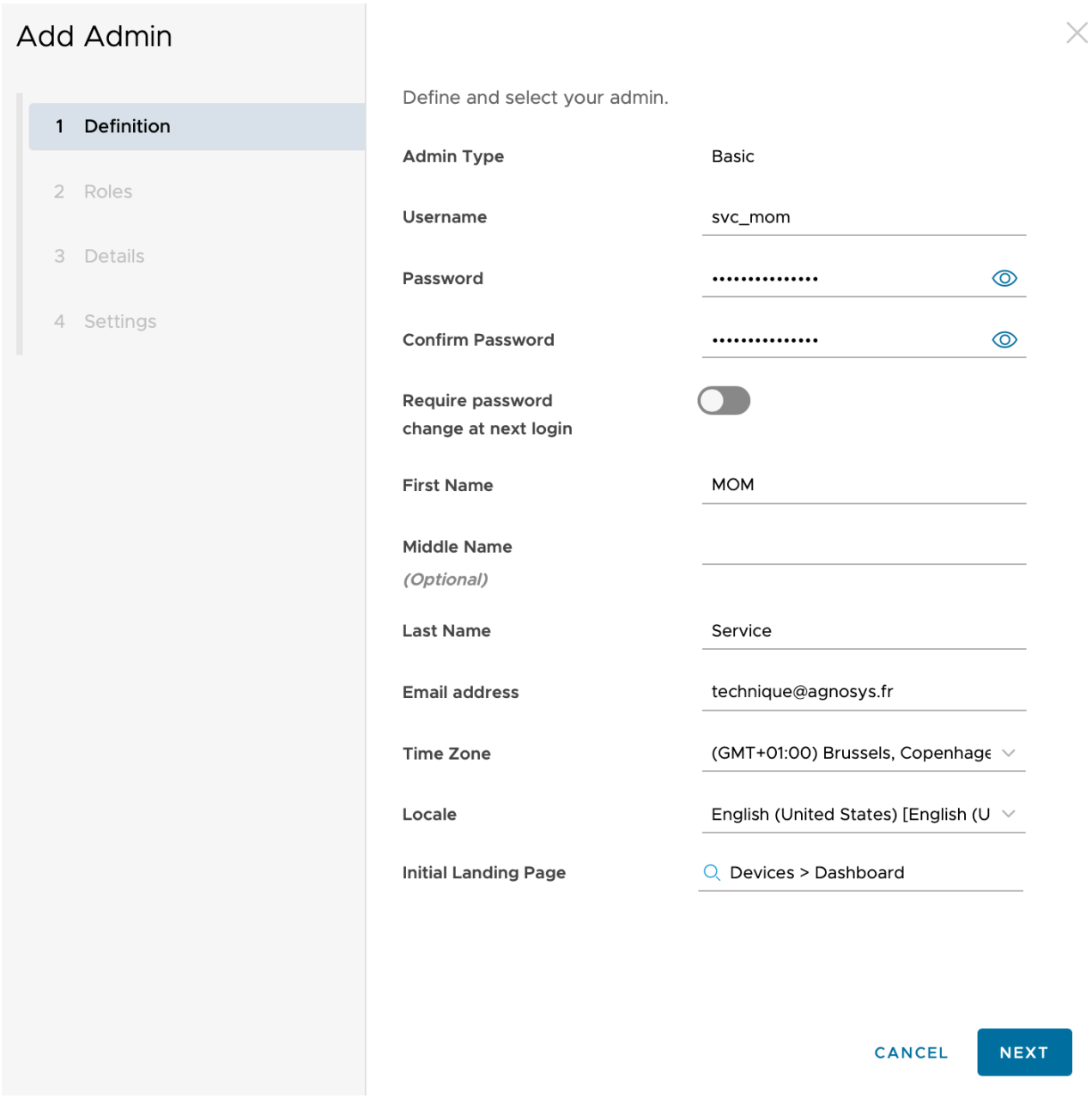
Click on "Save".

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

Go to Accounts > Administrators > List View.

Click on "Add" > "Add Admin".

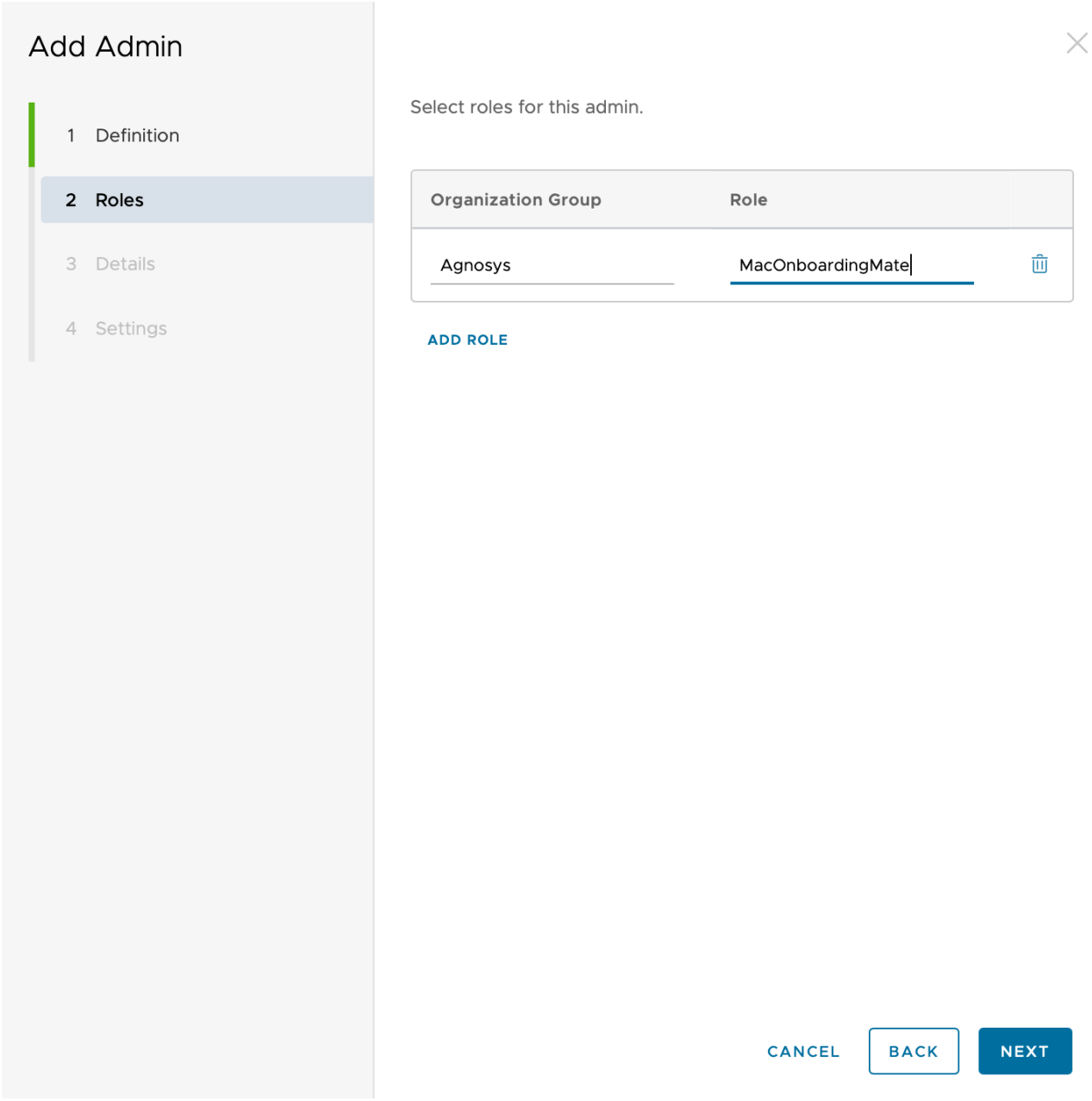
Select "Basic" then click on "Next".



Fill in the required fields.

Complete the text document with the chosen username and password.

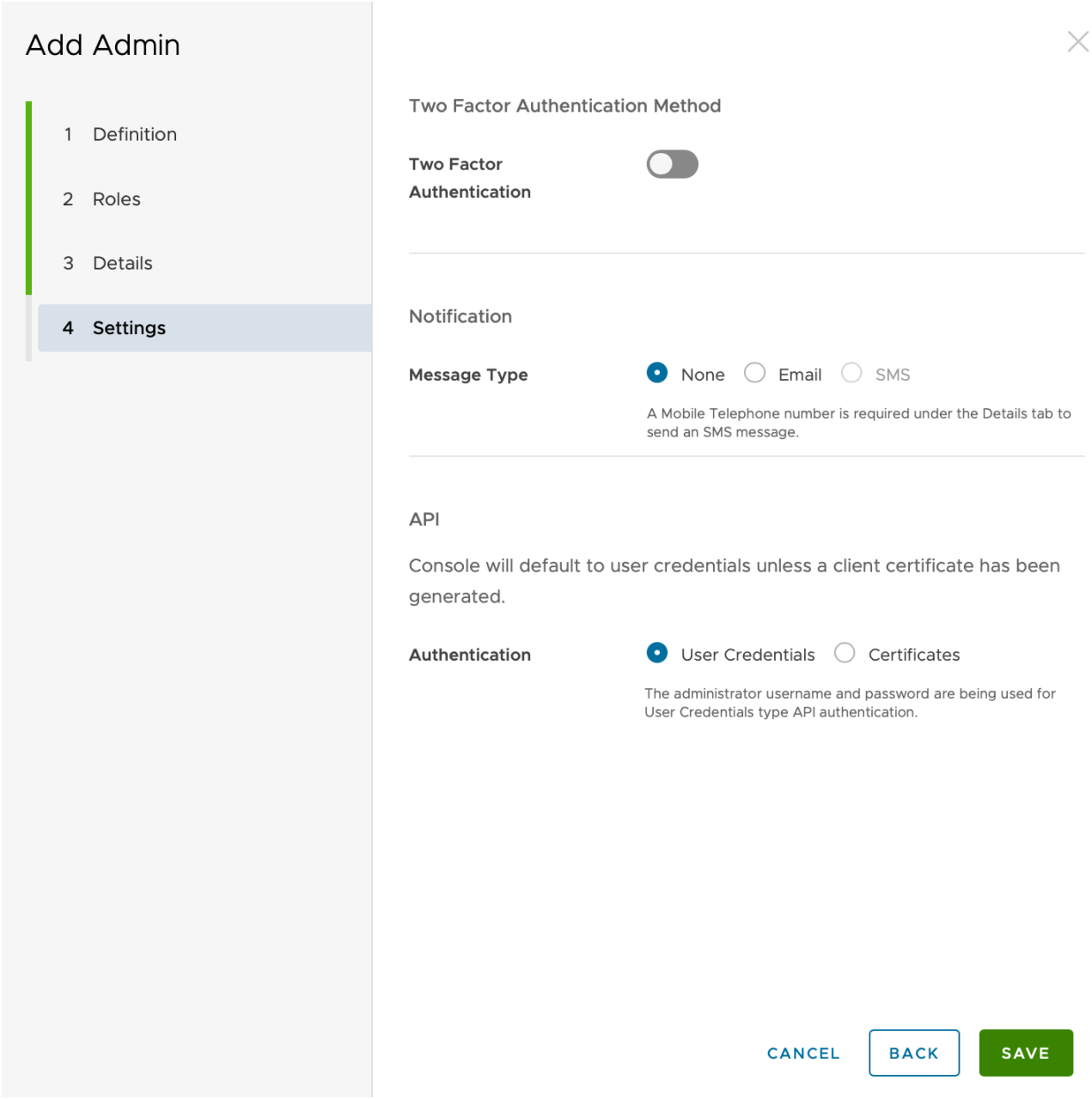
Click on "Next".



Select the Organization Group that encompasses the devices that are to be prepared with MOM, followed by the "MacOnboardingMate" role.

Click on "Next".

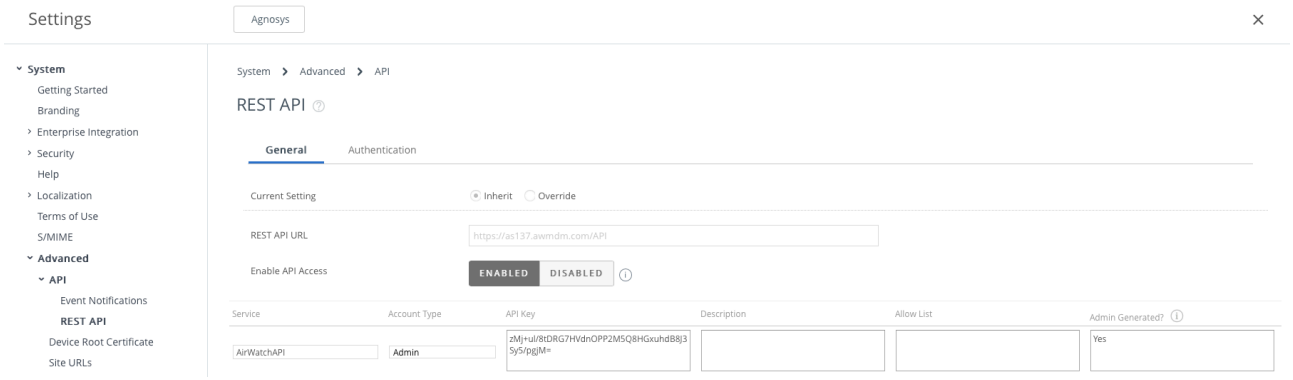
On the pane "3 Details", click on "Next".



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_mom
Password : SuperSecretPassword
API Key  : zMj+ul/8tDSG7HVdnOPQ2M5Q8HGxuhdB8J3Sy5/pgjN=

svc_mom,SuperSecretPassword,zMj+ul/8tDSG7HVdnOPQ2M5Q8HGxuhdB8J3Sy5/pgjN=
```

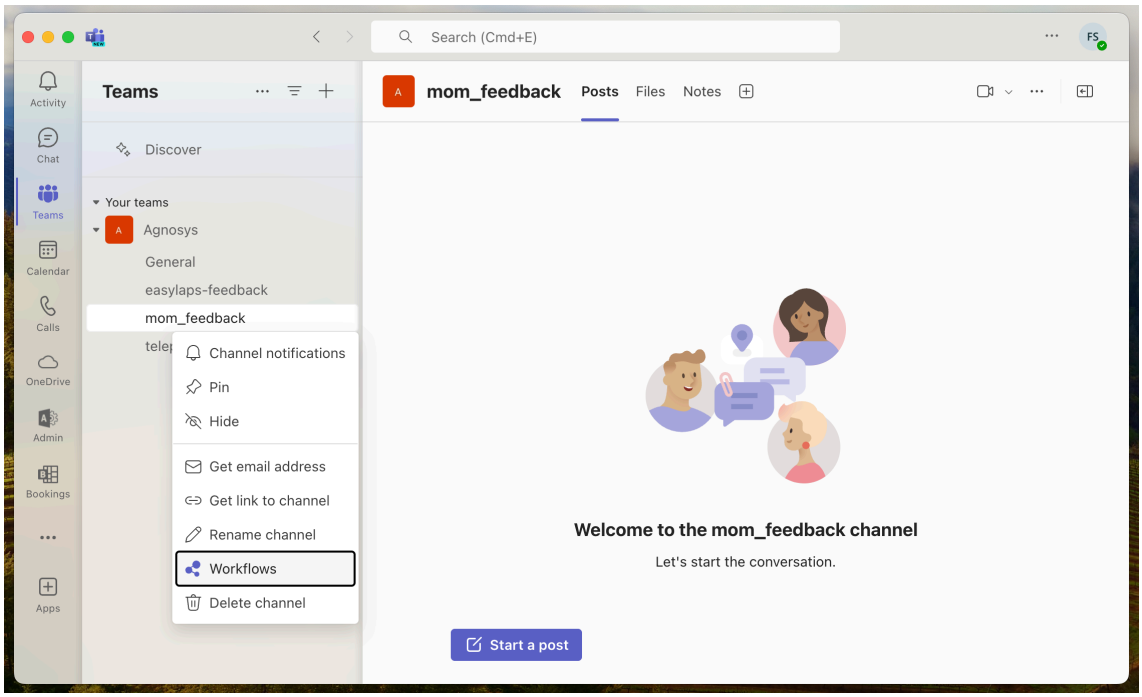
Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated 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.

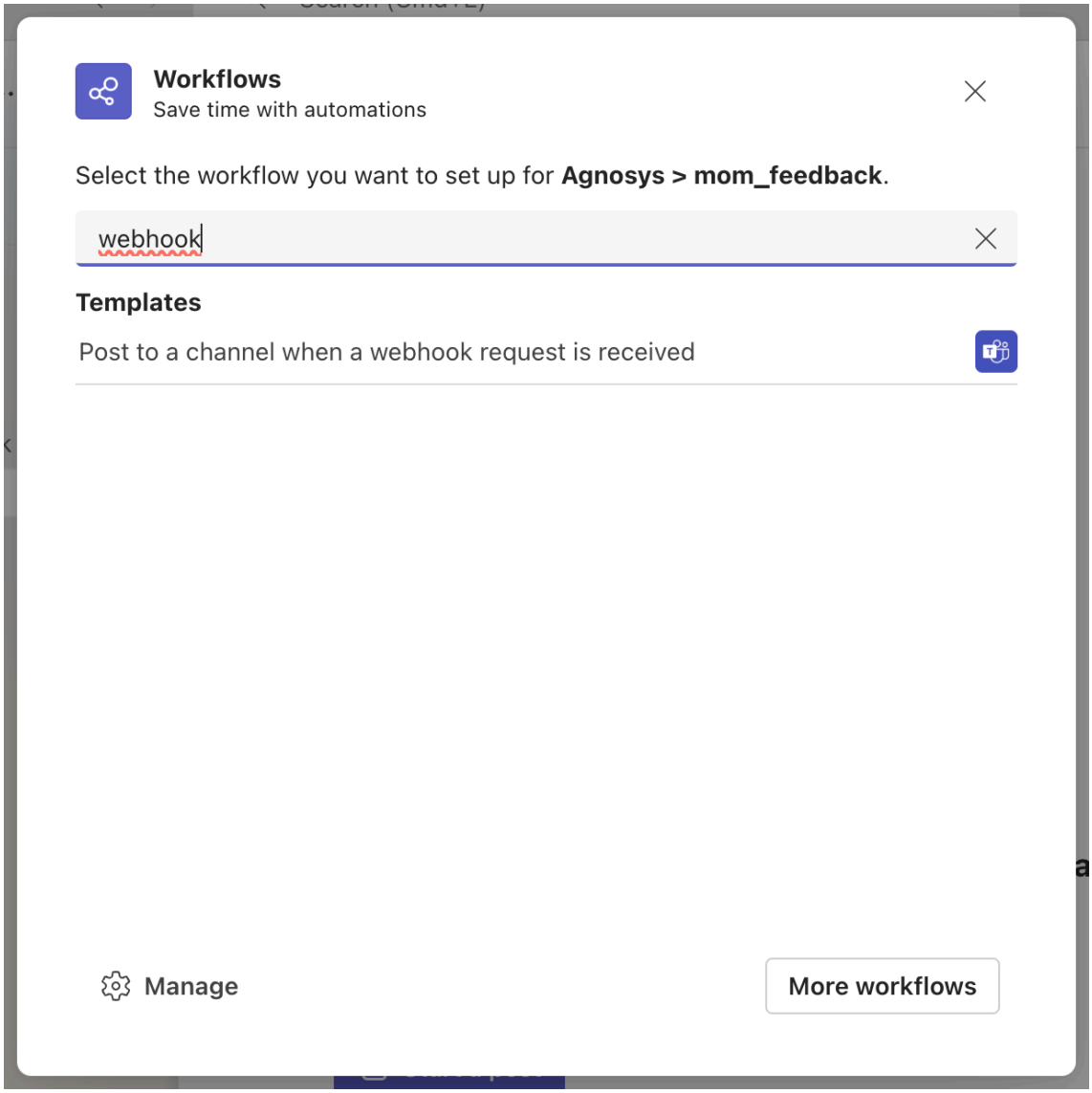
Microsoft Teams integration

MOM can report to a dedicated Microsoft Teams channel the successive status of a device's onboarding or migration.

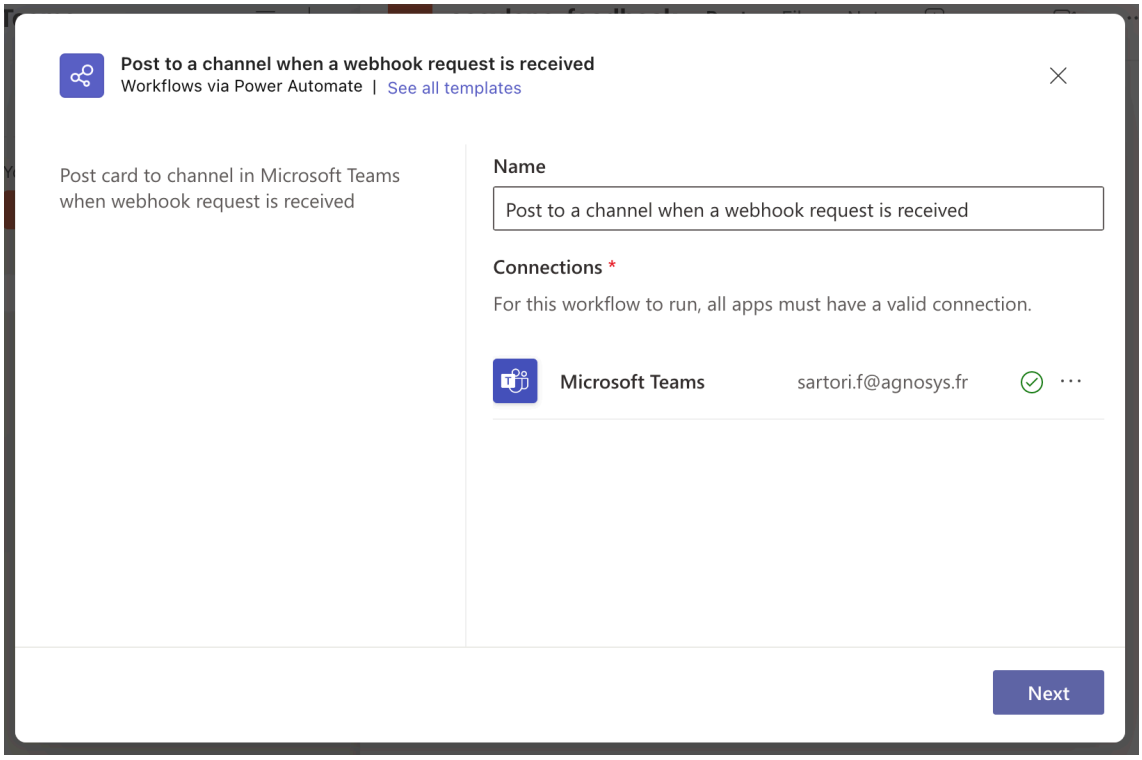
First create a dedicated Microsoft Teams channel of type "Standard" (everyone on the team has access).



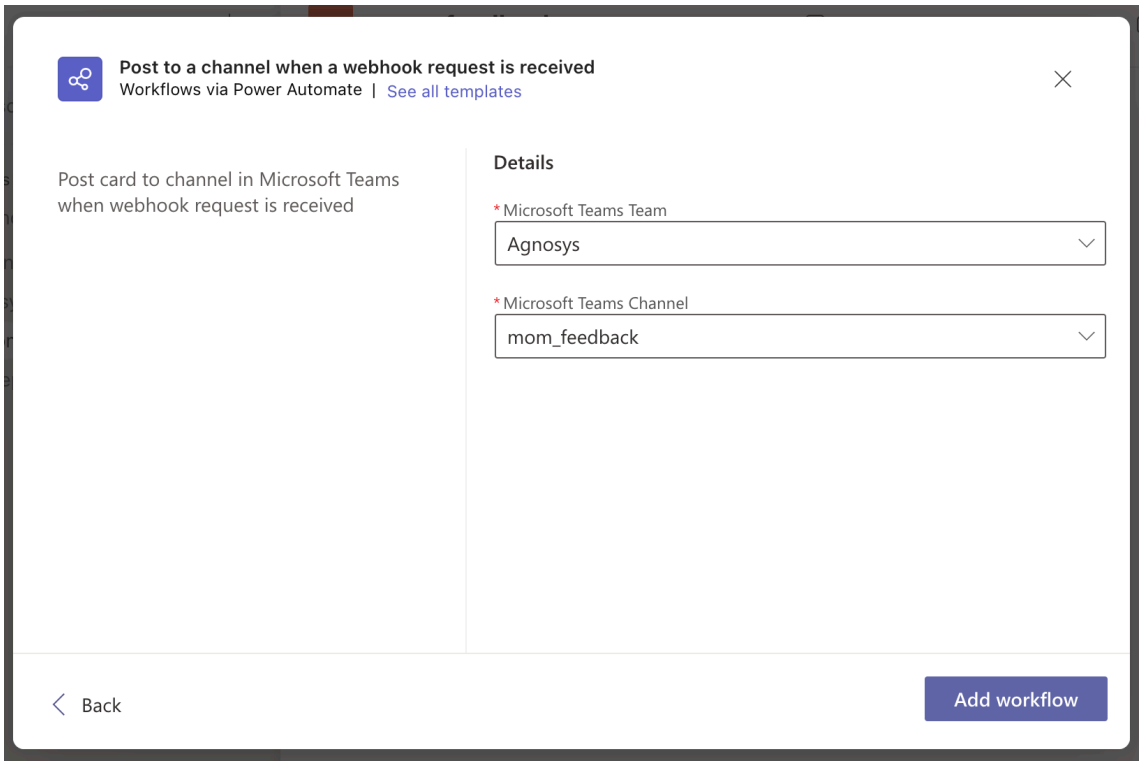
Click on the "..." button to the right of the channel name, then select "Workflows".



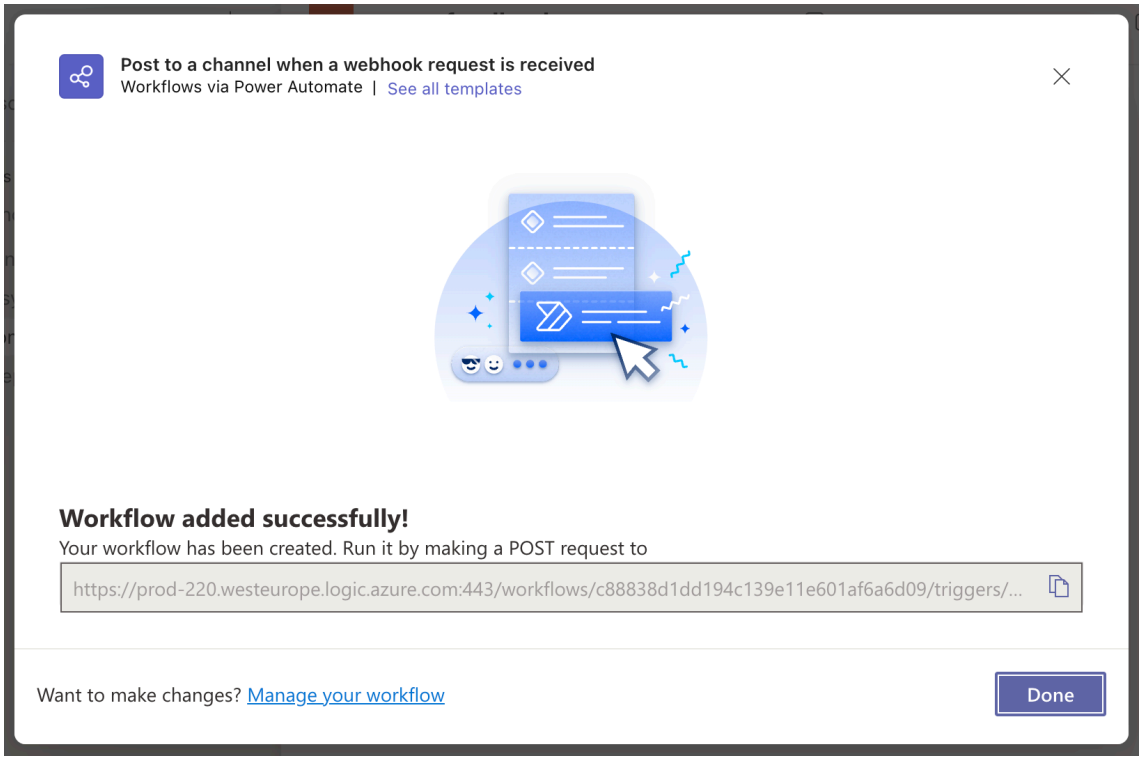
Type "webhook" in the search field, then click on "Post to a channel when a webhook request is received".



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



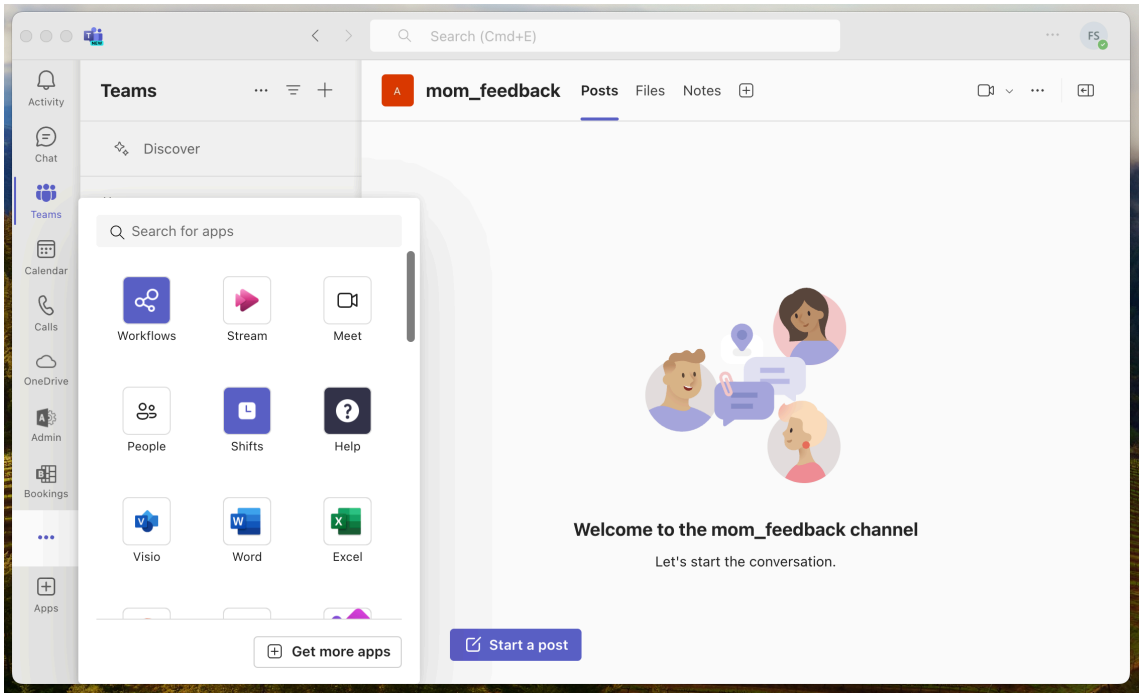
Check the Microsoft Teams team and the Microsoft Teams channel, then click on "Add workflow".



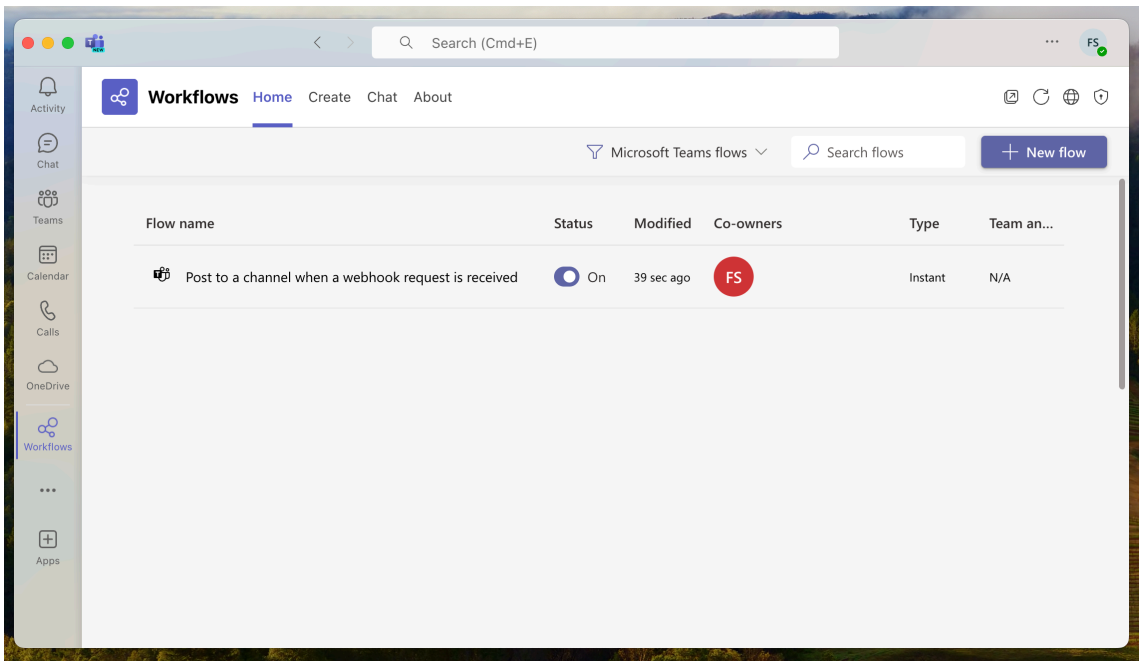
Click on the button to the right of the URL displayed to copy it, then follow these instructions :
- open the "MOM-Toolkit" folder
- open the "mom_secrets" subfolder
- execute the "mom_rsa_engine" script (double-click on the .command file)
- paste the copied URL
- the URL is encrypted, displayed and 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"
- the INTEGRATIONS > TEAMS_CONFIGURATION > MESSAGE_FLIGHT_RECORDER key uses \n\n to obtain new lines.

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.

Location configuration files to Custom configuration profiles conversion

This section only applies to AutoLauncher mode.

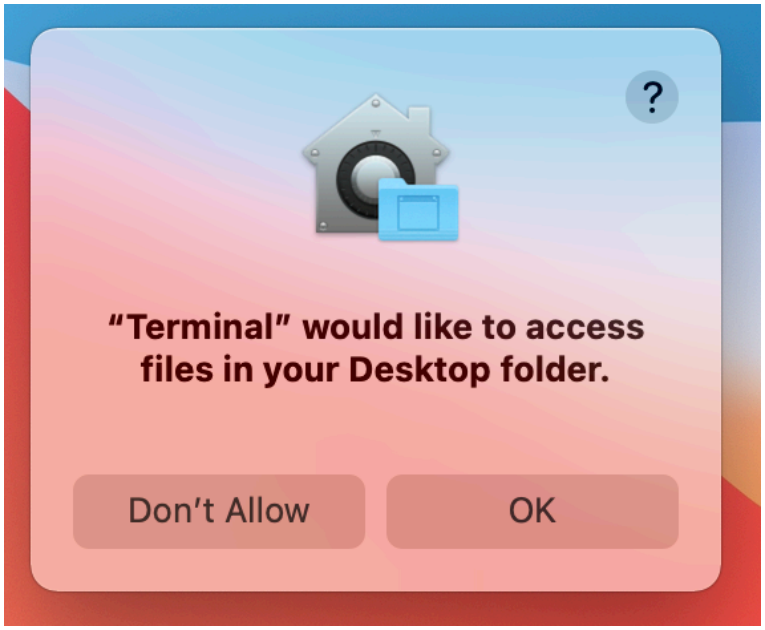
If the MDM solution is Jamf Pro, this step is optional because this MDM offers to upload a Location configuration file directly into a Configuration profile that includes an "Application & Custom Settings" payload. However, if you prefer to upload in Jamf Pro a pre-built Custom configuration profile,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

Open the "MOM-Toolkit" folder.

Open the "mom_configs" subfolder.

Open the "locations_profiles" folder.

Execute the "locations_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 two Location configuration files into two Custom configuration profiles ready to be deployed by the MDM (only one must be scoped to a specific device).

Please note that if the MDM solution is VMware Workspace ONE, the file extension is ".plist" instead of ".mobileconfig". The content of the file is used to populate a Custom Settings payload.

MOM Content building

All pictures (.png), files (.csv, .md, .txt), configuration profiles (.mobileconfig) and scripts (.sh) referenced in the Launcher configuration file and the Location configuration file(s) must be embedded in the MOM-Content package.

In the context of Launcher mode, the MOM-Content package is eventually embedded with the Launcher configuration file and the Location configuration file(s) in the MOM-Core-Companion disk image. The signature of the package is always recommended but is not required.

In the context of AutoLauncher mode, the MOM-Content package is deployed alongside the Custom configuration profile(s), derived from the Location configuration file(s), 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 for AutoLauncher mode

• **FileWave**

No signature required.

• **Hexnode UEM**

Signature required.

• **Jamf Now**

Signature required.

• **Jamf Pro**

This documentation plans that the MOM-Content package is deployed as a PreStage Enrollment package which requires that the package is signed.

However, if the package is deployed via the Packages payload of a policy, the package signature is not a requirement.

• **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 MOM-Content package is deployed either as a Bootstrap Package with the "Expedited Delivery" deployment type, or as a regular package with the "Full Software Management" deployment type.

With the "Expedited Delivery" deployment type, the package signature is a requirement.

With the "Full Software Management" deployment type, the package signature is not a requirement.

Package signature options

These are some options to sign the MOM-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 :

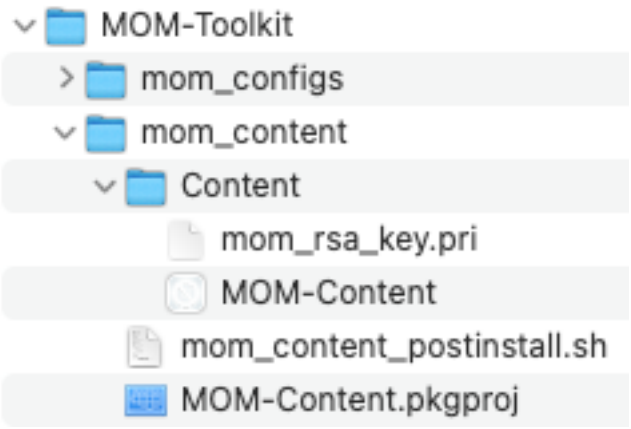
- the certificate forged with the Jamf Pro's Built-in CA can be validated by a device only if it is already enrolled in Jamf Pro
- in the context of Launcher mode, using such certificate is not an option because the device is not yet enrolled in Jamf Pro at the time MOM is executed
- in the context of AutoLauncher mode with no migration or a migration **from** Jamf Pro, using such certificate is an option because the device is enrolled in Jamf Pro at the time MOM is executed
- 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" MOM-Content.pkg MOM-Content_signed.pkg
```

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

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

Content gathering



Open the "MOM-Toolkit" folder.

Open the "mom_content" subfolder.

Open the "Content" folder.

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

You may add in this folder other resources used by other tools or helpers like a Login Window picture referenced by Jamf Connect, NoMAD Login or XCreds.

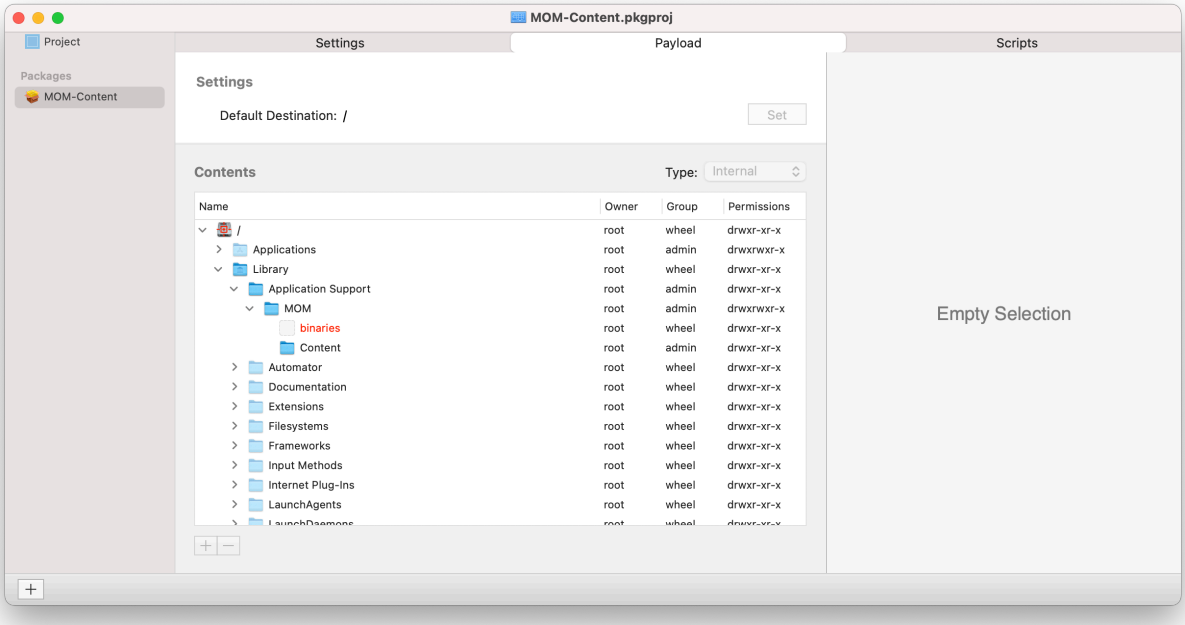
Optionally, you can create a folder named "binaries" in the "mom_content" subfolder and copy packages there. These packages will be embedded in the MOM-Content package and installed right after the installation of the MOM-Content (e.g. swiftDialog, DEPNotify). Do not try to install using this method the following software already planned in the Location configuration file(s) : Homebrew, Installomator, Munki Tools, Jamf Connect, NoMAD, NoMAD LaunchAgent, NoMAD Login, XCreds, Python (Macadmins), Dockutil, set_desktops.py, Wallpaper.

Project opening

Open the "MOM-Toolkit" folder.

Open the "mom_content" subfolder.

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

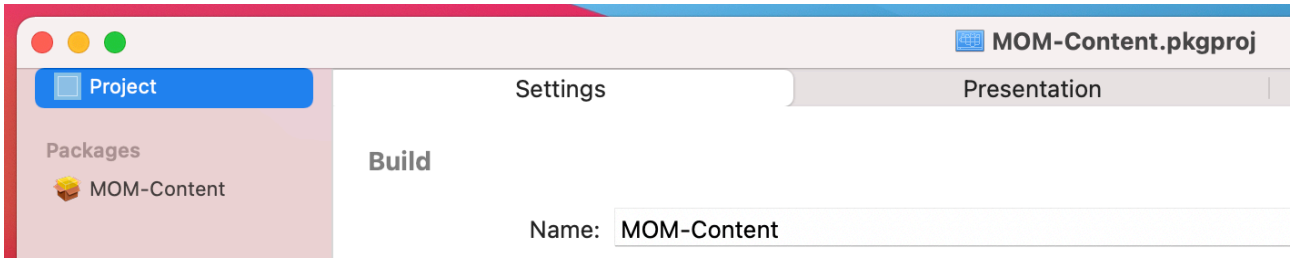


The generated package will embed the "Content" folder and optionally the "binaries" folder for an installation in /Library/Application Support/MOM/

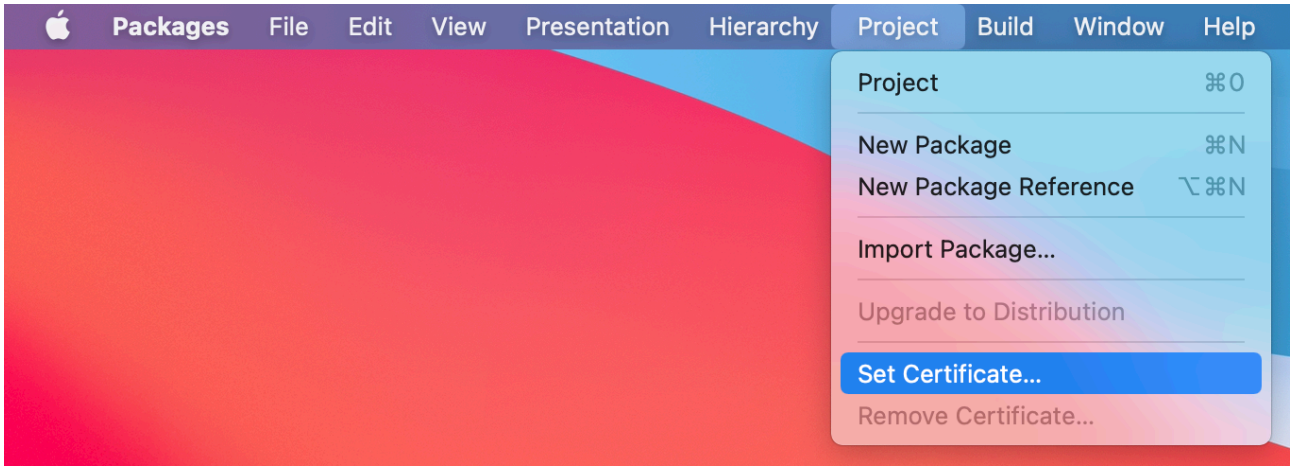
Please note that the missing "binaries" folder displayed in red will not prevent the building of the package. This behaviour is achieved because the build option "Treat missing files as simple warnings" is enabled in the Payload tab. You can keep the binaries folder declaration for future usage.

Signing configuration

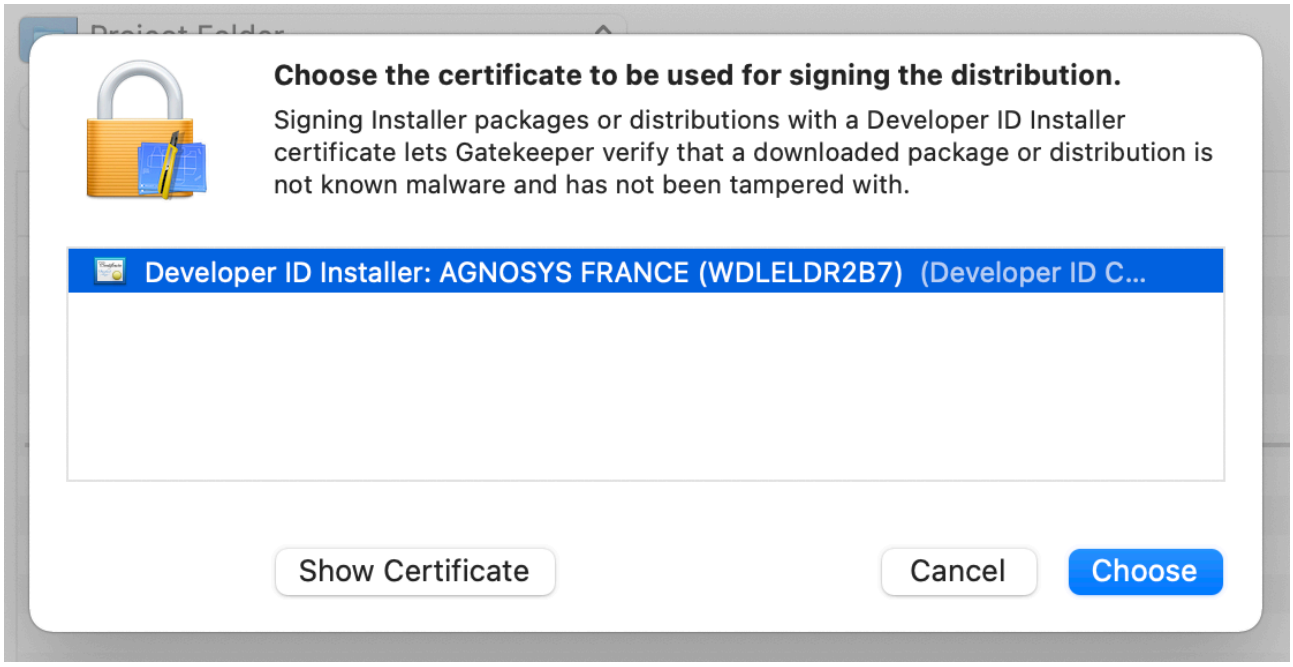
Open the Keychain Access app and check that your "Developer ID Installer" certificate is installed in the "login" keychain.



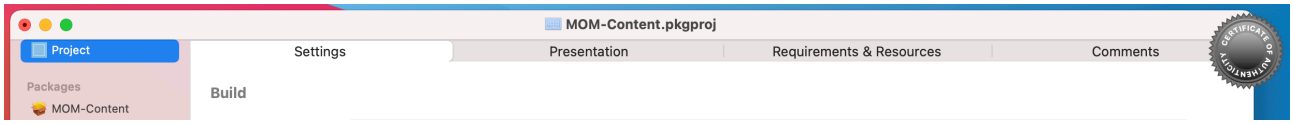
Click on "**Project**" then select the "Settings" tab.



Select Project > Set Certificate.

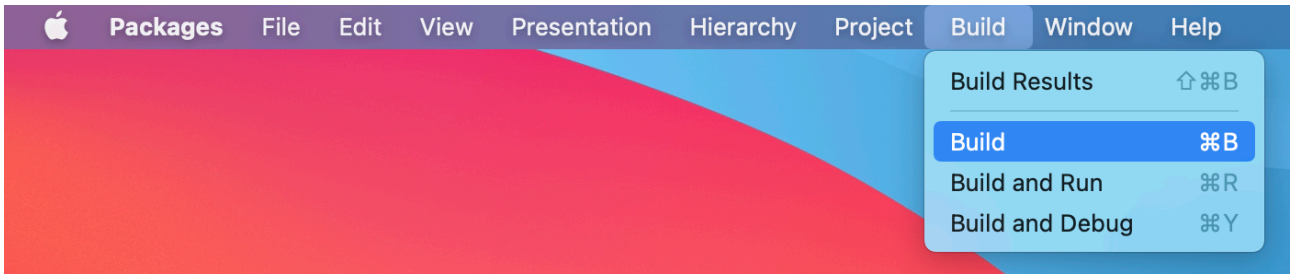


Select your "Developer ID Installer" certificate and click on "Choose".

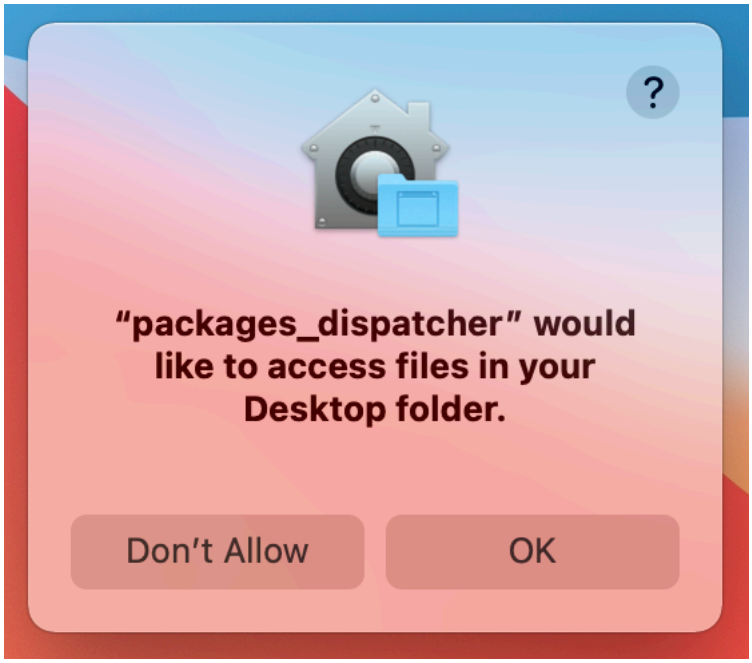


A "Certificate of authenticity" badge is now visible in the upper right corner of the project window.

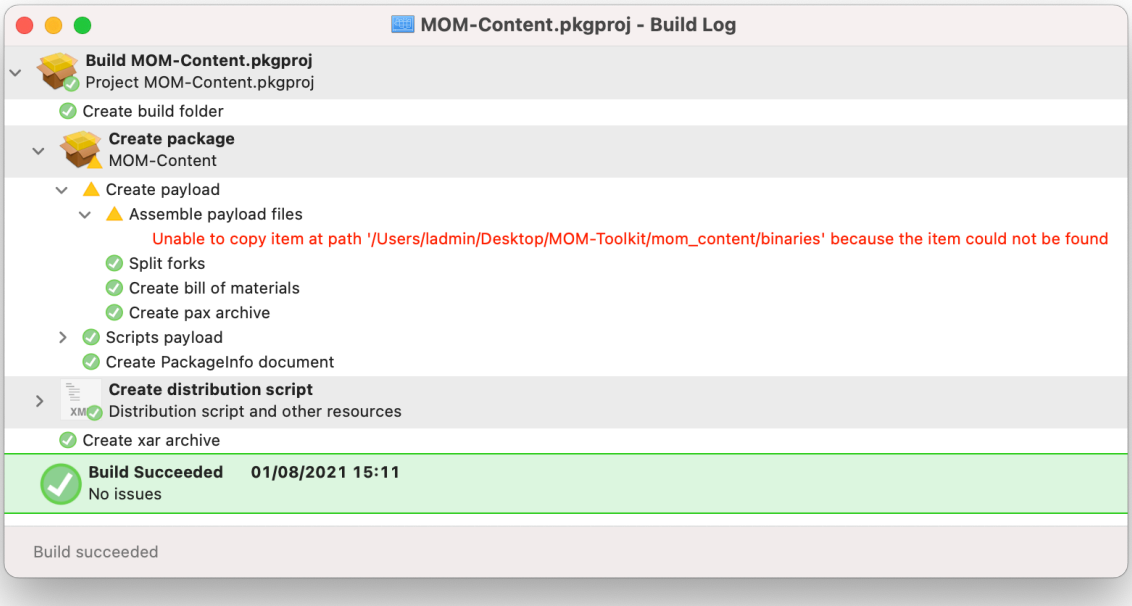
Project building



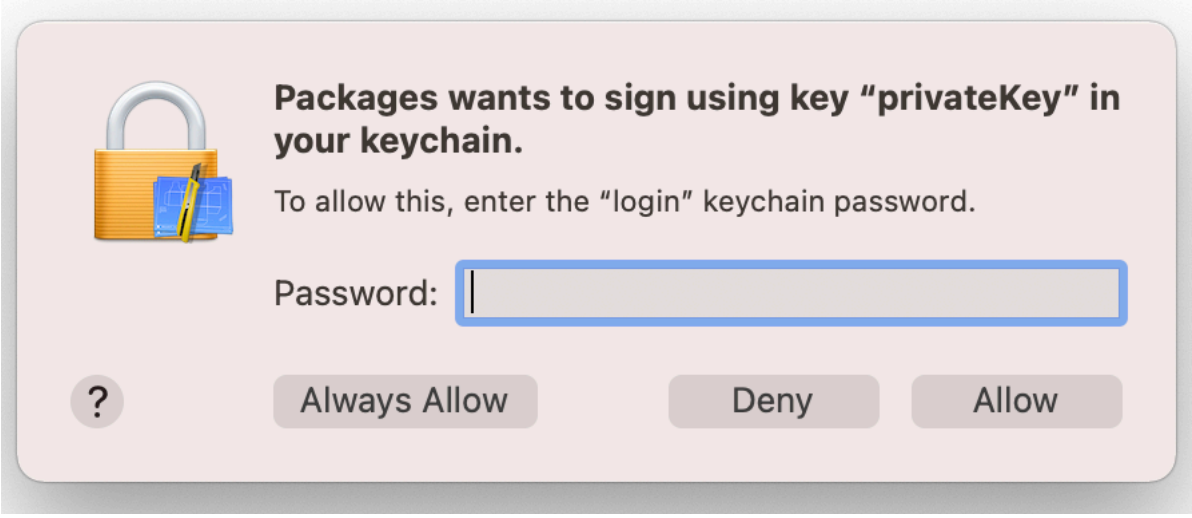
Select Build > Build.



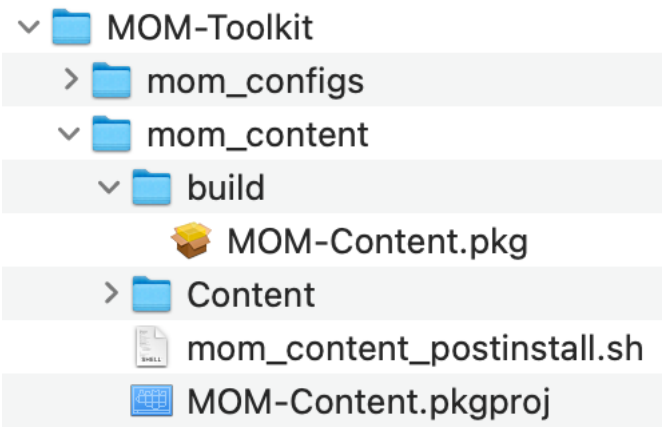
If prompted to authorize the Packages app to access files in a specific folder like your Desktop folder, click on "OK".



In the Build Log, the warning message in red is expected if you didn't create the optional folder named "binaries" in the "mom_content" subfolder as mentioned above. You can safely ignore this message unless you planned to embed packages in the MOM-Content package.



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 :
MOM-Toolkit > mom_content > build

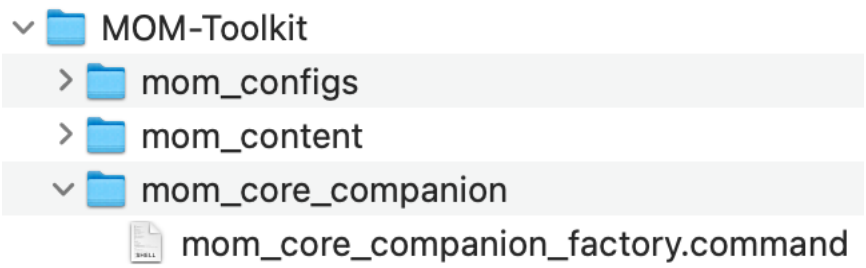
You can now quit the Packages app. Choose to save the changes made to the project if you are offered to do so.

MOM Core Companion building

This section only applies to Launcher mode.

The MOM-Core-Companion disk image embeds the MOM-Content package, the Launcher configuration file and the Location configuration file(s).

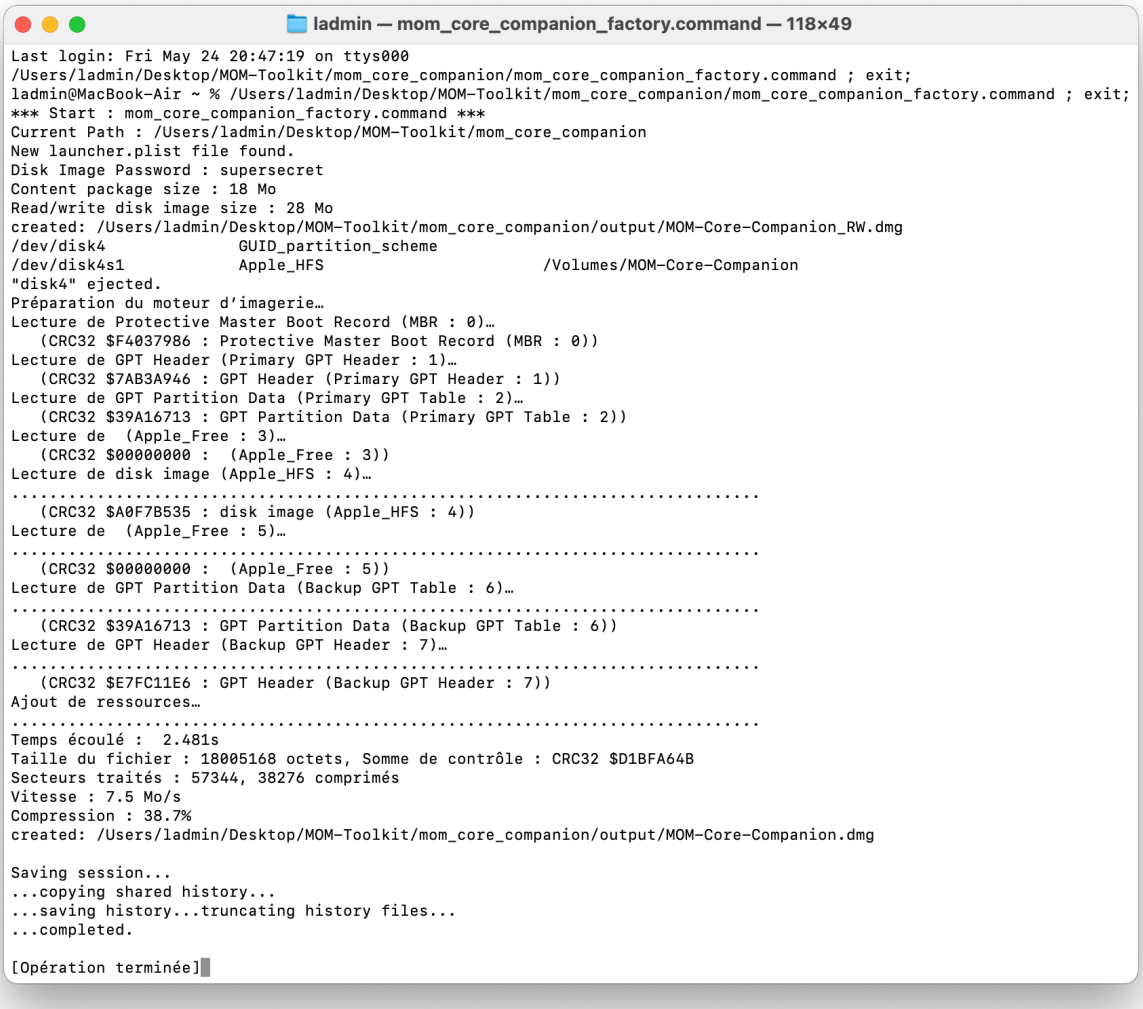
The disk image is protected from an unauthorized access using the encrypted password stored in the SECURITYCODE key of the Launcher configuration file.



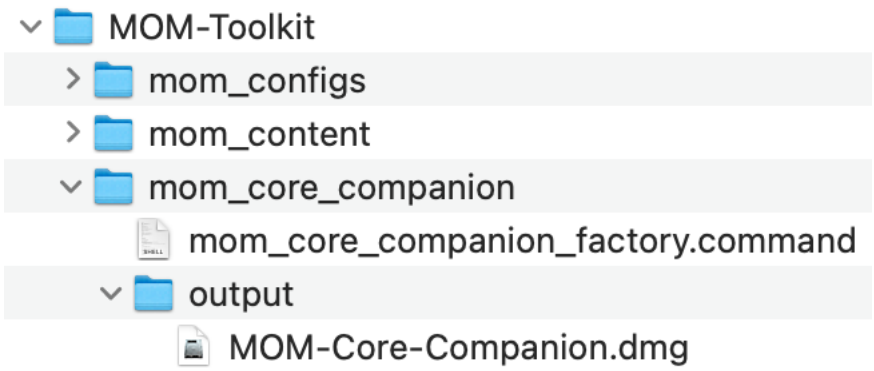
Open the "MOM-Toolkit" folder.

Open the "mom_core_companion" subfolder.

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



The disk image password is displayed in clear text for sanity check.



The disk image is built at the following path :
MOM-Toolkit > mom_core_companion > output

Configuration profiles requirements

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

In the context of an MDM switching, the recommendation is to deploy these configuration profiles from both the MDM the device is leaving and the MDM the device is joining if you are not concerned about deploying keys that are not absolutely necessary from one of them.

Privacy Preferences Policy Control

MOM includes a Privileged Helper to which it can delegate sensitive operations requiring extended privacy settings.

• Execution of scripts can leverage the Privileged Helper on demand :
- mSCP integration (MSCP_CONFIGURATION dictionary) :
    - compliance script execution for remediation
    - compliance script execution for scanning
- execution of the Preflight, Post Settings and Postflight script (SCRIPTS dictionary).

These scripts run via the Privileged Helper when their associated PREFER_PRIVILEGED_HELPER key is set to "true".

• The following MOM features require the Privileged Helper to be enabled :
- the "Restart and delete local accounts except management account" command on macOS 12 and later (EXIT_ACTION dictionary)
- the Privacy control feature (PRIVACY_CONTROL dictionary).

• Payload required : Privacy Preferences Policy Control

- Identifier Type : Bundle ID

- Identifier : com.agnosys.mom_privileged_helper

- Code Requirement : `identifier "com.agnosys.mom_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

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 MOM has installed several Login items that can run in the background and that can be managed in System Settings.

Payload required : Background Item Management

Required rules

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

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

Additional rules

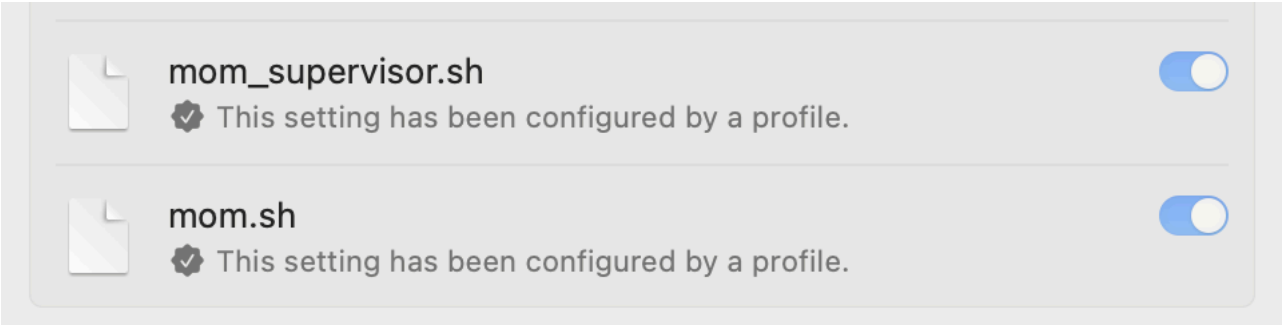
- Required only if the following conditions are met :
    - Automated Device Enrollment orchestrated outside of the Setup Assistant
    - PROMOTION_ALLOWED key set to true
- Rule Type : Label
- Rule Value : com.agnosys.promotion_supervisor

- Required only if the following condition is met :
    - EXIT_ACTION > COMMAND key set to restart_delete_local_accounts_except_management_account
- Rule Type : Label
- Rule Value : com.agnosys.delete_local_accounts_except_management_account

- Required only if the following condition is met :
    - JAMF_CONNECT_CONFIG key set to enabled
- Rule Type : Label
- Rule Value : com.agnosys.jamfconnect

- Required only if the following condition is met :
    - NOMAD_LOGINAD_CONFIG key set to enabled
- Rule Type : Label
- Rule Value : com.agnosys.nomadloginad

- Required only if the following condition is met :
    - LOGINUSERSCRIPT key set to a script
- Rule Type : Label
- Rule Value : com.agnosys.login_user



Once the configuration profile is deployed on a device running MOM, 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 "mom_btm_signed.mobileconfig" provided in the subfolder "mom_library" of the MOM Toolkit.

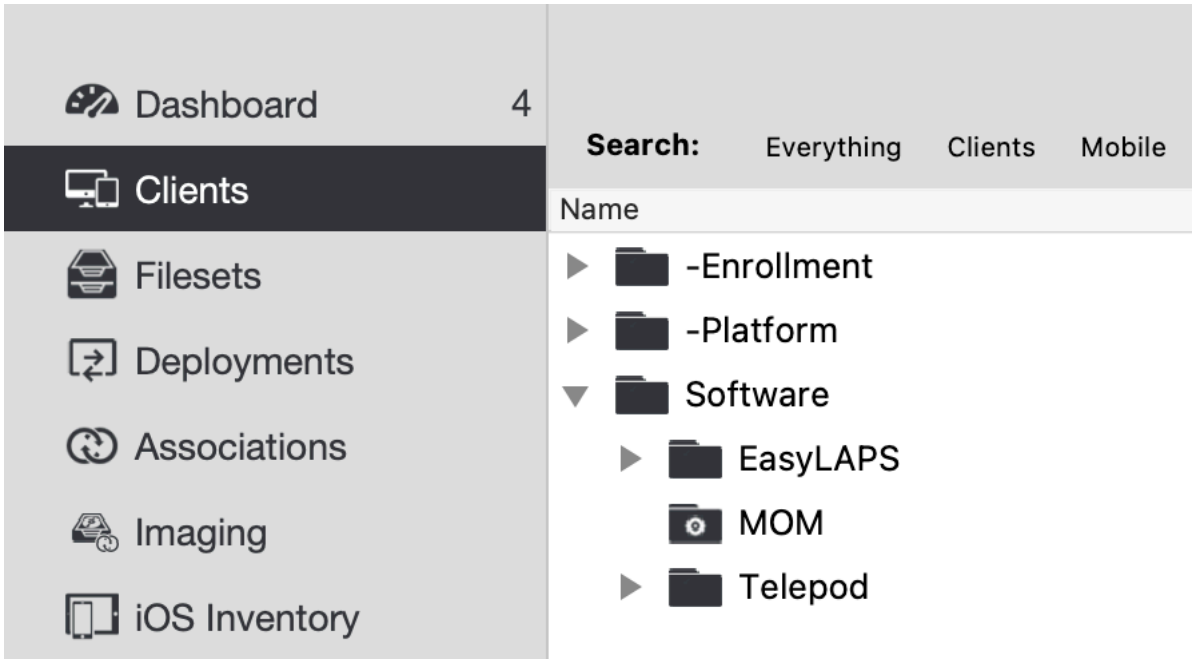
Provisioning FileWave for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

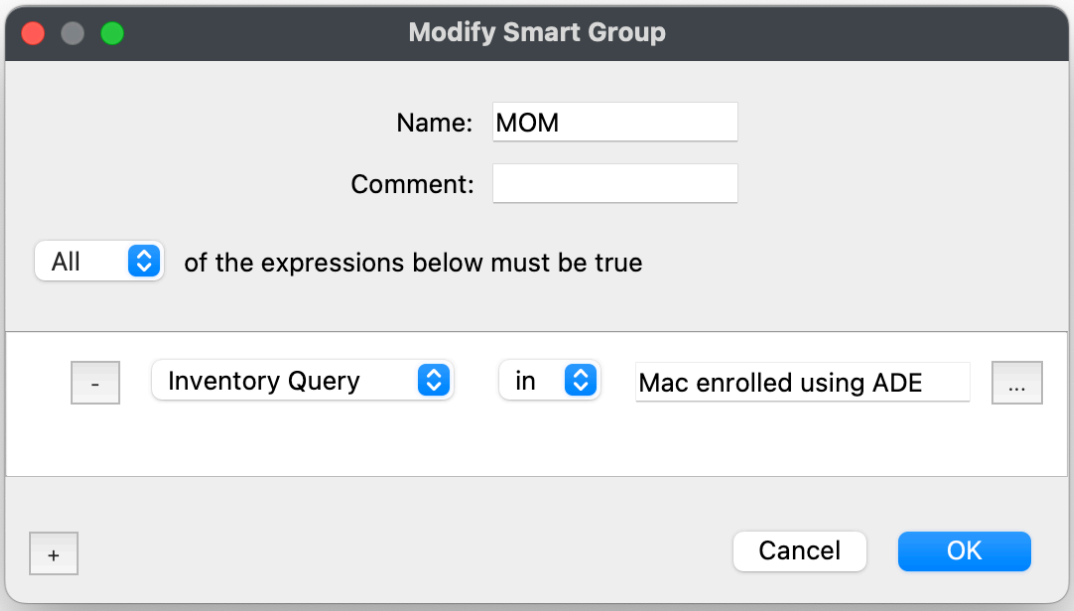
This section outlines the key points for the provisioning of these three components in FileWave. Please refer to FileWave documentation for details not specific to MacOnboardingMate.

General configuration

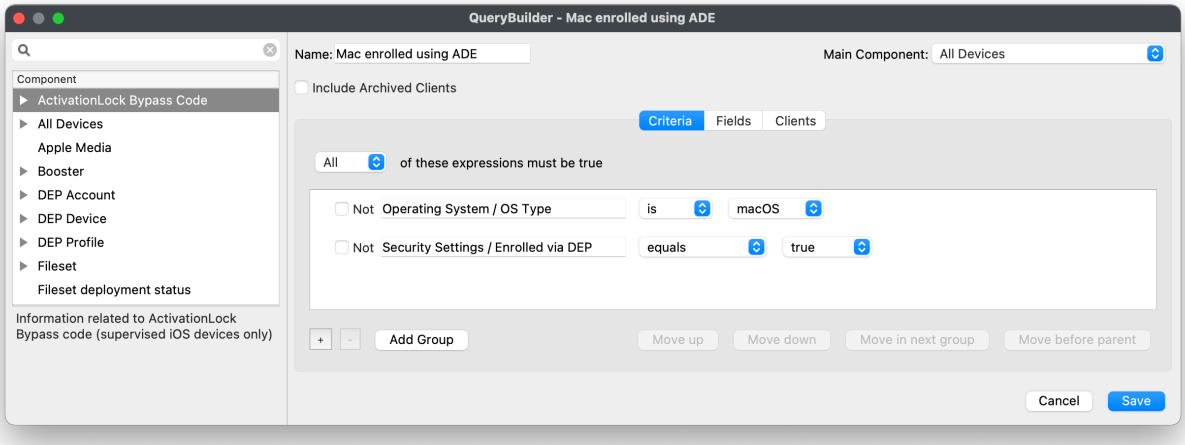
In this example, the devices are organized following this structure.



The devices installed with MOM are part of a Smart Group named "MOM".



Devices are member of the Smart Group "MOM" when they respond to the Inventory Query named "Mac enrolled using ADE".



The Inventory Query "Mac enrolled using ADE" is based on the following criteria :

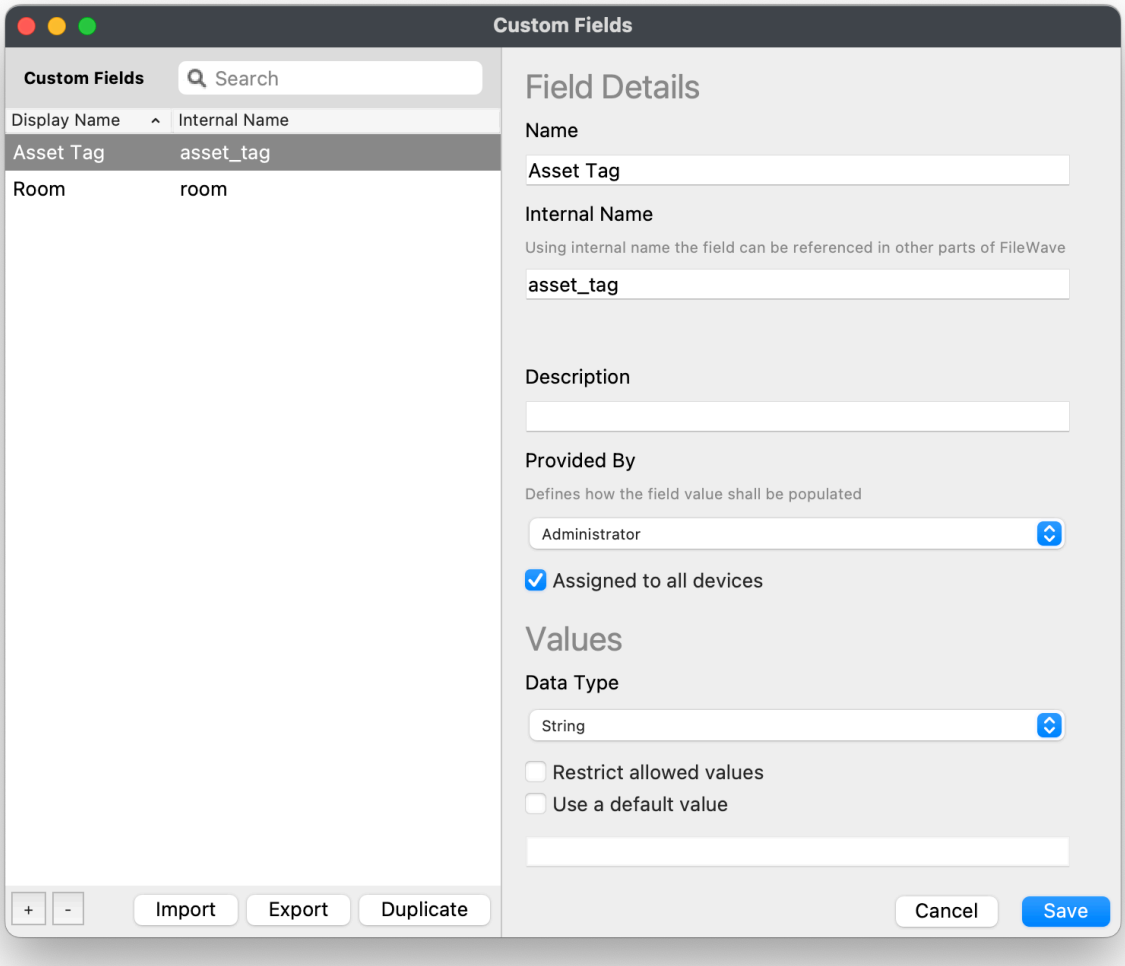
- Criteria : All
  - Operating System / OS Type — is — macOS
  - Security Settings / Enrolled via DEP — equals — true
- Main Component : All Devices

As a result, any Mac enrolled using Automated Device Enrollment will be member of the Smart Group "MOM".

Custom Fields

Custom Fields must be created manually.

FileWave Admin > Assistants > Custom Fields > Edit Custom Fields



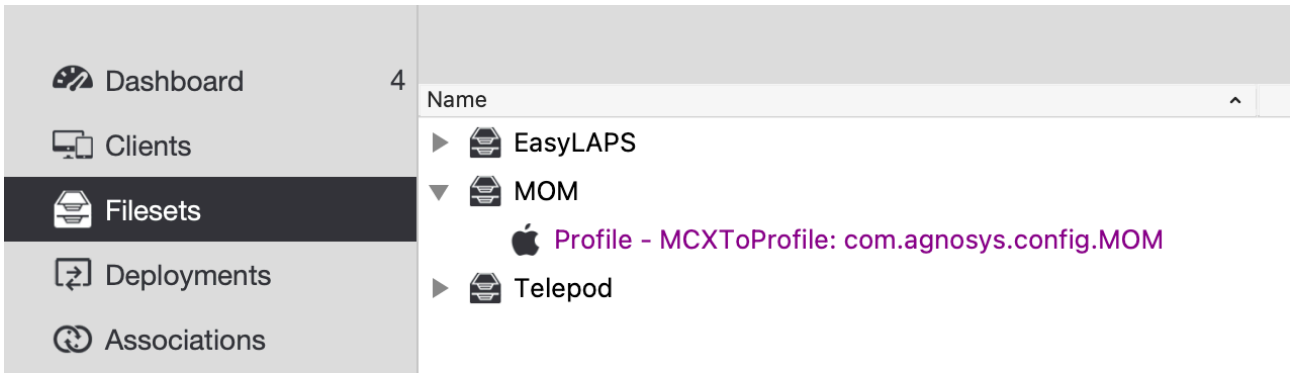
Enter the name of the Custom Field in the Name field and its internal name in the Internal Name field.

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

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

Custom configuration profile

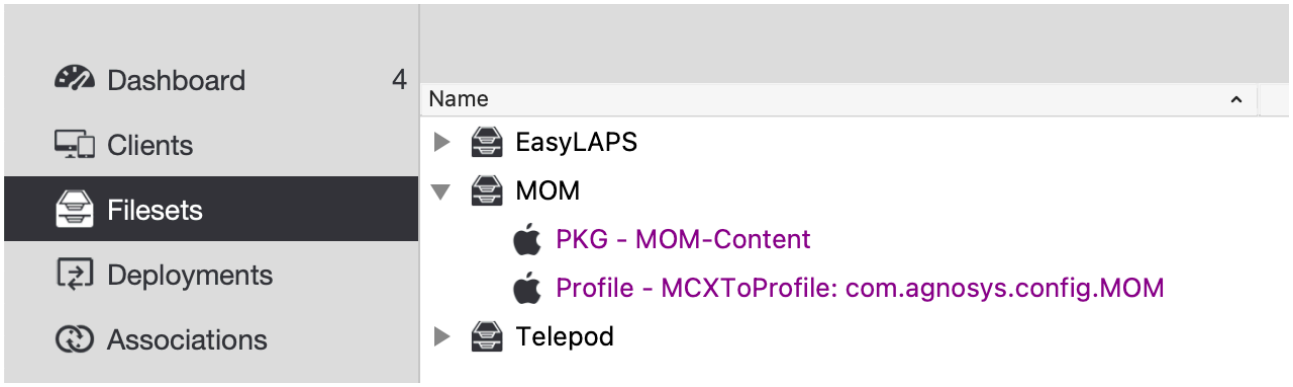
The Custom configuration profile is provisioned with the following steps :
- Filesets > New Fileset Group > Name : MOM
- Select the Fileset Group "MOM"
- Click on "New Desktop Fileset" then click on "Profile"
- In the Profile Editor, click on "Load Profile"
- Select the file : com.agnosys.config.FileWave.Paris.MOM.mobileconfig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



The Custom configuration profile is linked to the "MOM" Fileset Group.

MOM-Content package

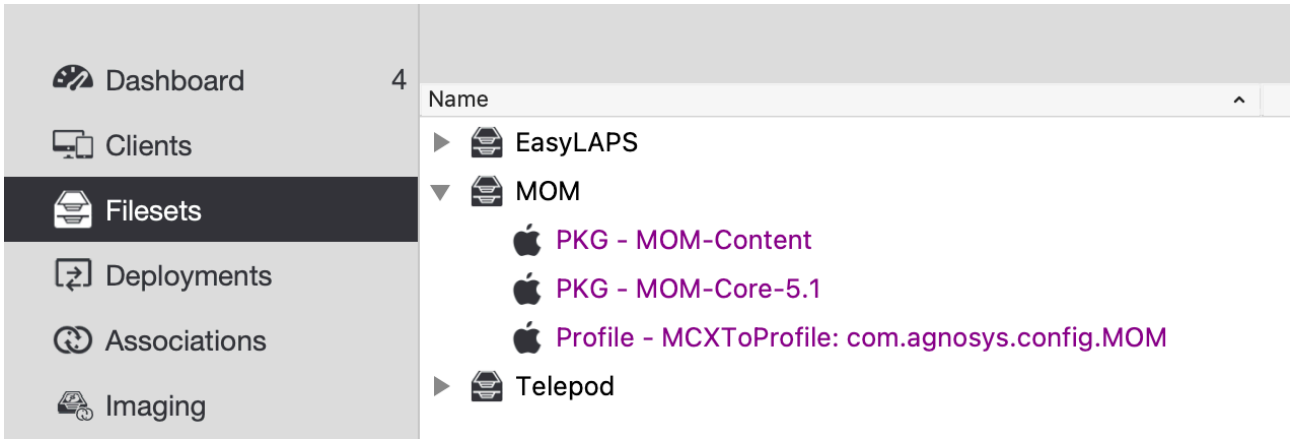
The MOM-Content package is defined with the following steps :
- Filesets > MOM
- Click on "New Desktop Fileset" then click on "MSI / PKG"
- Select the file : MOM-Content.pkg > Open.



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

MOM-Core package

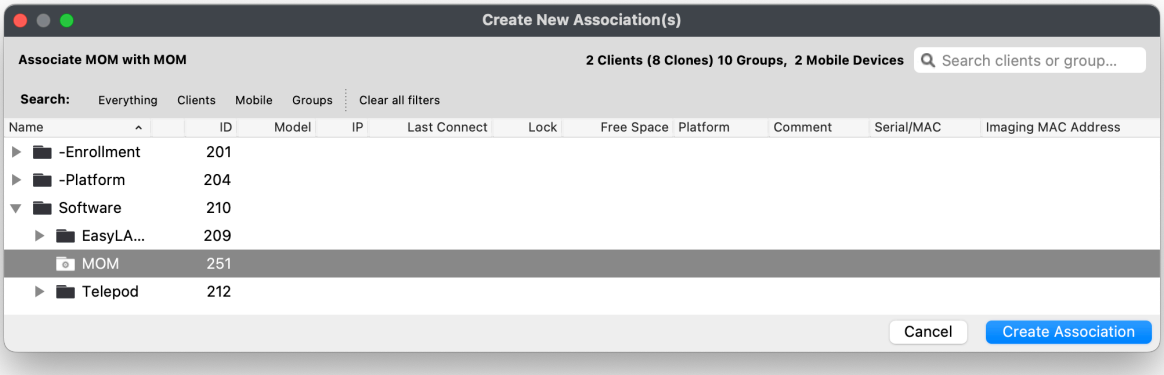
The MOM-Core package is defined with the following steps :
- Filesets > MOM
- Click on "New Desktop Fileset" then click on "MSI / PKG"
- Select the file : MOM-Core.pkg > Open.



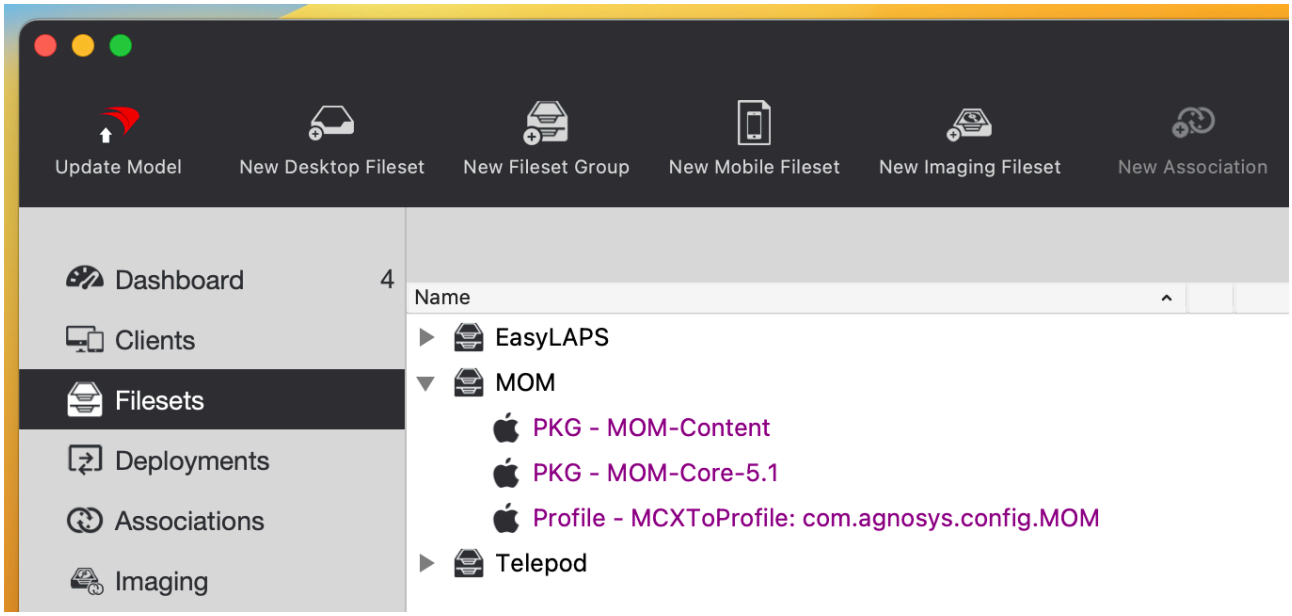
The MOM-Core package is linked to the "MOM" Fileset Group.

Deployment on the MOM group

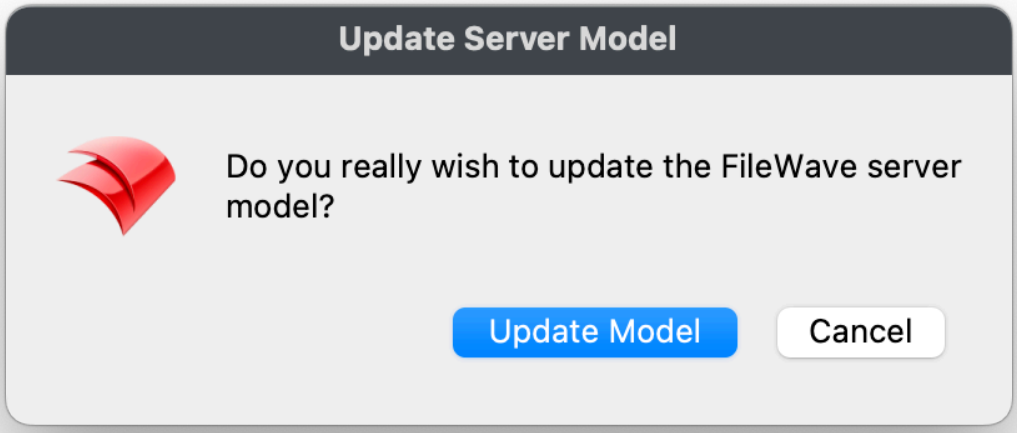
The MOM Fileset is associated to the MOM group with the following steps :
- Filesets > MOM
- In the toolbar, click on "New Association".



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



In the toolbar, click on "Update Model".



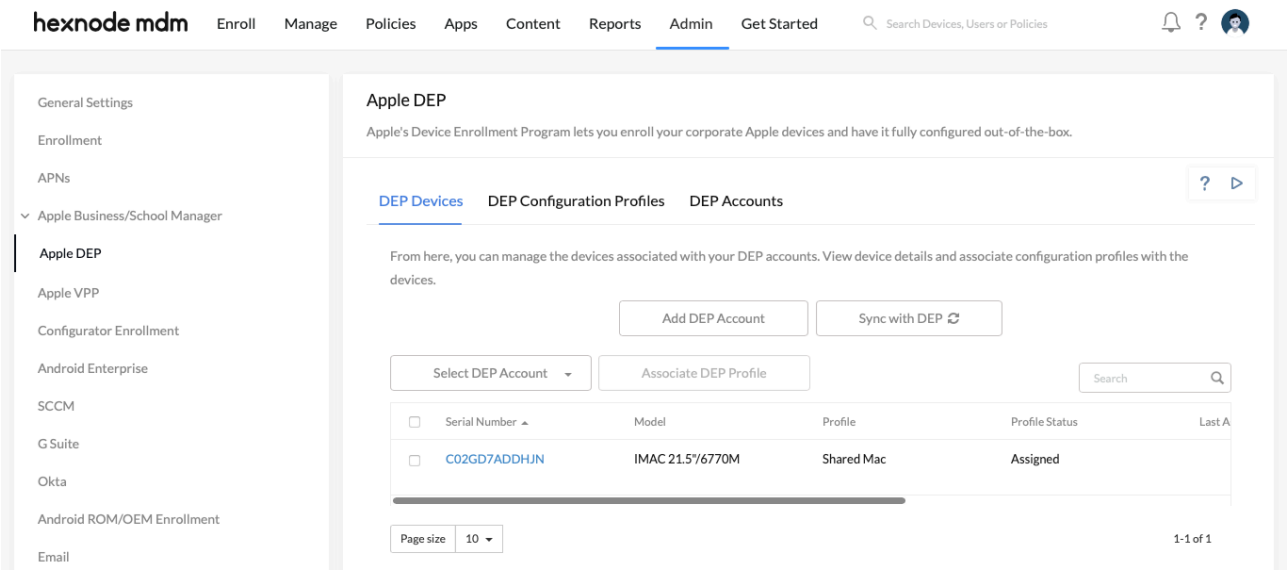
Click on "Update Model".

Provisioning Hexnode UEM for AutoLauncher mode

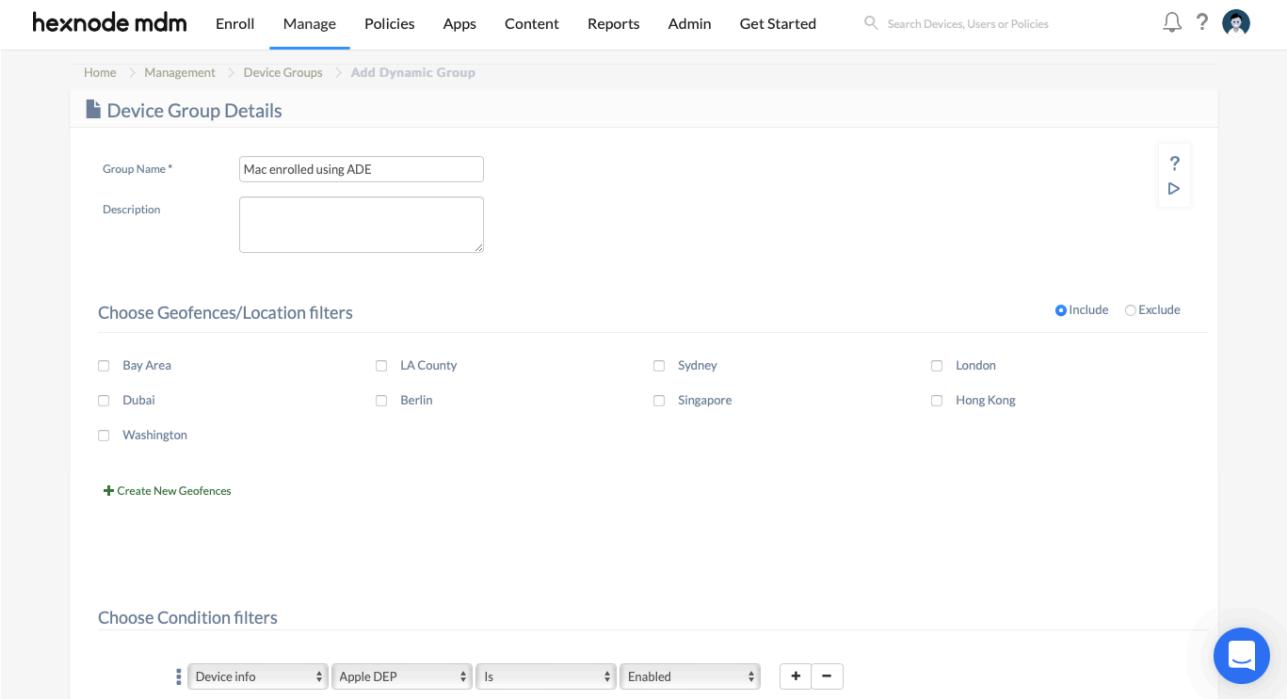
Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

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 MacOnboardingMate.

General configuration



In this example, the devices are part of an Automated Device Enrollment token and associated to a Profile named named "Shared Mac".



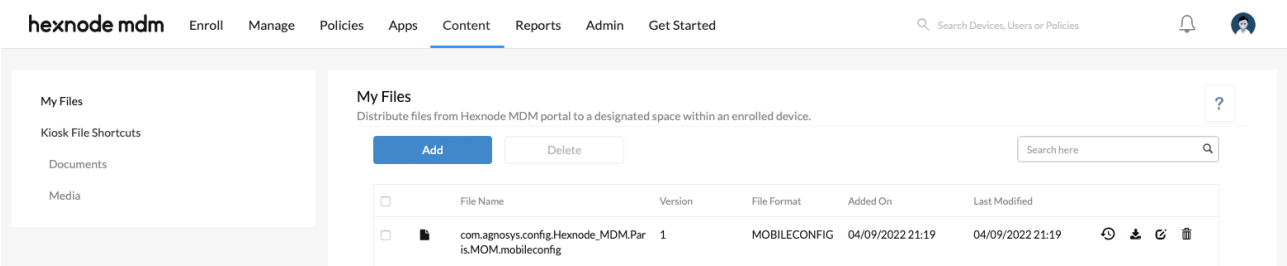
A dynamic group named "Mac enrolled using ADE" is created with the following criterion :

- Device info — Apple DEP — Is — Enabled

As a result, any Mac enrolled using Automated Device Enrollment will be member of the device group "Mac enrolled using ADE".

Custom configuration profile

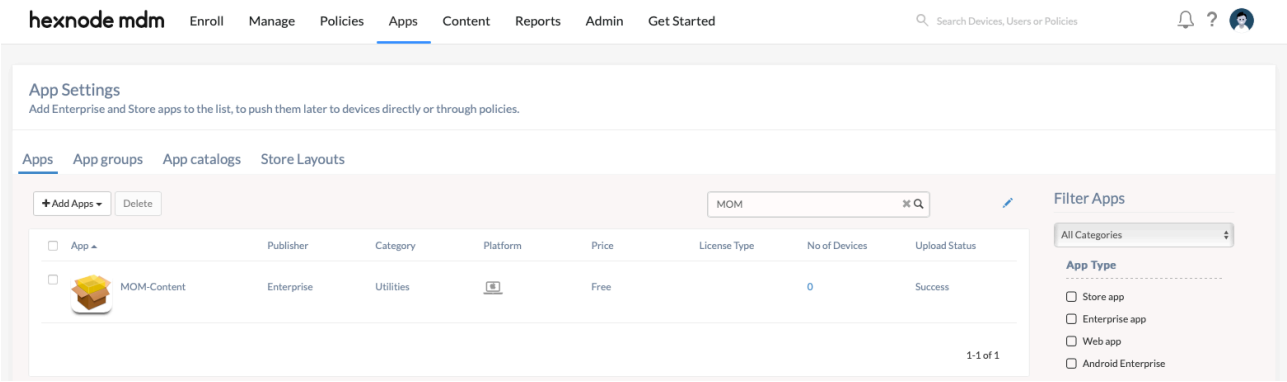
The Custom configuration profile is uploaded with the following steps :
- Content > Add
- Select the file : com.agnosys.config.Hexnode_MDM.Paris.MOM.mobileconfig > Upload
- Save



MOM-Content package

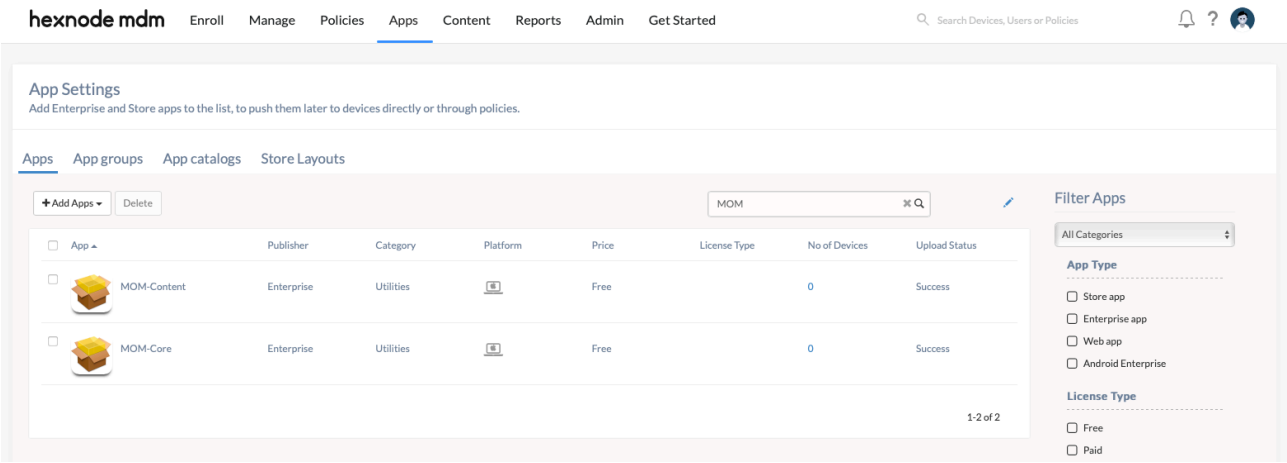
The MOM-Content package is uploaded with the following steps :
- Apps > Apps > Add Apps > Enterprise App
- Select the Platform "macOS" (laptop with Apple logo)
- App Name : MOM-Content
- Upload with : PKG/MPKG/DMG File

- Category : Utilities
- Description : MOM-Content
- Choose the PKG/MPKG/DMG File > Choose File > MOM-Content.pkg > Upload
- Add



MOM-Core package

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



Provisioning policy configuration

The three components can be provisioned via a unique policy with the following steps :
- Policies > New Policy > New Blank Policy
- Policy Name : MOM Provisioning
- Click on the "macOS" tab

    - Configurations > Deploy Custom Configuration
        - Configure
        - Choose File
        - Select "com.agnosys.config.Hexnode_MDM.Paris.MOM.mobileconfig"
        - Click "OK"
    - App Management > Mandatory Apps
        - Configure
        - Add > Add App
        - Select "MOM-Content" and "MOM-Core"
        - Click "Done"
- Click on the "Policy Targets" tab
        - Device Groups > Add Device Groups
        - Select "Mac enrolled using ADE"
        - Click "OK"
- Click "Save"
- In the "Associate Policy" message, click on "Yes"

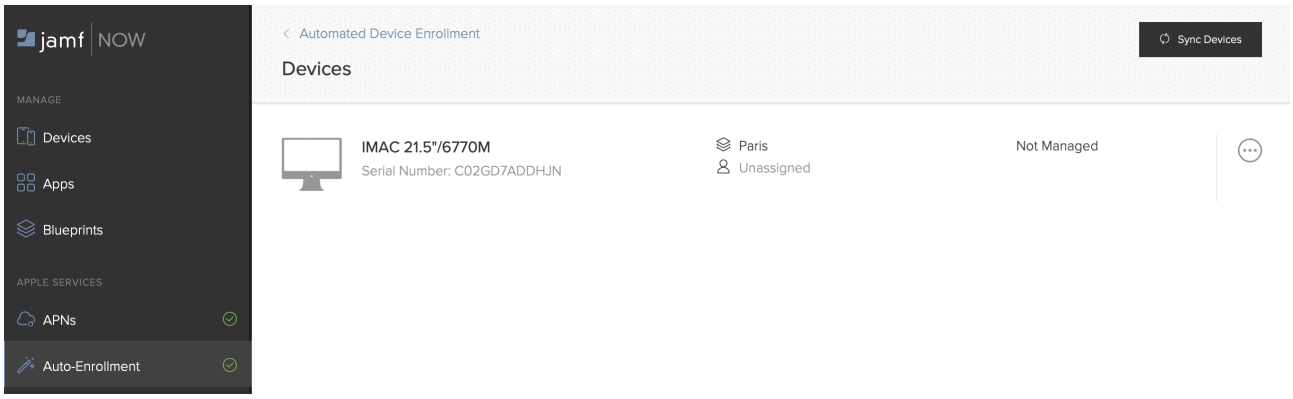
The policy is validated.

Provisioning Jamf Now for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-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 MacOnboardingMate.

General configuration



In this example, the devices are 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.Jamf_Now.Paris.MOM.mobileconfig > Add Custom Profile

MOM-Content package

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

MOM-Core package

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

Provisioning Jamf Pro for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

Because Jamf Pro offers to deploy multiple packages in the context of Automated Device Enrollment, these instructions plans that the three components are eventually installed via a PreStage Enrollment. The only counterpart is that signing the MOM-Content package is a requirement.

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 MacOnboardingMate.

General configuration

In this example, the devices are part of an Automated Device Enrollment token named "Jamf Pro" and associated to a PreStage Enrollment named "Shared Mac".

A smart group named "Mac enrolled using ADE" is created with the following criterion :
Enrolled via Automated Device Enrollment — is — Yes

As a result, any Mac enrolled using Automated Device Enrollment will be member of the device group "Mac enrolled using ADE".

Custom configuration profile : importing a .plist file

Follow these instructions if you want to upload in Jamf Pro a Location 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. MOM-Custom configuration profile)
    - Level : Computer Level
    - Distribution Method : Install Automatically
- Application & Custom Settings > Upload > Add
    - Preference Domain : com.agnosys.config.MOM
    - Upload > location_1.plist
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Mac enrolled using ADE > 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 Location configuration file to Custom configuration profile conversion.

The Custom configuration profile is provisioned with the following steps.

To upload the profile and to keep it on the device after it is enrolled :
- Computers > Content Management > Configuration Profiles > Upload
- Choose File : com.agnosys.config.Jamf_Pro.Paris.MOM.mobileconfig
- General
    - Name : a name of your choice (e.g. MOM-Custom configuration profile)
    - Level : Computer Level
    - Distribution Method : Install Automatically
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > Mac enrolled using ADE > 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.

MOM-Content package

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

MOM-Core package

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

Configuration of the PreStage Enrollment

To allow the components to be installed at enrollment :
- Computers > PreStage Enrollments > Shared Mac
- Edit
- Configuration Profiles : select the MOM Custom configuration profile
- Enrollment Packages :
    - Configure
    - Click "Add" to the right of MOM-Content.pkg
    - Click on the "+" button to add a supplemental package
    - Click "Add" to the right of MOM-Core.pkg
    - Distribution Point : select "Cloud Distribution Point (Jamf Cloud)"
- Save > Save

Provisioning Jamf School for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

Because Jamf School offers to deploy multiple packages in the context of Automated Device Enrollment, these instructions plans that the three components are eventually installed via an Automated Device Enrollment profile.

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 MacOnboardingMate.

General configuration

In this example, the devices are part of an Automated Device Enrollment token named "Jamf School" and associated to an Automated Device Enrollment profile named "Shared Mac".

Components are configured at the school level.

A smart group named "Mac enrolled using ADE" is created with the following criteria :
Match all rules
- Operating System — equals — maOS
- Enrollment Method — equals — Automated Device Enrollment / Apple School Manager

As a result, any Mac enrolled using Automated Device Enrollment will be member of the device group "Mac enrolled using ADE".

Custom configuration profile

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

MOM-Content package

The MOM-Content package is provisioned with the following steps :
- Apps > Inventory > Add App > Add In-House macOS Package
- Select "MOM-Content.pkg"
- Save

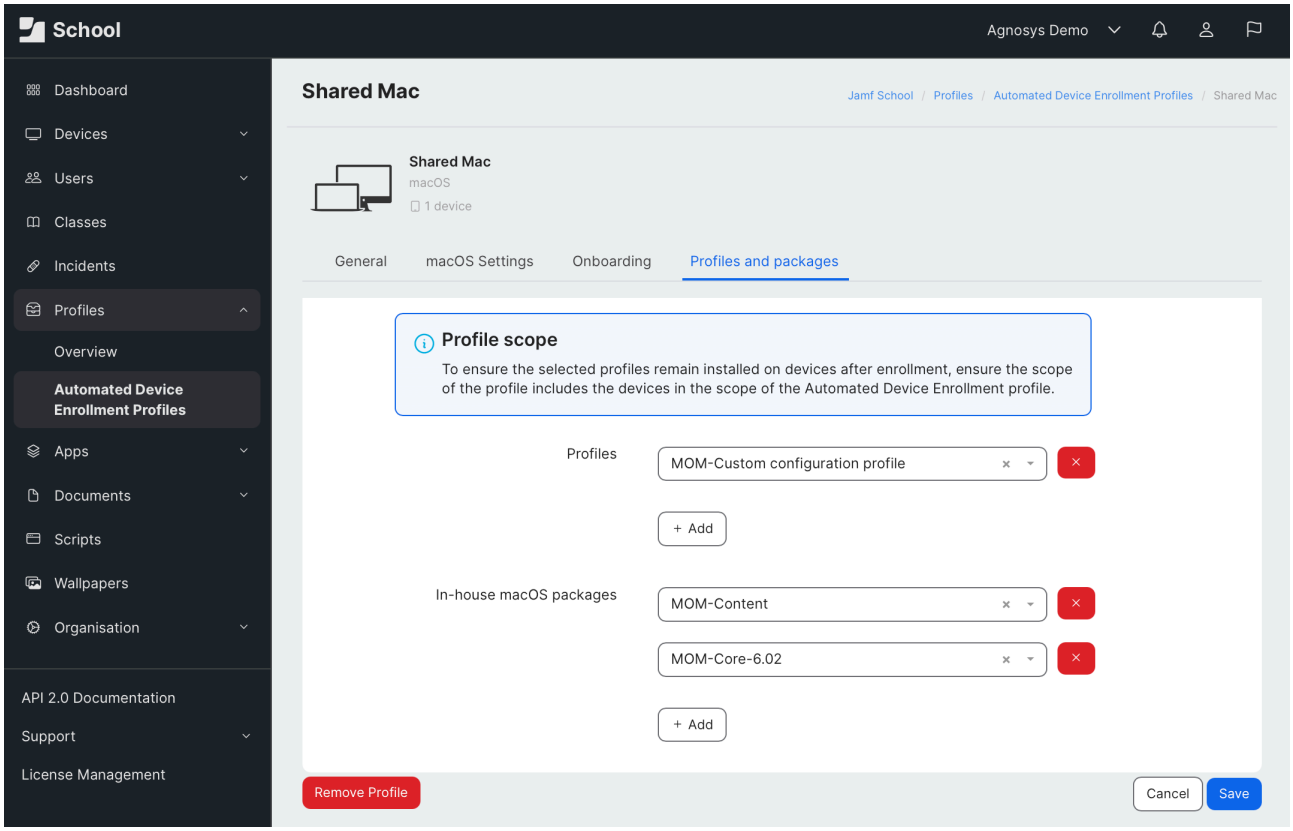
Please note that there is no need to define an installation scope for this package.

MOM-Core package

The MOM-Core package is provisioned with the following steps :
- Apps > Inventory > Add App > Add In-House macOS Package
- Select "MOM-Core.pkg"
- Save

Please note that there is no need to define an installation scope for this package.

Configuration of the Automated Device Enrollment profile



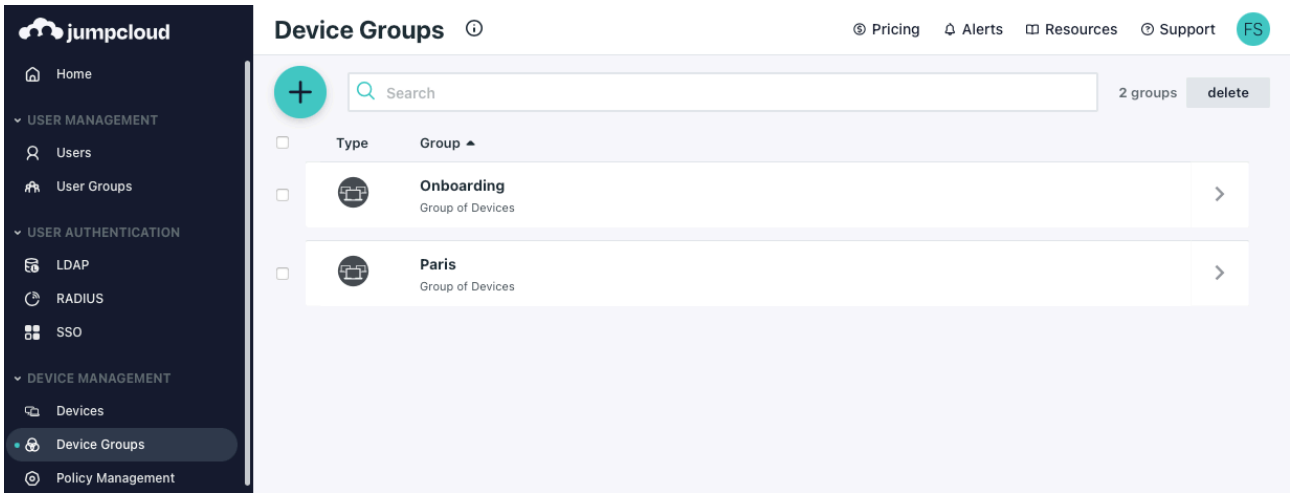
The Automated Device Enrollment Profile profile is provisioned with the following steps :
- Profiles > Automated Device Enrollment Profiles > Shared Mac
- Profiles and packages
- Profiles
    - click on "Add"
    - select profile > MOM-Custom configuration profile
- In-house macOS packages :
    - click on "Add"
    - select macOS package > MOM-Content
    - click on "Add
    - select macOS package > MOM-Core
    - click on "Save"

Provisioning JumpCloud for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

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 MacOnboardingMate.

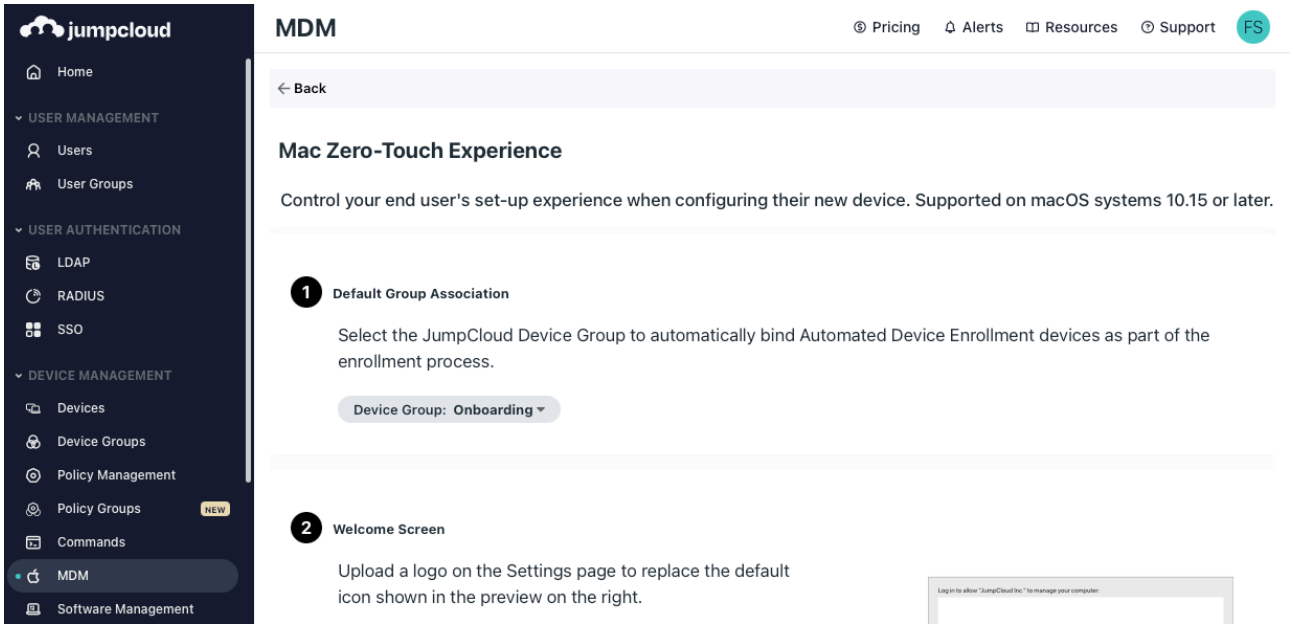
General configuration



Go to Device management > Device Groups and identify or create a device group (e.g. "Onboarding") to which devices will be automatically bound as part of the enrollment process.

Go to Device management > MDM > Automated Device Enrollment Configuration.

Click on "configure macOS".



At step 1, select the targeted device group (e.g. "Onboarding").

Configure the other settings and click on "save".

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 : MOM-Custom configuration profile
    - Settings > upload file : com.agnosys.config.JumpCloud.Onboarding.MOM.mobileconfig
- Select the "Device Groups" tab then select the "Onboarding" device group
- Save

MOM-Content package

The MOM-Content package is provisioned with the following steps :
- Device Management > Software Management
- Apple > "+" button > JumpCloud Private Repo
- From the "Details" tab :
    - Application Name : MOM-Content
    - Choose A File > MOM-Content.pkg > Upload
- Select the "Device Groups" tab then select the "Onboarding" 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.

MOM-Core package

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

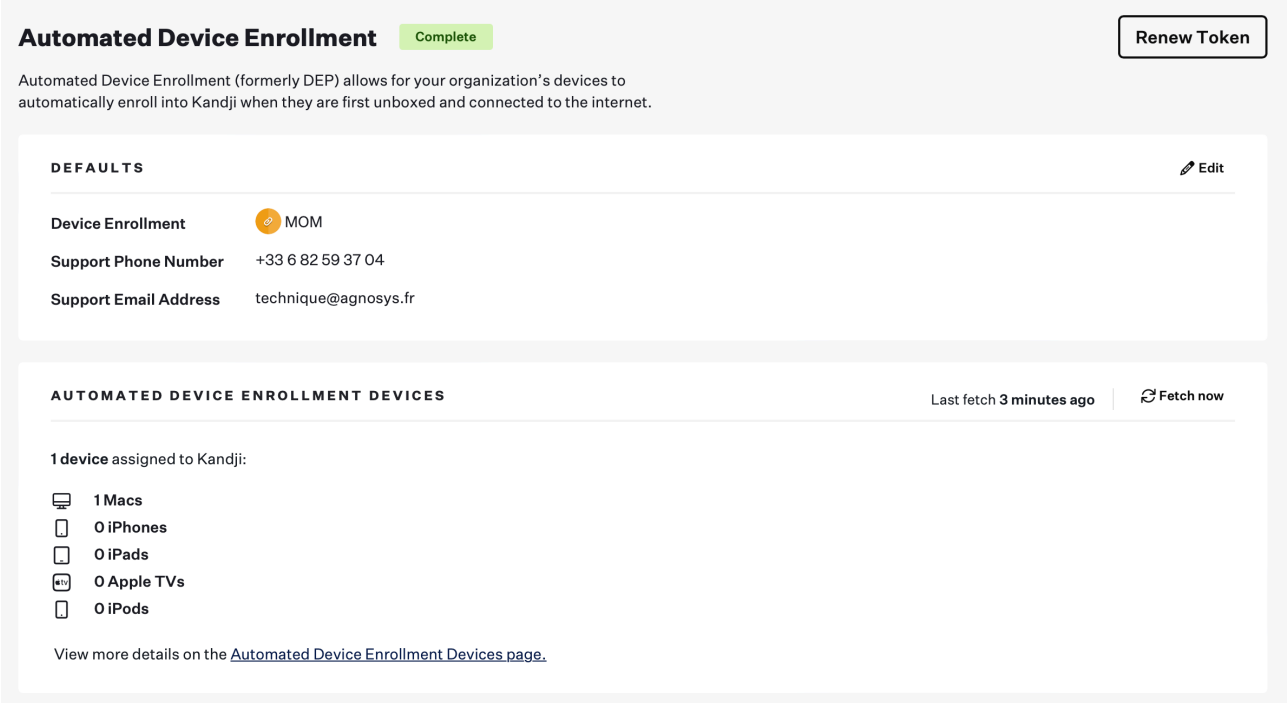
If you need to update the package, delete the configuration and start it over.

Provisioning Kandji for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-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 MacOnboardingMate.

General configuration



In this example, the devices enrolled using Automated Device Enrollment are assigned to the "MOM" Blueprint. An Automated Device Enrollment Configuration is associated to this Blueprint so the enrolled devices inherit its Library Items.

Custom configuration profile

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

- Save

MOM-Content package

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

MOM-Core package

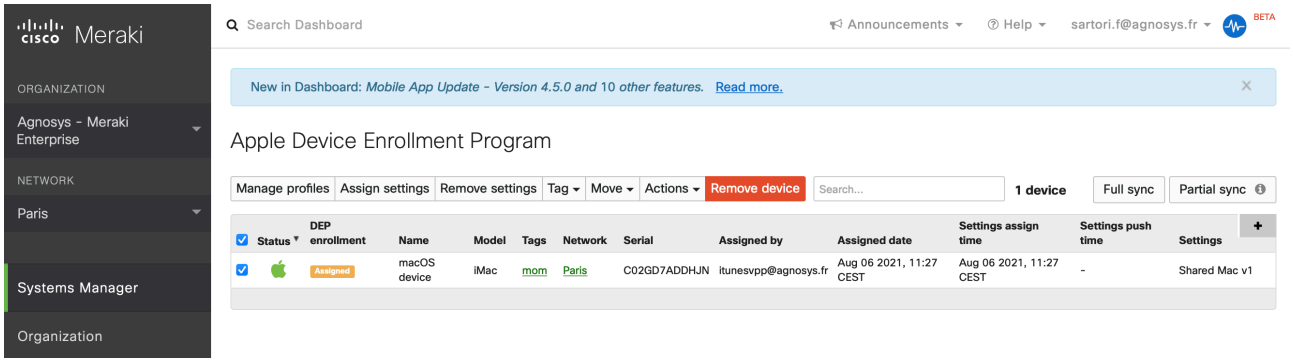
The MOM-Core package is provisioned with the following steps :
- Library > Add new > General > Custom Apps > Add & Configure
- Title : MOM-Core
- Assignment :
    - Blueprint : MOM
- Settings :
    - Installation : Install once per device
    - Install Details
        - Installer Package
        - Installer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

Provisioning Meraki Systems Manager for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-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 MacOnboardingMate.

General configuration



In this example, the devices are part of the "Paris" network and associated to the "mom" 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

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.Meraki_Systems_Manager.Paris.MOM.mobileconfig
- Deploy channel : Device
- Scope > Manual > with ANY of the followings tags
- Device tags : mom
- Save

MOM-Content package

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

MOM-Core package — Via Apps

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

MOM-Core package — Via Provisioning Packages

This alternative does not provide additional benefit.

The MOM-Core package is provisioned with the following steps :
- Systems Manager > Manage > ADE
- Manage profiles > Manage provisioning packages
- Add package
- Name : MOM-Core
- Package Upload > Upload : MOM-Core.pkg
- Save

Wait until the Status is "live" then create a new ADE Setting and add at the step "4 - macOS" the MOM-Core Package as the Provisioning Package. Assign the ADE Setting to the devices to onboard.

Provisioning Microsoft Intune for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

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 MacOnboardingMate.

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

In this example, the devices are part of an Automated Device Enrollment token named "Intune" and associated to a Profile named named "Shared Mac".

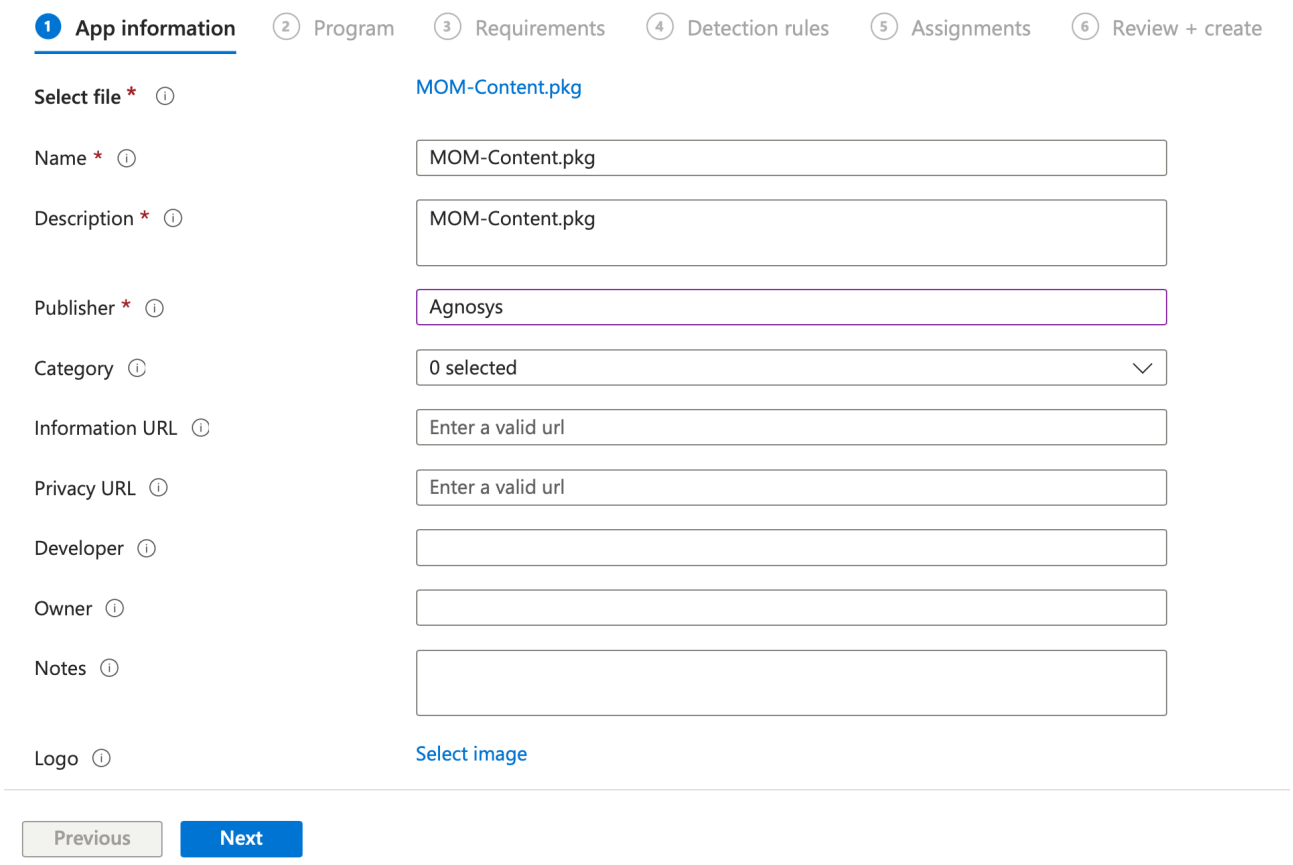
The scope of the components installation is here all devices but it should be a devices dynamic group containing only the Mac enrolled using Automated Device Enrollment.

Custom configuration profile

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

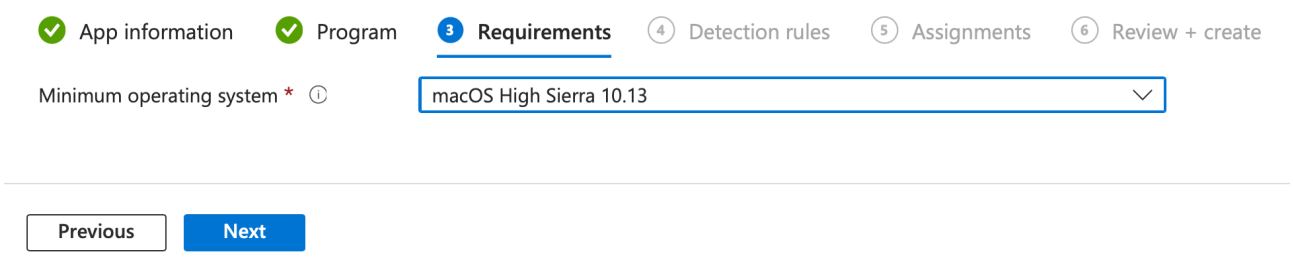
MOM-Content package

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

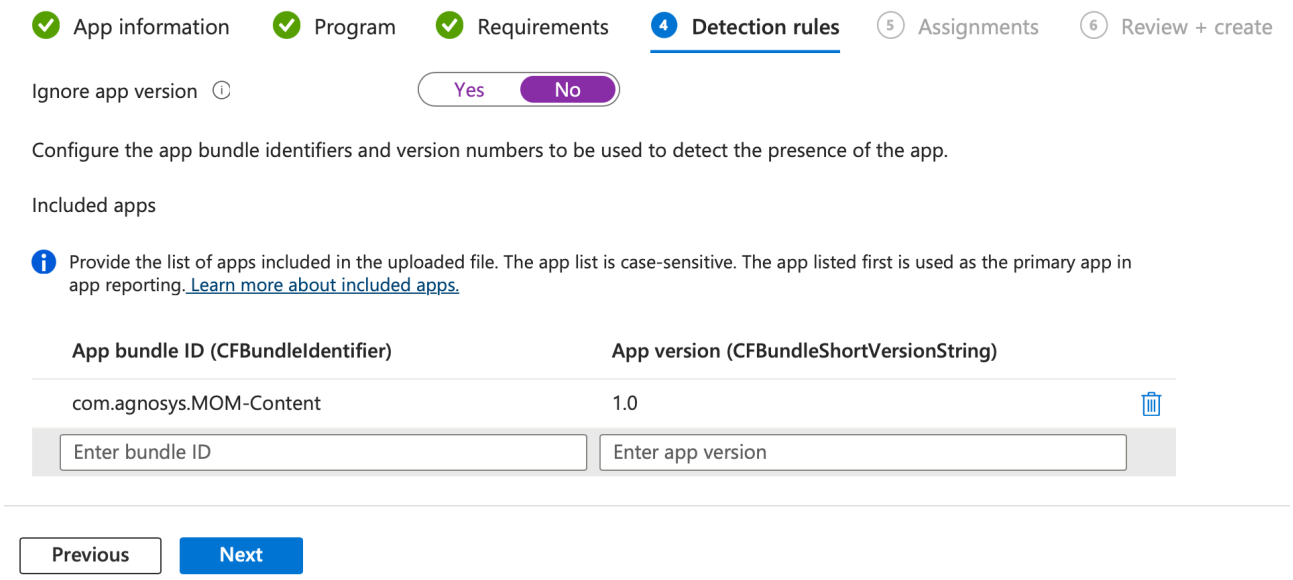


- App information
    - Select file > Select app package file
    - App package file > Select a file > MOM-Content.pkg > OK
    - Publisher : Agnosys

- Program : no scripts need to be configured



- Requirements
    - Minimum operating system : macOS High Sierra 10.13



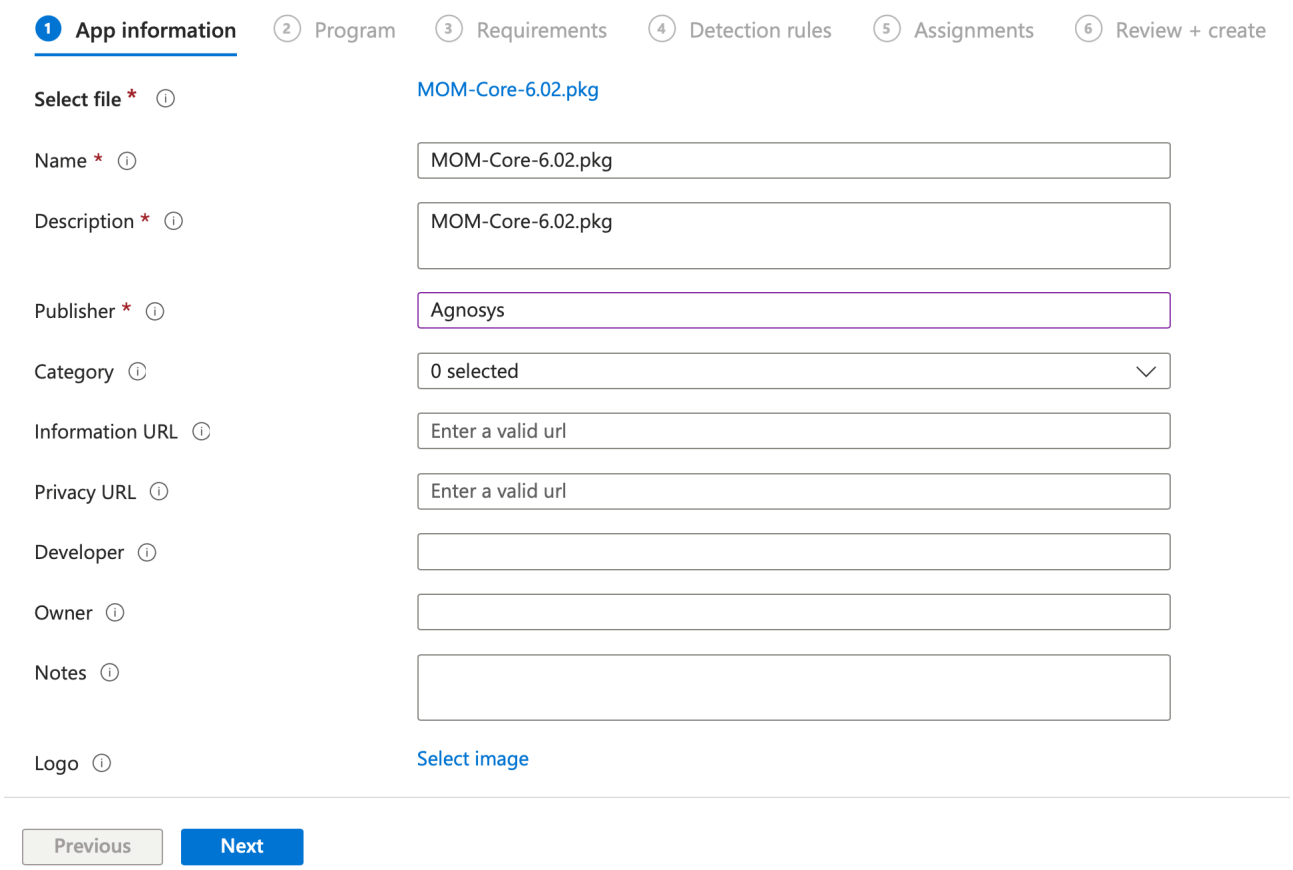
- Detection rules
    - Ignore app version : **No**
    - Detection method table :
        - App bundle ID : **com.agnosys.MOM-Content**
          Warning : Keep only this App bundle ID if others have been automatically added.
        - Build number : keep current value (e.g. 1.0)

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

- Review + create
    - Create

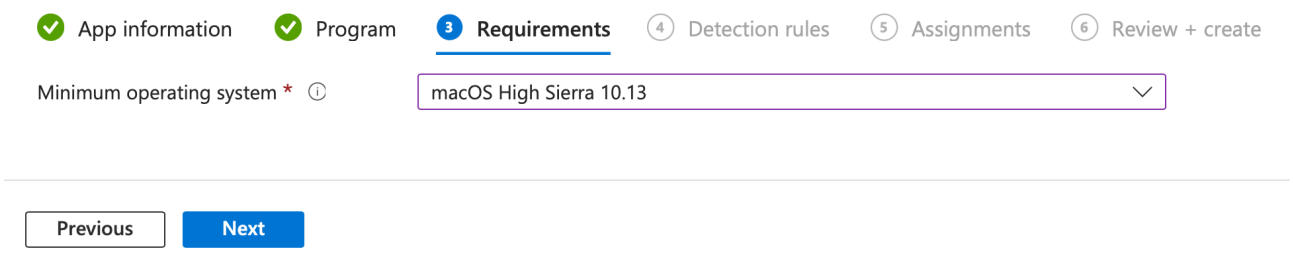
MOM-Core package

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

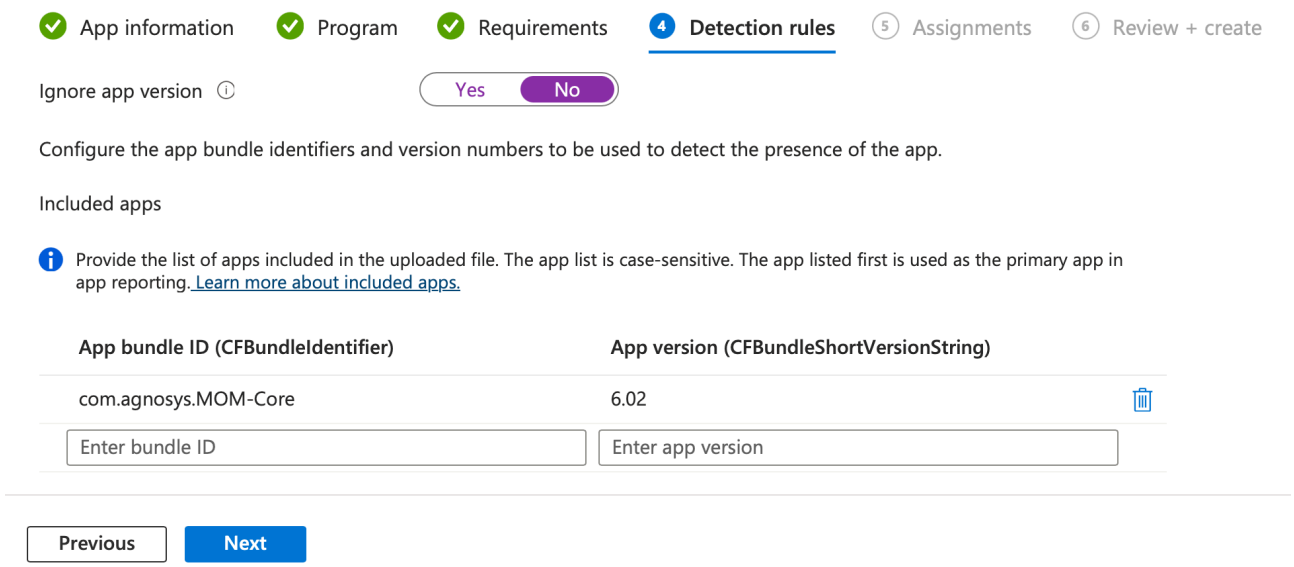


- App information
    - Select file > Select app package file
    - App package file > Select a file > MOM-Core.pkg > OK
    - Publisher : Agnosys

- Program : no scripts need to be configured



- Requirements
    - Minimum operating system : macOS High Sierra 10.13



- Detection rules
    - Ignore app version : **No**
    - Detection method table :
        - App bundle ID : **com.agnosys.MOM-Core**
        - App version : keep current value (e.g. 6.02)

- Assignments
    - Required : Add all devices

- Review + create
    - Create

Provisioning Miradore for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

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 MacOnboardingMate.

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.Miradore.Paris.MOM.mobileconfig
- Name : MOM-Custom configuration profile > Create

MOM-Content package

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

MOM-Core package

The MOM-Core package is defined with the following steps :
- Management > Applications > Applications tab > Add
- macOS application > PKG (Uploaded)
- File > Select file > MOM-Core.pkg
- Application name : MOM-Core
- Bundle identifier : com.agnosys.MOM-Core
- Version : the version imported (e.g. 4.26)
- 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 : MOM
- Double-click on the Business policy
- Add > Application > Check MOM-Content and MOM-Core > Add
- Add > Configuration profile > Check MOM-Custom configuration profile > Add
- Click on the Items tab and check the Business policy content
- Click on "Enable"

Provisioning Mosyle Business for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-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 MacOnboardingMate.

General configuration

In this example, the devices are part of an Automated Device Enrollment token named "Mosyle Business" and associated to the default Automated Device Enrollment profile named "Shared Mac".

In Management > Devices > Device Groups, a Device Group "Agnosys > Paris" was created with the following criterion :
DEP Profile — is/are — Shared Mac

As a result, any enrolled Mac associated to the "Shared Mac" profile will be member of the device group "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 : MOM-Custom configuration profile
- Select the file > com.agnosys.config.Mosyle_Business.Paris.MOM.mobileconfig
- Profile Assignment > Add Assignment > Device Enrollment > Devices from specific Device Groups > Paris > Tick
- Save

MOM-Content package

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

The MOM-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 > MOM-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 MOM-Content package is **signed** :
    - Management Profiles > Install PKG > PKGs > com.agnosys.pkg.MOM-Content
    - Enable "This app is Signed"
    - Save

The MOM-Content package is provisioned with the following steps :
- Management > macOS
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : MOM-Content
- Add application > Enterprise Apps > com.agnosys.pkg.MOM-Content > Tick
- **Only** if the MOM-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

MOM-Core package — Via Management Profile

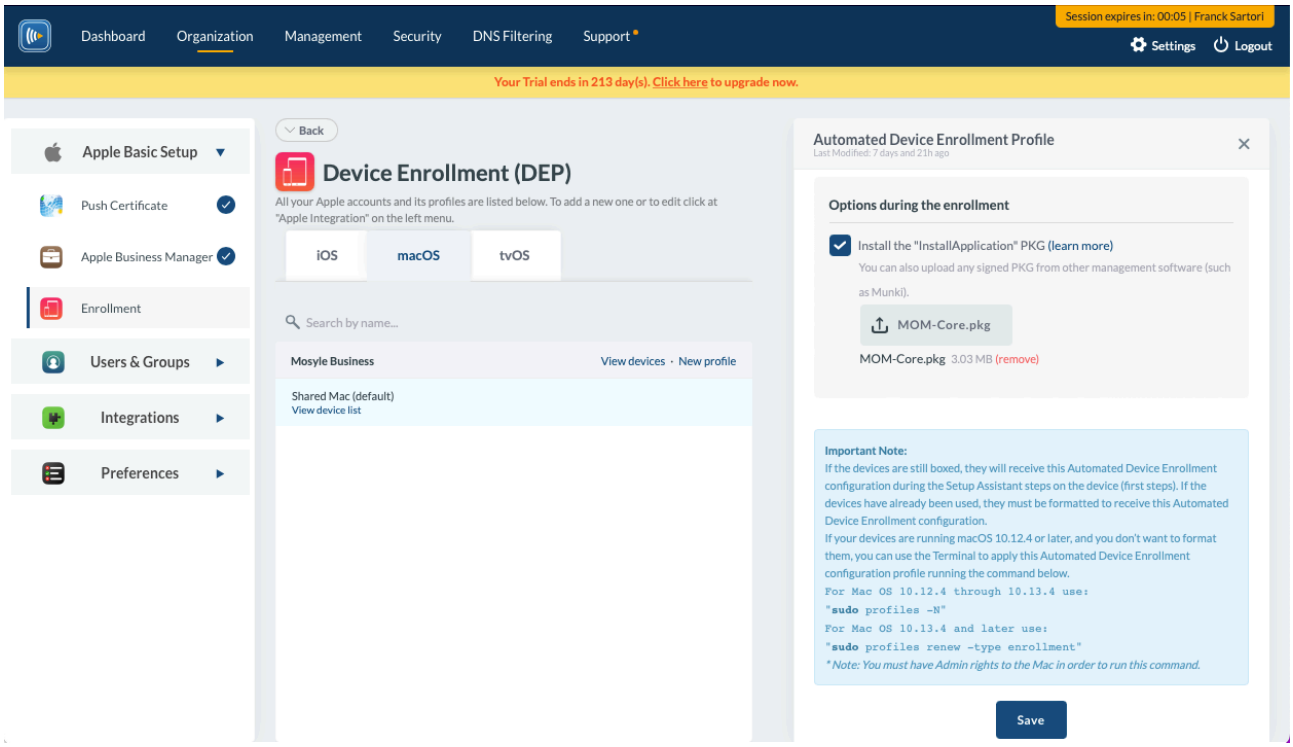
Mosyle FUSE offers to host packages in Mosyle's CDN. With Mosyle Business Premium, the MOM-Core package must be hosted on your own Web server.

The MOM-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 > MOM-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 > com.agnosys.pkg.MOM-Core
- Enable "This app is Signed"
- Save

The MOM-Core package is provisioned with the following steps :
- Management > macOS
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : MOM-Core
- Add application > Enterprise Apps > com.agnosys.pkg.MOM-Core > Tick
- 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

MOM-Core package — Via InstallApplication

This alternative requires less steps but does not provide additional benefit.



The MOM-Core package is provisioned with the following steps :
- Organization > Apple Basic Setup > Enrollment > macOS > Automated Device Enrollment
- Shared Mac (default) > Options during the enrollment
- Enable "Install the InstallApplication PKG"
- Upload new file > select "MOM-Core.pkg"
- Save

Provisioning Mosyle Manager for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-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 MacOnboardingMate.

General configuration

In this example, the devices are part of an Automated Device Enrollment token named "Mosyle Manager" and associated to the default Automated Device Enrollment profile named "Shared Mac".

In Management > Device Groups, a Device Group "Paris" was created with the following criterion :
DEP Profile — is/are — Shared Mac

As a result, any enrolled Mac associated to the "Shared Mac" profile will be member of the device group "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 : MOM-Custom configuration profile
- Select the file > com.agnosys.config.Mosyle_Manager.Paris.MOM.mobileconfig
- Profile Assignment > Select specific users or devices
- Select the users and devices > Assign to Device Groups > Select > Paris > Tick
- Save

MOM-Content package

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

The MOM-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 MOM-Content package is **signed** :
    - Management Profiles > Install PKG > PKGs > com.agnosys.pkg.MOM-Content
    - Enable "This app is Signed"
    - Save

The MOM-Content package is provisioned with the following steps :
- macOS > Management
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : MOM-Content
- Add application > Enterprise Apps > com.agnosys.pkg.MOM-Content > Tick
- **Only** if the MOM-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

MOM-Core package — Via Management Profile

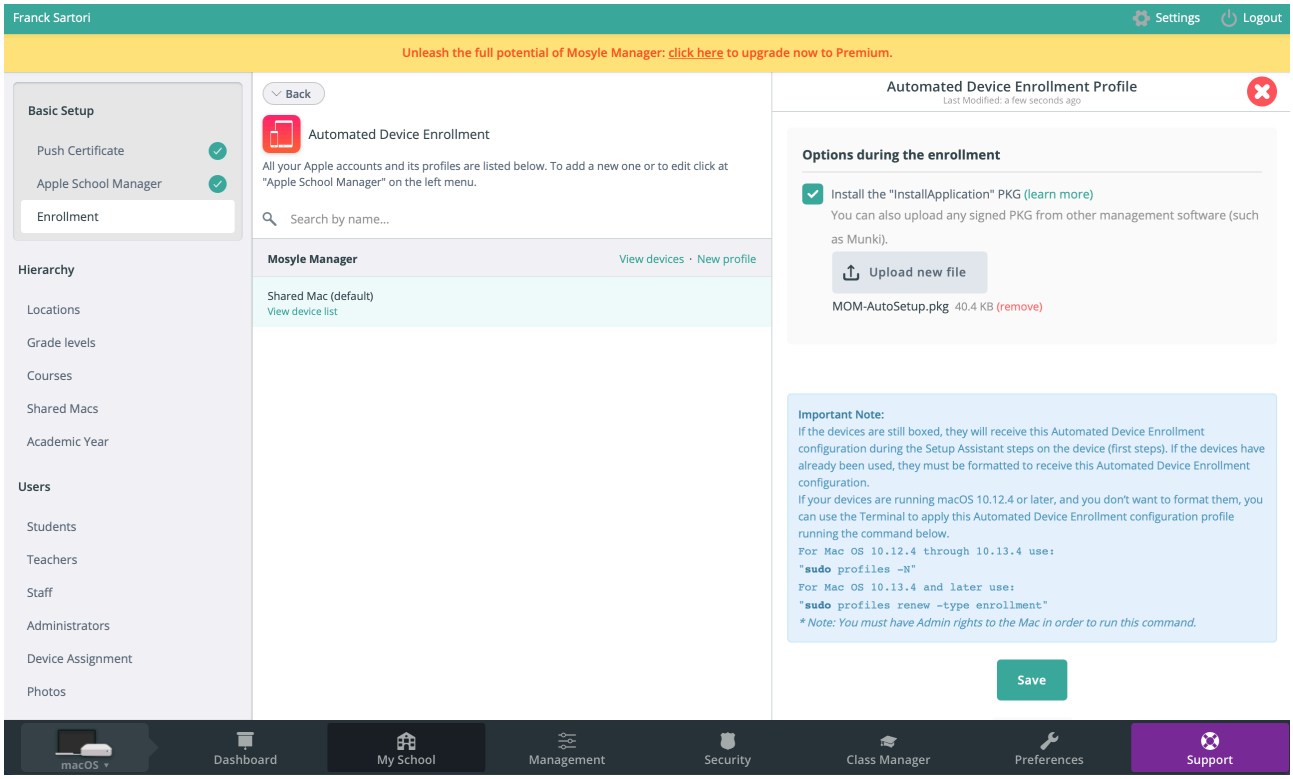
The MOM-Core package is hosted on a Web server.

The MOM-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 > com.agnosys.pkg.MOM-Core
- Enable "This app is Signed"
- Save

The MOM-Core package is provisioned with the following steps :
- macOS > Management
- Management Profiles > Install PKG > Profiles > Add new profile
- Name : MOM-Core
- Add application > Enterprise Apps > com.agnosys.pkg.MOM-Core > Tick
- 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

MOM-Core package — Via InstallApplication

This alternative requires less steps but does not provide additional benefit.



The MOM-Core package is provisioned with the following steps :
- macOS > My School > Basic Setup > Enrollment > Automated Device Enrollment
- Shared Mac (default) > Options during the enrollment
- Enable "Install the InstallApplication PKG"
- Upload new file > select "MOM-Core.pkg"
- Save

Provisioning SimpleMDM for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package
- the MOM-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 MacOnboardingMate.

General configuration

In this example, the devices are part of an Enrollment with type "Automated Enrollment" named "SimpleMDM" and configured with an initial device group named "Paris".

As a result, any enrolled Mac associated with this Enrollment will be member of the device group "Paris".

Custom configuration profile

The Custom configuration profile is provisioned with the following steps :
- Configs > Profiles > Create Profile > Custom Configuration Profile
- Name : MOM-Custom configuration profile
- Mobileconfig > Choose File > com.agnosys.config.SimpleMDM.Paris.MOM.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
- MOM-Custom configuration profile > Assign

MOM-Content package

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

The MOM-Content package is provisioned with the following steps :
- Apps & Media > Assignment
- Create Assignment Group
    - Name : MacOnboardingMate
    - Type : Standard — Auto deploy enabled
    - Save
- MacOnboardingMate
    - Search for an app or media to add > MOM-Content.pkg
    - Search for a group or device to add > Paris

MOM-Core package

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

The MOM-Core package is provisioned with the following steps :
- Apps & Media > Assignment
- MacOnboardingMate (previously created)
    - Search for an app or media to add > MOM-Core.pkg
    - Search for a group or device to add > Paris

Provisioning VMware Workspace ONE for AutoLauncher mode

Three components must be automatically deployed once the device is enrolled to achieve the onboarding :
- a Custom configuration profile
- a MOM-Content package (signed or unsigned package)
- the MOM-Core package.

Because VMware Workspace ONE offers to deploy multiple packages in the context of Automated Device Enrollment, these instructions plans that the two packages are eventually installed as Bootstrap Packages. The only counterpart is that signing the MOM-Content package is a requirement. However, this procedure provides an alternative to this ideal deployment path if the MOM-Content package cannot be signed.

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 MacOnboardingMate.

General configuration

In this example, the devices are part of an Automated Device Enrollment token named "Workspace ONE" and associated to a Profile named named "Shared Mac".

The scope of the components installation is here all devices but it should be a devices dynamic group containing only the Mac enrolled using Automated Device Enrollment.

Custom configuration profile

Open the VMware Workspace ONE console.

Go to Resources > Profiles & Baselines > Profiles.

Click on "Add" > "Add Profile".

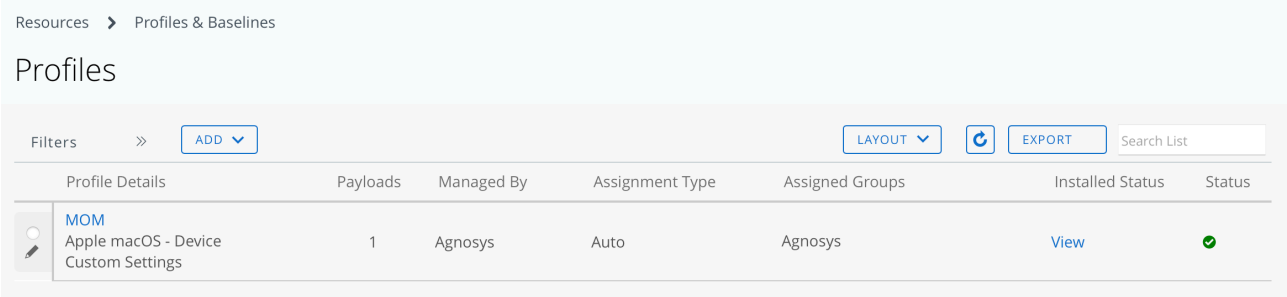
Select the platform "macOS" then click on "Device Profile".

Name the configuration profile (e.g. "MOM") and optionally add a description (e.g. "MOM 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 devices that are to be prepared with MOM. Click on "Save and Publish".

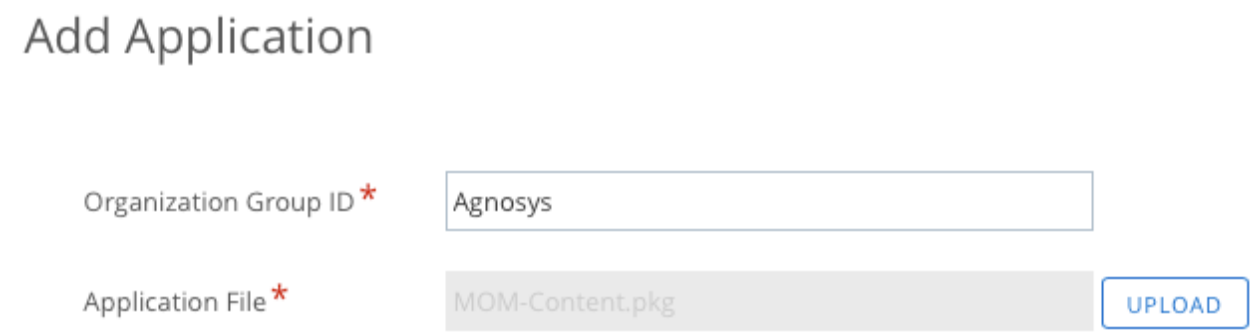
Check that the Custom configuration profile is published and assigned.

MOM-Content package (signed package)

This section only applies if the MOM-Content package is **signed**. In this situation, the package can be deployed as a Bootstrap Package with the "Expedited Delivery" deployment type.

Open the VMware Workspace ONE console.

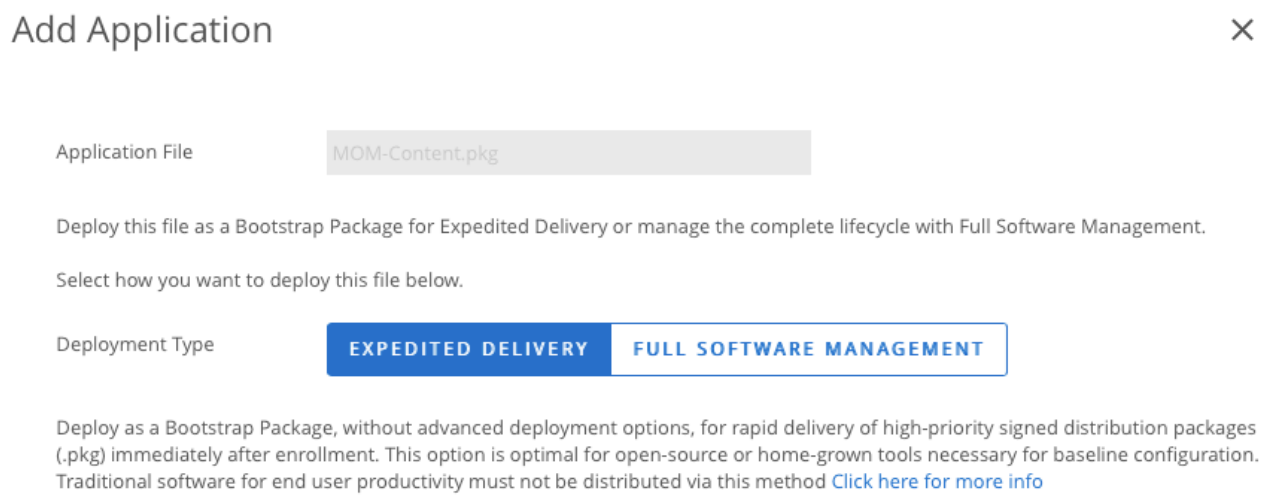
Go to Resources > Apps > Native.
Click on "Add" > "Application File".



Select the Organization Group that encompasses the devices that are to be prepared with MOM.

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

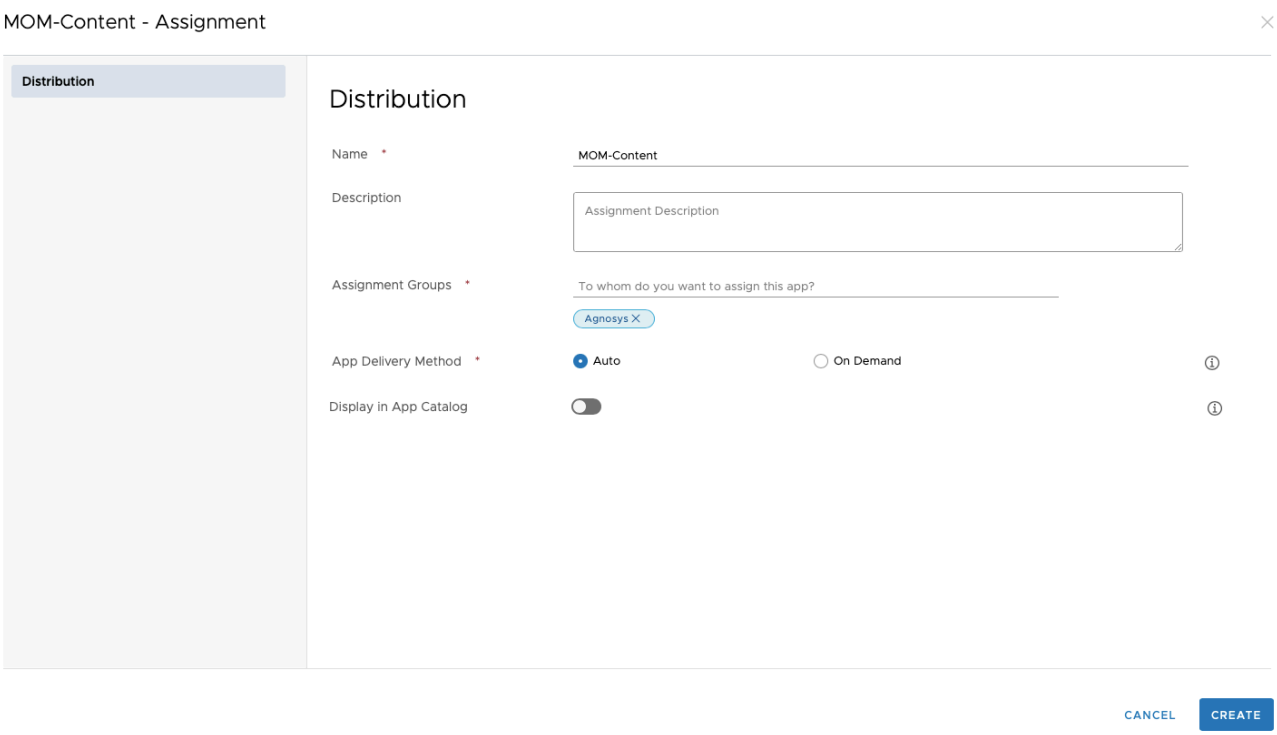
Click on "Continue".



Select "Expedited Delivery".

Click on "Continue".

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

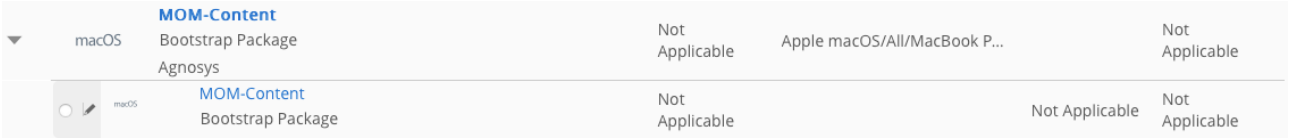


Complete the assignment form :
- Name : MOM-Content
- Assignment Groups : select the Organization Group that encompasses the devices that are to be prepared with MOM
- App Delivery Method : Auto
- Display in App Catalog : disabled.

Click on "Create".

In the Assignment pane, click on "Save".

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



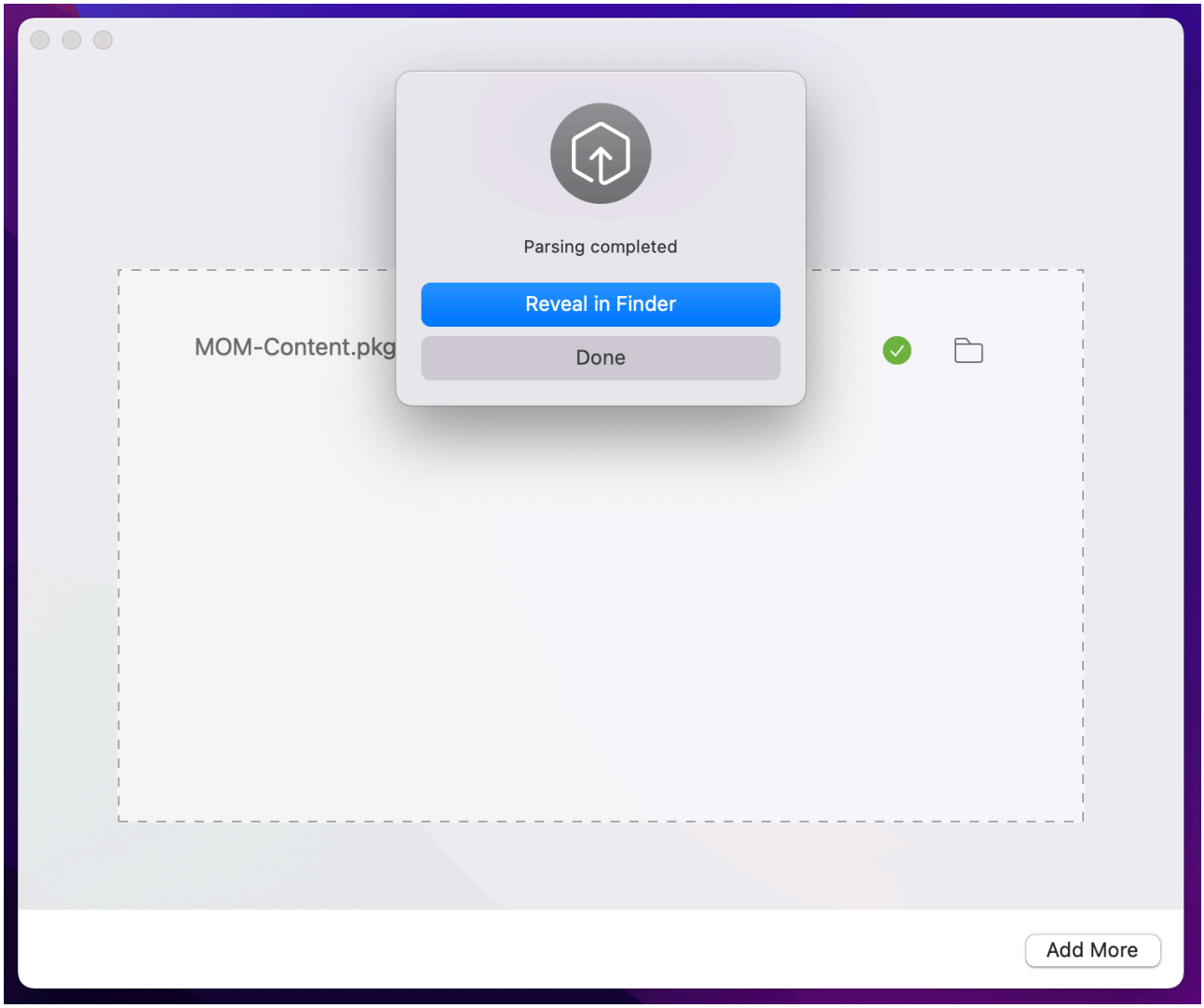
Go to Resources > Apps > Native and check that the application is published and assigned.

MOM-Content package (unsigned package)

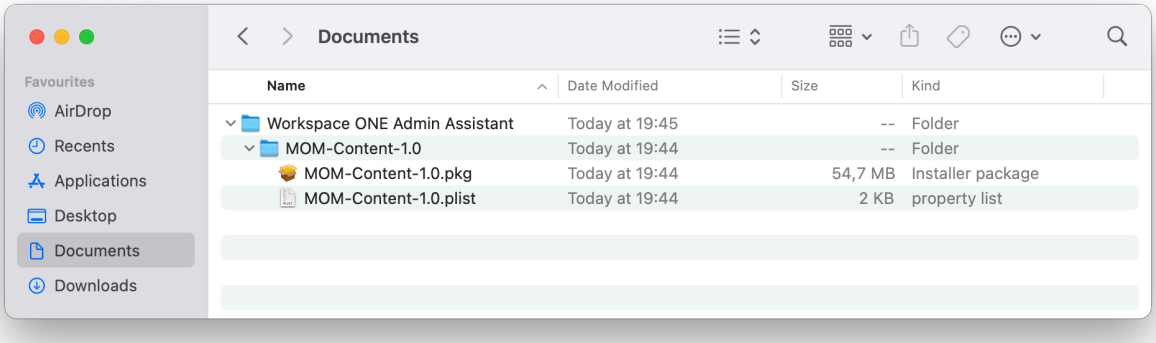
This section only applies if the MOM-Content package is **unsigned**. In this situation, the package cannot be deployed as a Bootstrap Package with the "Expedited Delivery" deployment type. Thus, it must be deployed as a regular package with the "Full Software Management" deployment type, which adds extra steps.

Open /Applications/Workspace ONE Admin Assistant.

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



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

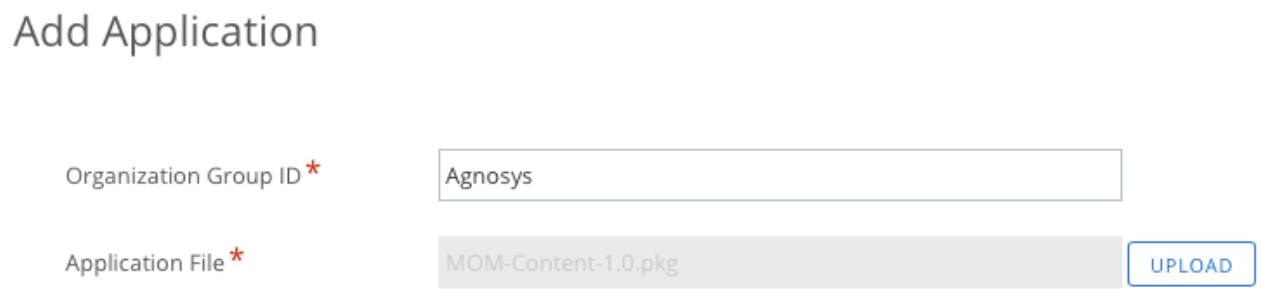


Identify the package and its associated property list file that are both going to be uploaded.

Open the VMware Workspace ONE console.

Go to Resources > Apps > Native.

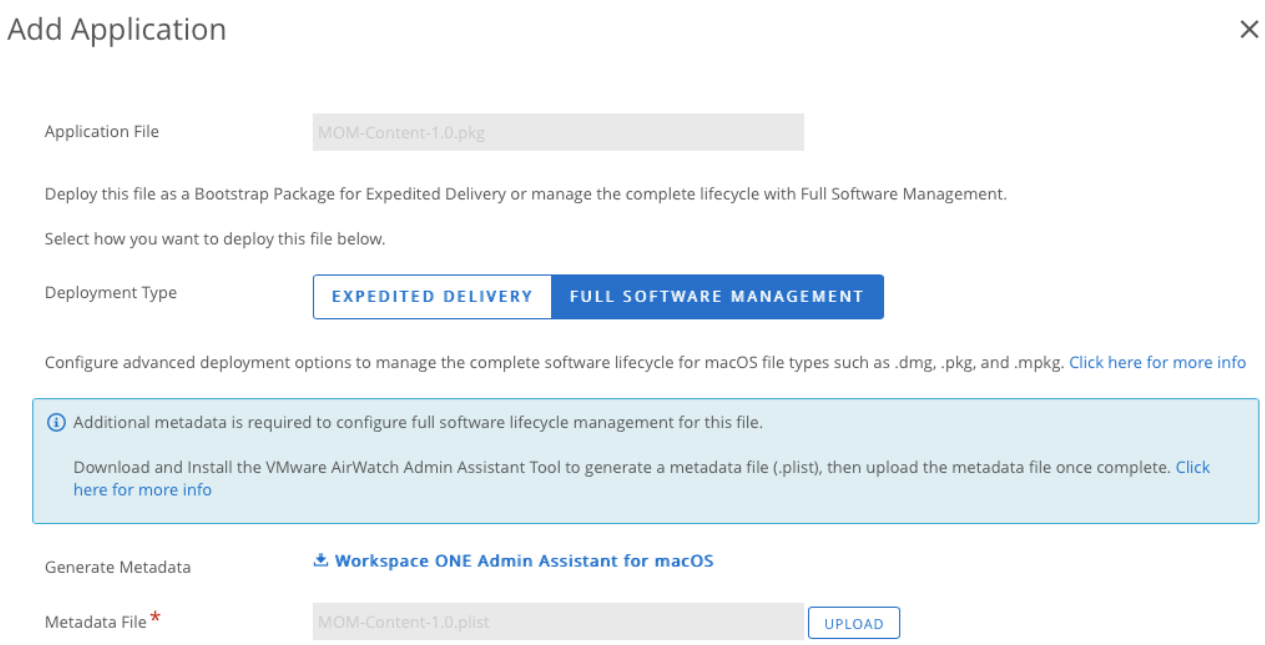
Click on "Add" > "Application File".



Select the Organization Group that encompasses the devices that are to be prepared with MOM.

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

Click on "Continue".

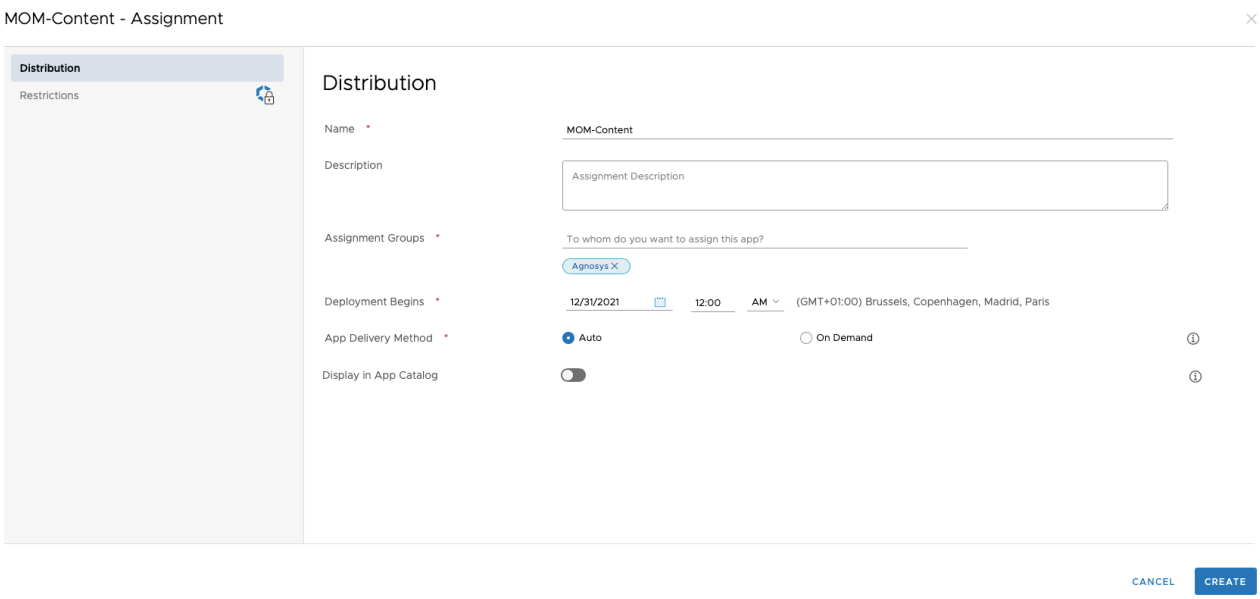


Select "Full Software Management".

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 : MOM-Content
- Assignment Groups : select the Organization Group that encompasses the devices that are to be prepared with MOM
- App Delivery Method : Auto
- Display in App Catalog : disabled.

Click on "Create".

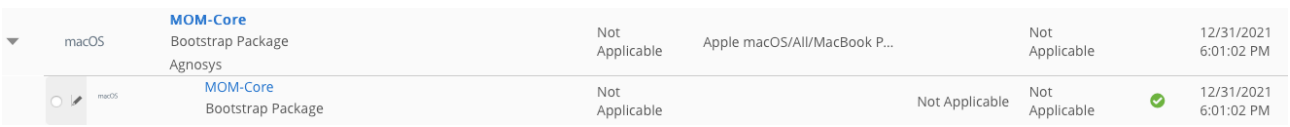
In the Assignment pane, click on "Save".

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

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

MOM-Core package

Reproduce the same steps as for the MOM-Content package (signed package) :
- add the MOM-Core package as a native application
- deploy the application to the same devices using "Expedited Delivery".



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

Implementing provisioning over the Setup Assistant or Login Window

This section applies to implementing MacOnboardingMate for provisioning over the Setup Assistant or Login Window. All onboarding tasks are performed during these phases. Afterward, the Mac shuts down, restarts, or displays the Login Window, allowing an end user to log in.

MOM provisioning over the Setup Assistant or Login Window combined with macOS Automated Device Enrollment offers a similar feature as Windows Autopilot for pre-provisioned deployment. From the end user's perspective, the User-driven experience remains unchanged, but getting their Mac to a fully provisioned state is faster.

The graphical interface for provisioning over the Setup Assistant, previously referred to as "White Glove Provisioning" in MacOnboardingMate v5, is demonstrated in this online video.

The key concept behind MOM provisioning over the Setup Assistant or Login Window is that MOM is displayed on top of the Setup Assistant or Login Window, which continues to run in the background. During onboarding over the Setup Assistant, the hidden pane should be the "Time Zone" pane, whose setting can be configured automatically by MOM.

The workflow showcased in the aforementioned online video does not display the "Create a Computer Account" pane during the provisioning over the Setup Assistant.

When this pane is skipped, the workflow must ensure that the end user can create an account via a mechanism of your choice once the device is provisioned. This account can be a local account when using a third party login window (e.g. Jamf Connect, XCreds, Mosyle Auth 2, NoMAD Login AD, etc.), or a mobile account when using traditional AD binding (which is not recommended).

When this pane is not skipped, MOM is displayed on top of the Setup Assistant as soon as the defined local account is detected as created.

The "End User License Agreement" and "Device customization" steps are optional, so the provisioning can be automated once the Remote Management pane has been passed.

The user experience is also detailed in the "Onboarding a Mac using MOM in AutoLauncher mode" chapter.

Requirements for provisioning over the Setup Assistant

• The MDM must be provisioned for AutoLauncher mode.

• The MDM must support the installation of packages while the Setup Assistant is running.

To date, all supported MDM solutions are known to meet this requirement except Kandji.

• The UI Helper must be swiftDialog.

• The Automated Device Enrollment profile applied to devices to be provisioned is expected to skip all the Setup Assistant steps, except the "Create a Computer Account" pane if necessary (see above).

In the context of Jamf Pro, MOM Custom configuration profile must be checked in the Configuration Profiles pane of the Prestage Enrollment, but it does not have to be associated with a scope, as MOM caches its configuration at launch.

Requirements for provisioning over the Login Window

• The MDM must be provisioned for AutoLauncher mode.

• The MDM must support the installation of packages while the Login Window is displayed.

To date, all supported MDM solutions are known to meet this requirement.

• The UI Helper must be swiftDialog.

In the context of Jamf Pro, MOM Custom configuration profile must be checked in the Configuration Profiles pane of the Prestage Enrollment, but it does not have to be associated with a scope, as MOM caches its configuration at launch.

Location configuration file

Implementing over the Setup Assistant or Login Window involves editing keys which are detailed in the Dictionary.

Those that should be examined first are grouped below.

• **Keys located at the root level**

AWAITED_ITEMS : list of items awaited before the workflow can proceed with the Postflight script step, the Device inventory step and the landing pane ; the purpose of this list of path names and bundle names is to prevent the Mac from shutting down, restarting or displaying the Login Window before critical items have been installed, although a timeout can be set per item.

In the context of Jamf Pro, the awaited items step also includes waiting for the end of Jamf Pro policies detected as being in progress.

UIHELPER : set to "swiftdialog".

SWIFTDIALOG_URL : set to the URL used to download the swiftDialog package.

Note that provisioning over the Login Window is supported with swiftDialog 2.5.2 and later.

TIMEZONE : set to the name of a time zone from among those returned by the `systemsetup -listtimezones` command ; when MOM is displayed on top of the Setup Assistant and the hidden pane of the Setup Assistant should be the "Time Zone" pane, it is recommended to set the expected time zone.

Note that the following keys are ignored, so their corresponding capabilities are forcibly disabled :
- MGTACCOUNTFILEVAULT (FileVault enablement of the management account)
- MGTACCOUNTSECURETOKEN (SecureToken granting to the management account)
- MIGRATION_CHOOSE_INVENTORY_SOURCE (choice of the inventory source for Device Customization).

• **Provisioning over the Setup Assistant**

The following keys are located inside the PROVISIONING > OVER_SETUP_ASSISTANT Dictionary.

ATTEMPT : set to "true" to enable an attempt at onboarding over the Setup Assistant

FOCUS : set to "true" to blur the background while MOM is running

WAIT_LOCAL_ACCOUNT_CREATION :
- set to "true" if the Automated Device Enrollment profile is set to **display** the "Create a Computer Account" pane of the Setup Assistant (MOM waits for the end user account to be created before covering the Setup Assistant)
- set to "false" if the Automated Device Enrollment profile is set to **skip** the "Create a Computer Account" pane of the Setup Assistant (MOM does not wait for an end user account to be created before covering the Setup Assistant).

Note that MOM itself cannot set whether the Automated Device Enrollment profile plans to display or skip the "Create a Computer Account" pane of the Setup Assistant. Therefore, the key must be manually set to "true" or "false".

• **Provisioning over the Login Window**

The following keys are located inside the PROVISIONING > OVER_LOGIN_WINDOW Dictionary.

ATTEMPT : set to "true" to enable an attempt at onboarding over the Login Window

FOCUS : set to "true" to blur the background while MOM is running

• **Keys located inside the EXIT_ACTION Dictionary**

Provisioning over the Setup Assistant — COMMAND : "logout", "restart" and "shutdown" are supported ; "logout" causes the Mac to display the Login Window once provisioning is complete.

Provisioning over the Login Window — COMMAND : "undefined", "restart" and "shutdown" are supported ; "undefined" causes the Mac to display the Login Window once provisioning is complete.

COMMAND_DELAY : set to the time in seconds after which the "logout", restart" or "shutdown" is automatically triggered once the landing pane is displayed (set to "0" to disable the automation).

• **Companion keys to name the device**

COMPUTERNAME_CONFIG_AUTOLAUNCHER : this key should be set to "template" (computer name derived from a template) or "csv" (computer name retrieved from a CSV file).

COMPUTERNAME_CSV : the CSV file that dictates the computer name.

COMPUTERNAME_TEMPLATE : the template that dictates the computer name (:ModelName:, :Random[digits:*n*][padding:true|false]:, :SerialNumber: and :SerialNumber[length:*n*][truncate:start|end]: are available variables).

The Settings pane for manual naming or definition of device attributes is fully supported with provisioning over the Setup Assistant or Login Window, but implies an interaction.

• **Companion keys to ease third party login window installation**

JAMF_CONNECT_INTEGRATION and JAMF_CONNECT_CONFIGURATION (inside INTEGRATIONS Dictionary) : installation and enablement of Jamf Connect.

NOMAD_INTEGRATION and NOMAD_CONFIGURATION (inside INTEGRATIONS Dictionary) : installation and enablement of NoMAD Login AD.

XCREDS_INTEGRATION and XCREDS_CONFIGURATION (inside INTEGRATIONS Dictionary) : installation of XCreds.

Mosyle Auth 2 installation is entirely under Mosyle Business or Mosyle Manager governance.

• **Companion keys to ease software installations**

HOMEBREW_INTEGRATION and HOMEBREW_CONFIGURATION > FORMULAE : installation of packages identified by their formula name.

INSTALLOMATOR_INTEGRATION and INSTALLOMATOR_CONFIGURATION > LABELS : installation of the latest available software titles identified by their label name.

JAMF_PRO_INTEGRATION and JAMF_PRO_CONFIGURATION > JAMF_PRO_POLICIES > LIST (inside INTEGRATIONS Dictionary) : execution of Jamf Pro Policies triggered by their Custom event or Identifier.

MUNKI_INTEGRATION and MUNKI_CONFIGURATION > MUNKI_CHECKINAFTERSETUP (inside INTEGRATIONS Dictionary) : installation of the packages planned for the onboarded device.

Implementing MOM for MDM switching

This section applies to implement MacOnboardingMate to ease the transition between 2 MDM, and migrate Mac and device details from one MDM to another MDM, using both Launcher or AutoLauncher modes.

MDM switching using Launcher mode

Let's consider that a device in production must be migrated from "MDM A" to "MDM B".

The migration configuration is all defined by migration dedicated keys in the Location configuration file.

If no inventory values must be migrated during the device exodus, the "MIGRATION_ATTRIBUTE_REDIRECTS" key is not required in the "MDM B" location configuration file. In this context, the migration is limited to an unenrollment from "MDM A" followed by an enrollment in "MDM B" with facilitation options.

If selected inventory values must be migrated during the device exodus, the "MDM B" location configuration file must contain migration keys relative to "MDM A". The required keys are the "MDM A" solution name, the required informations to make authenticated API calls towards "MDM A" and the attribute redirections between "MDM A" and "MDM B".

Let's say that the attribute "**Tags**" in "MDM A" must be redirected to the attribute "**Asset Tag**" in "MDM B". During the migration process, MOM will use the "MDM A" informations to create a local device inventory containing this redirected attribute, unenroll the device from "MDM A", enroll the device in "MDM B" and eventually use the local device inventory to update the device details in "MDM B".

Please note that if the "MDM B" location configuration file plans to offer the editing of the attribute "Asset Tag" during the customization, the value of attribute "Tags" will be used as a placeholder and the final value of the attribute "Asset Tag" will be updated in "MDM B". The redirected attributes not planned for editing have their values directly copied as is from "MDM A" to "MDM B".

If the migrated device must be enrolled in "MDM B" with Automated Device Enrollment, in this context invoked by MacOnboardingMate and not by the Setup Assistant, please ensure that the targeted device is already provisioned for an automated enrollment in AxM and "MDM B" before the migration process is triggered. Otherwise, the device may silently migrate from "MDM A" to "MDM A" while executing a workflow planned for an enrollment in "MDM B".

MDM switching using AutoLauncher mode

Two scenarios must be considered :
- the device is in production, currently enrolled in "MDM A", and must be migrated to "MDM B"
- the device was enrolled in "MDM A", was resetted and is now provisioned to enroll in "MDM B" during the Setup Assistant using Automated Device Enrollment.

Scenario #1 — The device is in production, currently enrolled in "MDM A", and must be migrated to "MDM B"

Let's consider that a device in production must be migrated from "MDM A" to "MDM B".

The migration configuration is all set up in "MDM A" for MOM-Core, MOM-Content and "MDM B" configuration profile with migration dedicated keys. The migration from "MDM A" to "MDM B" is therefore under the gouvernance of "MDM A".

Planning the migration for devices in production, the main focus is to ensure that only the targeted devices receive those three components and therefore the others won't trigger a migration process inadvertently. Depending of your MDM capabilities, you may use dedicated smart or static device groups, and trigger the migration process manually from a Self Service instead of automatically.

If no inventory values must be migrated during the device exodus, the "MIGRATION_ATTRIBUTE_REDIRECTS" key is not required in the "MDM B" configuration file. In this context, the migration is limited to an unenrollment from "MDM A" followed by an enrollment in "MDM B" with facilitation options.

If selected inventory values must be migrated during the device exodus, the "MDM B" configuration file must contain migration keys relative to "MDM A". The required keys are the "MDM A" solution name (and location name in the context of Meraki Systems Manager), the required informations to make authenticated API calls towards "MDM A" and the attribute redirections between "MDM A" and "MDM B".

Let's say that the attribute "**Tags**" in "MDM A" must be redirected to the attribute "**Asset Tag**" in "MDM B". During the migration process, MOM will use the "MDM A" informations to create a local device inventory containing this redirected attribute, unenroll the device from "MDM A", enroll the device in "MDM B" and eventually use the local device inventory to update the device details in "MDM B".

Please note that if the "MDM B" configuration file plans to offer the editing of the attribute "Asset Tag" during the customization, the value of attribute "Tags" will be used as a placeholder and the final value of the attribute "Asset Tag" will be updated in "MDM B". The redirected attributes not planned for editing have their values directly copied as is from "MDM A" to "MDM B".

If the migrated device must be enrolled in "MDM B" with Automated Device Enrollment, in this context invoked by MacOnboardingMate and not by the Setup Assistant, please ensure that the targeted device is already provisioned for an automated enrollment in AxM and "MDM B" before the migration process is triggered. Otherwise, the device may silently migrate from "MDM A" to "MDM A" while executing a workflow planned for an enrollment in "MDM B".

Scenario #2 — The device was enrolled in "MDM A", was reset and is now provisioned to enroll in "MDM B" during the Setup Assistant using Automated Device Enrollment.

In this scenario, the reset devices have an history in "MDM A". Rather than migrating devices in production, you may decide to reset the devices before onboarding them in "MDM B". In this context, MOM may help the MDM switching process by migrating selected inventory values of devices from "MDM A" to "MDM B" while the devices are directly enrolled in "MDM B" during Setup Assistant using Automated Device Enrollment.

Let's consider that a reset device is onboarded in "MDM B" grabbing selected inventory values of this device in "MDM A".

The onboarding configuration is all set up in "MDM B" for MOM-Core, MOM-Content and "MDM B" configuration profile with migration dedicated keys. The copy of selected inventory values from "MDM A" to "MDM B" is therefore under the gouvernance of "MDM B".

The "MDM B" configuration file must contain migration keys relative to "MDM A". The required keys are the "MDM A" solution name (and location name in the context of Meraki Systems Manager), the required informations to make authenticated API calls towards "MDM A" and the attribute redirections between "MDM A" and "MDM B".

Let's say that the attribute "**Tags**" in "MDM A" must be redirected to the attribute "**Asset Tag**" in "MDM B". During the onboarding process, MOM will use the "MDM A" informations to create a local device inventory containing this redirected attribute and eventually use the local device inventory to update the device details in "MDM B" after the device was enrolled.

Please note that if the "MDM B" configuration file plans to offer the editing of the attribute "Asset Tag" during the customization, the value of attribute "Tags" will be used as a placeholder and the final value of the attribute "Asset Tag" will be updated in "MDM B". The redirected attributes not planned for editing have their values directly copied as is from "MDM A" to "MDM B".

Implementing mSCP compliance

The macOS Security Compliance Project (mSCP) is a collaborative effort involving the National Institute of Standards and Technology (NIST), the National Aeronautics and Space Administration (NASA), the Defense Information Systems Agency (DISA), and Los Alamos National Lab (LANL). The project aims to develop and maintain security guidance for organizations that must adhere to specific security compliance frameworks and policies.

MOM integrates with mSCP to apply one of the supported security baselines at the end of the workflow. In addition to the Flight Recorder report, the mSCP compliance report, which includes a compliance score, is displayed in the Landing pane and can be shared via Slack and Teams webhooks.

References

This chapter outlines the key points for implementing mSCP compliance in MacOnboardingMate.

For more details, please consider the following suggestions :

• Official project documentation
https://github.com/usnistgov/macos_security

• Compliance Made Even Easier | JNUC 2023
https://www.youtube.com/watch?v=Xp7vvhm6fPc

• Implementing mSCP Using Jamf Pro | JNUC 2022
https://www.youtube.com/watch?v=hCq4PbLX0Tc

• Enforcing macOS Security Compliance Project Baselines: Workspace ONE Operational Tutorial
https://techzone.omnissa.com/resource/enforcing-macos-security-compliance-project-baselines-workspace-one-operational-tutorial

• Secure, Contain, Protect... Your Mac: Deploy mSCP with Intune
https://www.intuneirl.com/secure-contain-protect-your-data-deploy-mscp-with-intune/

To get straight to the point with a functional example, follow these instructions to generate a default CIS Benchmark - Level 1 compliance report using Jamf Pro or another MDM.

Step 1 : Generate compliance assets with Jamf Compliance Editor

Jamf Compliance Editor (JCE) is a native macOS app built on mSCP that generates compliance assets needed to assess and enhance the security posture of devices.

Go to https://github.com/Jamf-Concepts/jamf-compliance-editor

Download the latest released package and then install it.

Open the Jamf Compliance Editor located in /Applications.

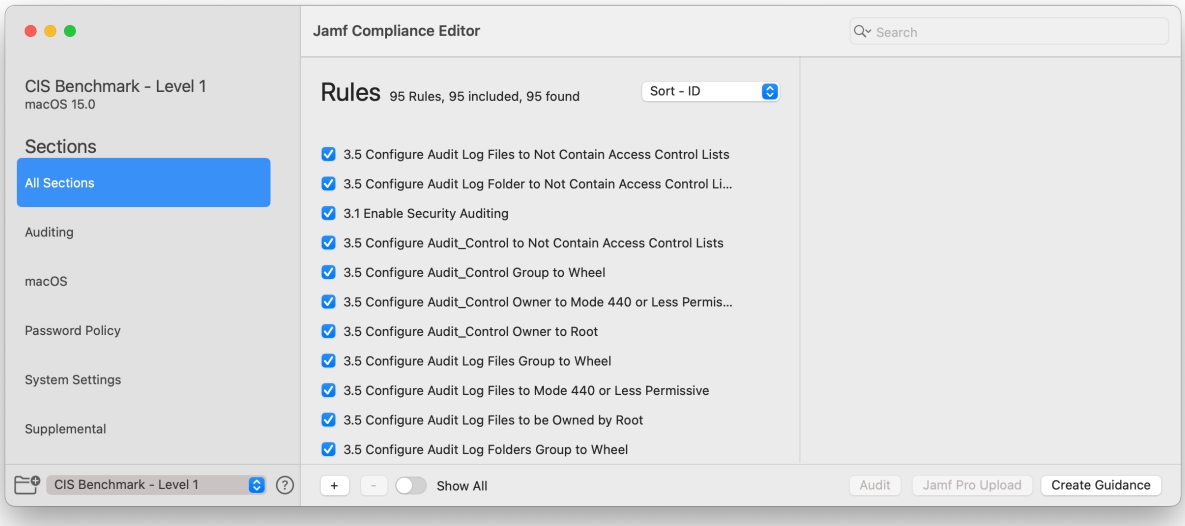
Accept the Terms of Use. On the splash screen, select "macOS" and then click "Create New Project."

When prompted to select a macOS Security Compliance Project branch, choose "sequoia" (or any other version you need) and click "Create".

Note : To configure JCE to show all branches of the mSCP project, run the command `defaults write com.jamf.complianceeditor showAllBranches -bool true` and then re-open JCE ; JCE will then display all branches, including those still under development.

When prompted to select where to save the mSCP directory, choose "Desktop" (or any other folder you prefer) and click "Save".

When prompted to select a Security Benchmark, choose "CIS Benchmark - Level 1" and click "OK".



Click "Create Guidance".

The guidance will be created in Desktop > macOS_security-sequoia/build/cis_lvl1.

Click "View Project" to open this folder in Finder.

Step 2 : Provision Jamf Pro

1/ Identify the compliance assets

The compliance assets to consider in the cis_lvl1 folder are :

• cis_lvl1_compliance.sh : a script to fix and check the security posture

• jamfpro :

    • cis_lvl1.json : a custom schema to configure the baseline

    • compliance-*.xml : Extension attributes (ready to be uploaded)

• mobileconfigs > unsigned > *.mobileconfig : configuration profiles (ready to be uploaded)

2/ Upload the compliance assets

Back in Jamf Compliance Editor, click "Jamf Pro Upload".

Complete the form as follows :
- Display Name : Jamf Pro - Production (a name for the configured server)
- Server URL : https://hostname.jamfcloud.com
- Untick "Use API Role"
- Username : enter the login of an account with administrator privileges
- Password : enter the password for this account
- By default, the script, extension attributes, and configuration profiles are ticked.

Click "Add", and then click "Continue".

You are informed that the json schema must be manually uploaded in Jamf Pro.

Quit Jamf Compliance Editor.

3/ Observe the uploaded compliance assets

Log in Jamf Pro with your administrator account.

Go to Settings > Computer management > Scripts.
Note the script named "Sequoia_cis_lvl1_compliance.sh" associated with the category "Sequoia_cis_lvl1".

Go to Settings > Computer management > Extension attributes.
Note the four Extension Attributes with names starting with "Compliance".
By default, they are displayed in the "Extension Attributes" section of the device records.

Go to Computers > Configuration Profiles.
Note the collection of configuration profiles associated with the category "Sequoia_cis_lvl1".

4/ Make the script available to MOM

Create a policy that MOM will trigger for compliance remediation :

- Options
    - Payload "General"
        - Name : Sequoia_cis_lvl1-fix
        - Category : Sequoia_cis_lvl1
        - Trigger > Custom : Sequoia_cis_lvl1-fix
        - Execution Frequency : Ongoing
    - Payload "Scripts"
        - Sequoia_cis_lvl1_compliance.sh
        - Parameter 4 : `--fix`
- Scope : the devices that will execute MOM during an onboarding or an MDM switching.

Create a policy that MOM will trigger for compliance scan :

- Options
    - Payload "General"
        - Name : Sequoia_cis_lvl1-fix
        - Category : Sequoia_cis_lvl1
        - Trigger > Custom :Sequoia_cis_lvl1-fix
        - Execution Frequency : Ongoing
    - Payload "Scripts"
        - Sequoia_cis_lvl1_compliance.sh
        - Parameter 4 : `--check`
- Scope : the devices that will execute MOM during an onboarding or an MDM switching.

5/ Distribute the configuration profiles

Scope the configuration profiles to the devices that will execute MOM during an onboarding or an MDM switching.

6/ Configure the baseline

This process allows setting exemptions to specific security rules based on your company's unique policies.

Go to Computers > Configuration Profiles.

Click "New".

- Options
    - Payload "General"
        - Name : Sequoia_cis_lvl1-audit
        - Category : Sequoia_cis_lvl1
    - Payload "Application & Custom settings" > External Applications > Add
        - Source : Custom Schema

- Preference Domain : org.cis_lvl1.audit

Note : To get the domain, open the JSON file and use the value for "Preference Domain"

- Custom Schema > Add schema > Upload > select the JSON file > Save
- Preference Domain Properties

To disable a rule :

- choose "Configured"
  - exempt : choose "true"
  - exempt reason : enter a reason for disabling the rule (required)

- Scope : the devices that will execute MOM during an onboarding or an MDM switching.

Step 3 : Provision another MDM

1/ Identify the compliance assets

The compliance assets to consider in the cis_lvl1 folder are :

• cis_lvl1_compliance.sh : a script to fix and check the security posture

• mobileconfigs :

- preferences > *.plist : plist files used **exclusively with VMware Workspace ONE**

- unsigned > *.mobileconfig : configuration profiles used **for all other MDM solutions**

• preferences > org.cis_lvl1.audit.plist : a property list file to configure the baseline

Quit Jamf Compliance Editor.

2/ Embed the compliance script in the MOM-Content

Refer in this documentation to the chapter entitled "MOM Content Building" and specifically the section entitled "Content gathering" to embed the compliance script in the MOM-Content package.

Multiple scripts for different versions of macOS can be embedded in a single MOM-Content package. MOM will automatically select the correct script based on the configuration of the mSCP integration.

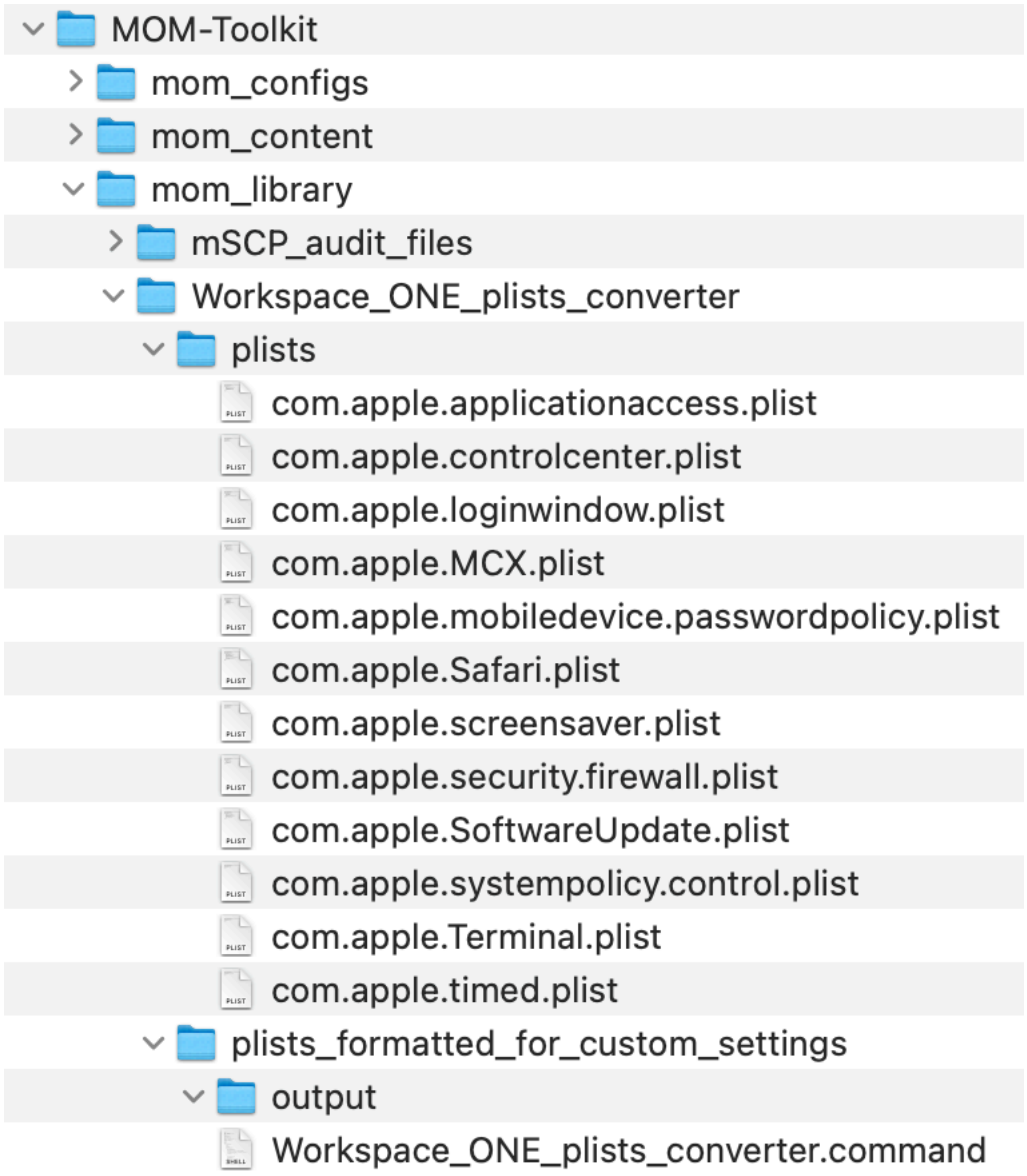
3A/ VMware Workspace ONE — Upload and distribute the configuration profiles

Follow these instructions to prepare the plist files for distribution as Custom Settings.

Open the "MOM-Toolkit" folder.

Go to "mom_library > Workspace_ONE_plists_converter > plists".

Copy the plist files into the "plists" subfolder.

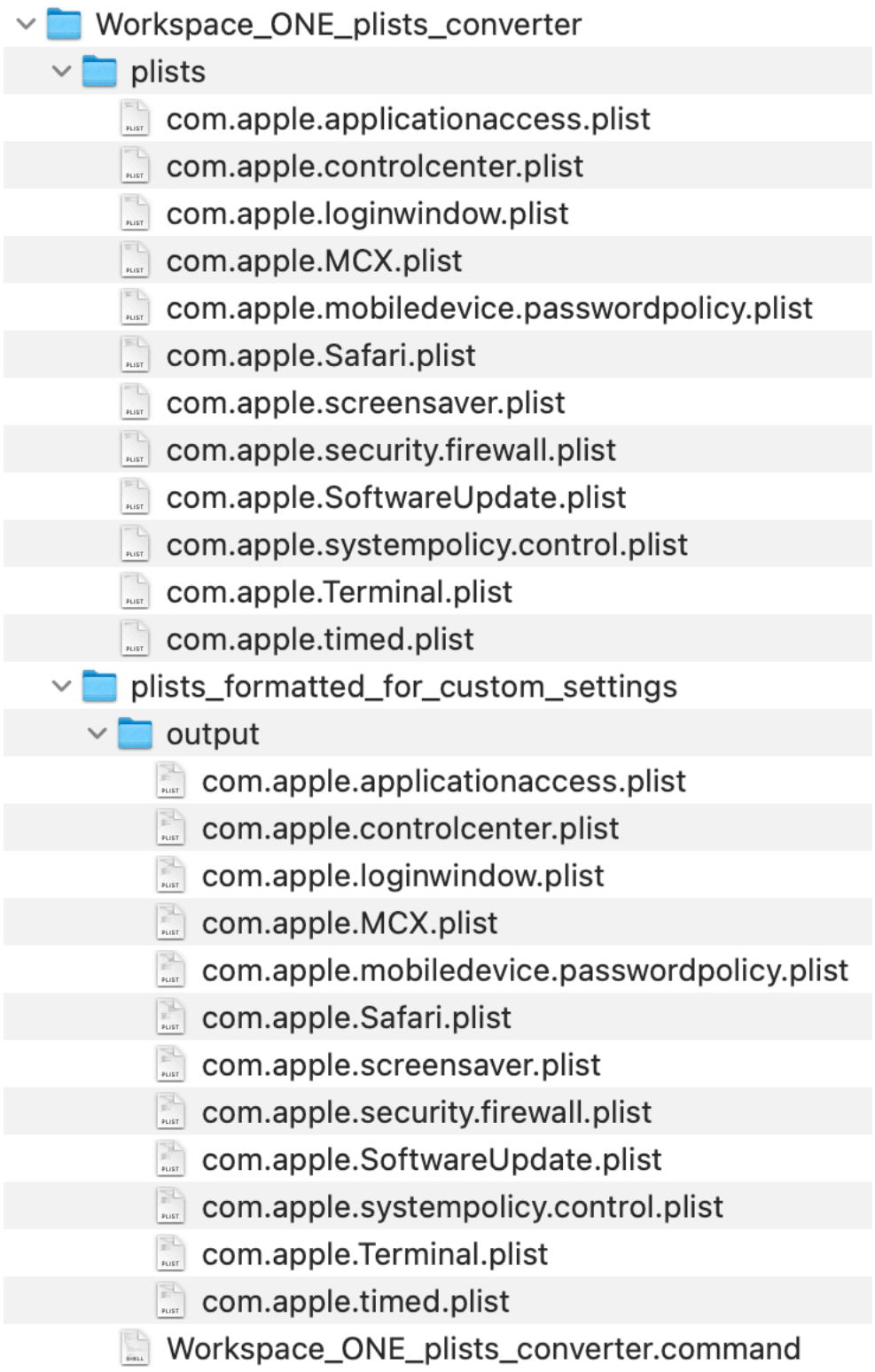


Open the "MOM-Toolkit" folder.

Go to "mom_library > Workspace_ONE_plists_converter > plists_formatted_for_custom_settings".

Execute the "Workspace_ONE_plists_converter" 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 several plist files for distribution as Custom Settings.

Distribute each converted plist file through the Custom Settings payload of a Custom configuration profile to the devices that will execute MOM during an onboarding or an MDM switching.

Refer in this documentation to the section entitled "Custom configuration profile" included in the chapter entitled "Provisioning VMware Workspace ONE", and consult the MDM documentation if necessary, to revise the process.

3B/ All other MDM solutions — Upload and distribute the configuration profiles

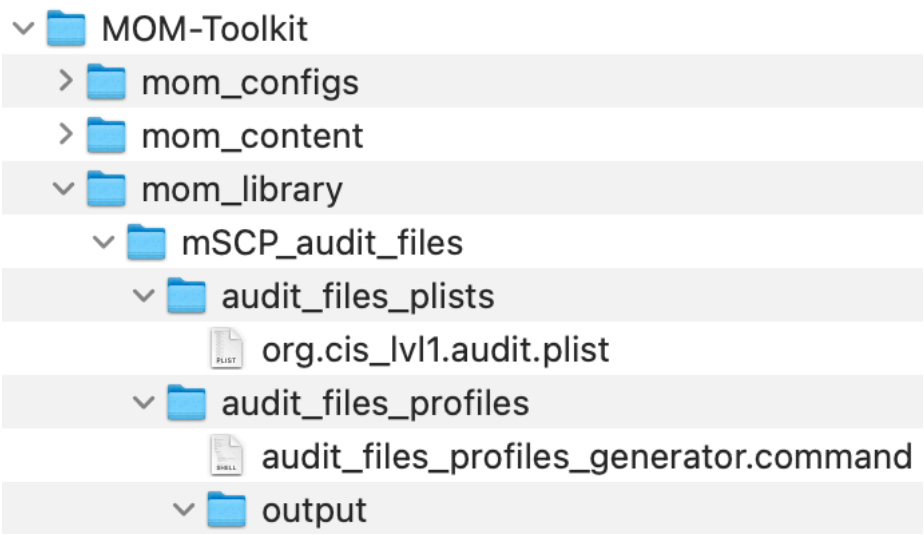
Distribute each configuration profile to the devices that will execute MOM during an onboarding or an MDM switching.

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 revise the process.

4/ Copy the audit file in the MOM Library

Open the "MOM-Toolkit" folder.

Go to "mom_library > mSCP_audit_files > audit_files_plists".

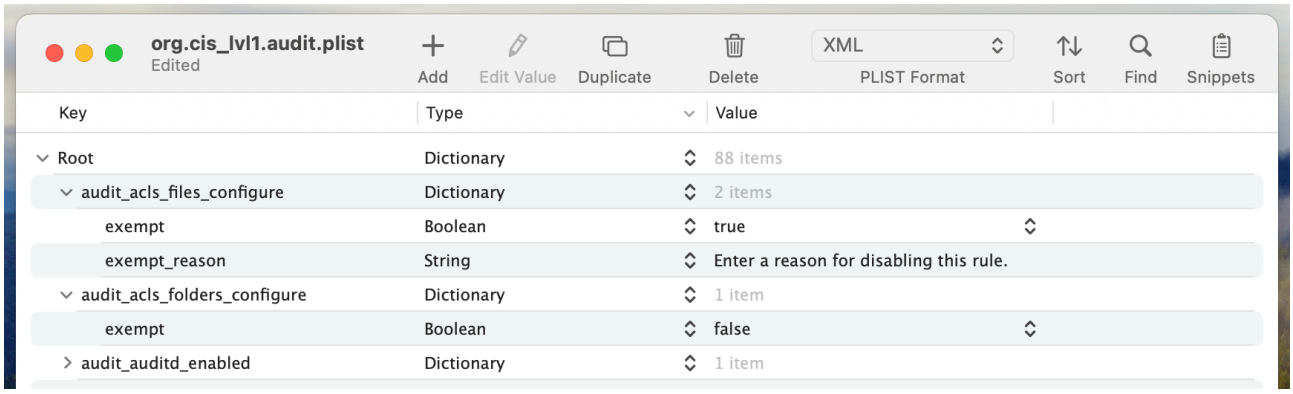


Copy the audit file into the "audit_files_plists" subfolder.

5/ Configure the baseline

This process allows setting exemptions to specific security rules based on your company's unique policies.

Open the audit file located in the "audit_files_plists" subfolder with your preferred Property List editor.



To disable a rule :
- set the "exempt" key to "true"
- add an "exempt_reason" key with the type "String" and enter a reason for disabling the rule (required).

Close the audit file.

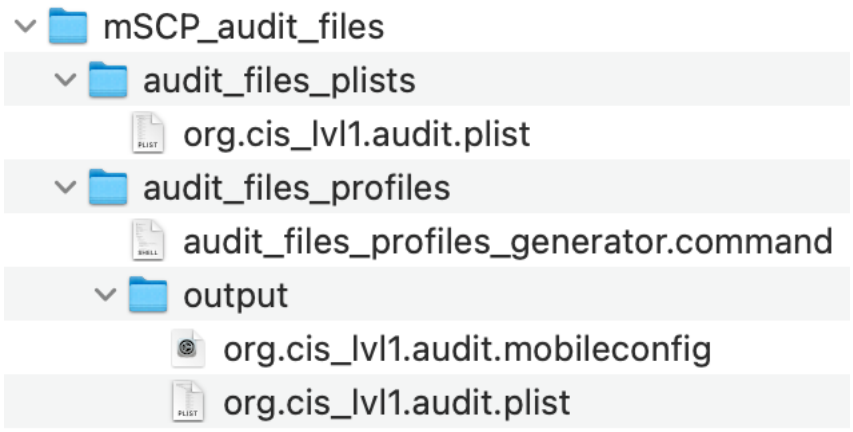
6/ Convert the audit file to a Custom configuration profile

Open the "MOM-Toolkit" folder.

Go to "mom_library > mSCP_audit_files > audit_files_profiles".

Execute the "audit_files_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 audit file into two files :
- one Custom configuration profile with the extension ".mobileconfig"
- one 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 device) :
- 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.

7/ Upload and distribute the generated Custom configuration profile

Distribute the generated Custom configuration profile to the devices that will execute MOM during an onboarding or an MDM switching.

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 revise the process.

Step 4 : Configure MOM for Jamf Pro or another MDM

Implementing mSCP compliance involves editing keys in the Location configuration file which are detailed in the Dictionary.

• **Key located inside the INTEGRATIONS Dictionary**

MSCP_INTEGRATION : set to "true"

• **Keys located inside the INTEGRATIONS > MSCP_CONFIGURATION Dictionary**

COMPLIANCE_REMEDIATION : set to "true" to trigger the remediation planned by the compliance script before a scan

COMPLIANCE_REMEDIATION_METHOD
For each macOS version supported in your environment, specify the method to use for executing the script for compliance remediation. Example of a value :
- `script:cis_lvl1_compliance.sh` : name of the script embedded in the MOM-Content
- `event:Sequoia_cis_lvl1-fix` : name of the Jamf Pro policy custom trigger
- `id:100` : Jamf Pro policy ID (alternative to a custom trigger)

Note : Depending on the MDM used, keep only one dictionary named exactly "COMPLIANCE_REMEDIATION_METHOD" from the template.

COMPLIANCE_REMEDIATION_SETTINGS > PREFER_PRIVILEGED_HELPER : set to "true" to delegate the execution of the script to the MOM Privileged Helper

COMPLIANCE_SCAN : set to "true" to trigger a scan

COMPLIANCE_SCAN_METHOD
For each macOS version supported in your environment, specify the method to use for executing the script for compliance scan. Example of a value :
- `script:cis_lvl1_compliance.sh` : name of the script embedded in the MOM-Content
- `event:Sequoia_cis_lvl1-check` : name of the Jamf Pro policy custom trigger
- `id:101` : Jamf Pro policy ID (alternative to a custom trigger)

Note : Depending on the MDM used, keep only one dictionary named exactly "COMPLIANCE_SCAN_METHOD" from the template.

COMPLIANCE_SCAN_SETTINGS > PREFER_PRIVILEGED_HELPER : set to "true" to delegate the execution of the script to the MOM Privileged Helper

COMPLIANCE_SCORE_FAILURE : percentage of compliance score below which a failure message is processed by the Compliance report and webhook alerts

COMPLIANCE_SCORE_WARNING : percentage of compliance score below which a warning message is processed by the Compliance report and webhook alerts

• **Key located inside the INTEGRATIONS > SLACK_CONFIGURATION Dictionary**

MESSAGE_MSCP_COMPLIANCE : message sent for the compliance report

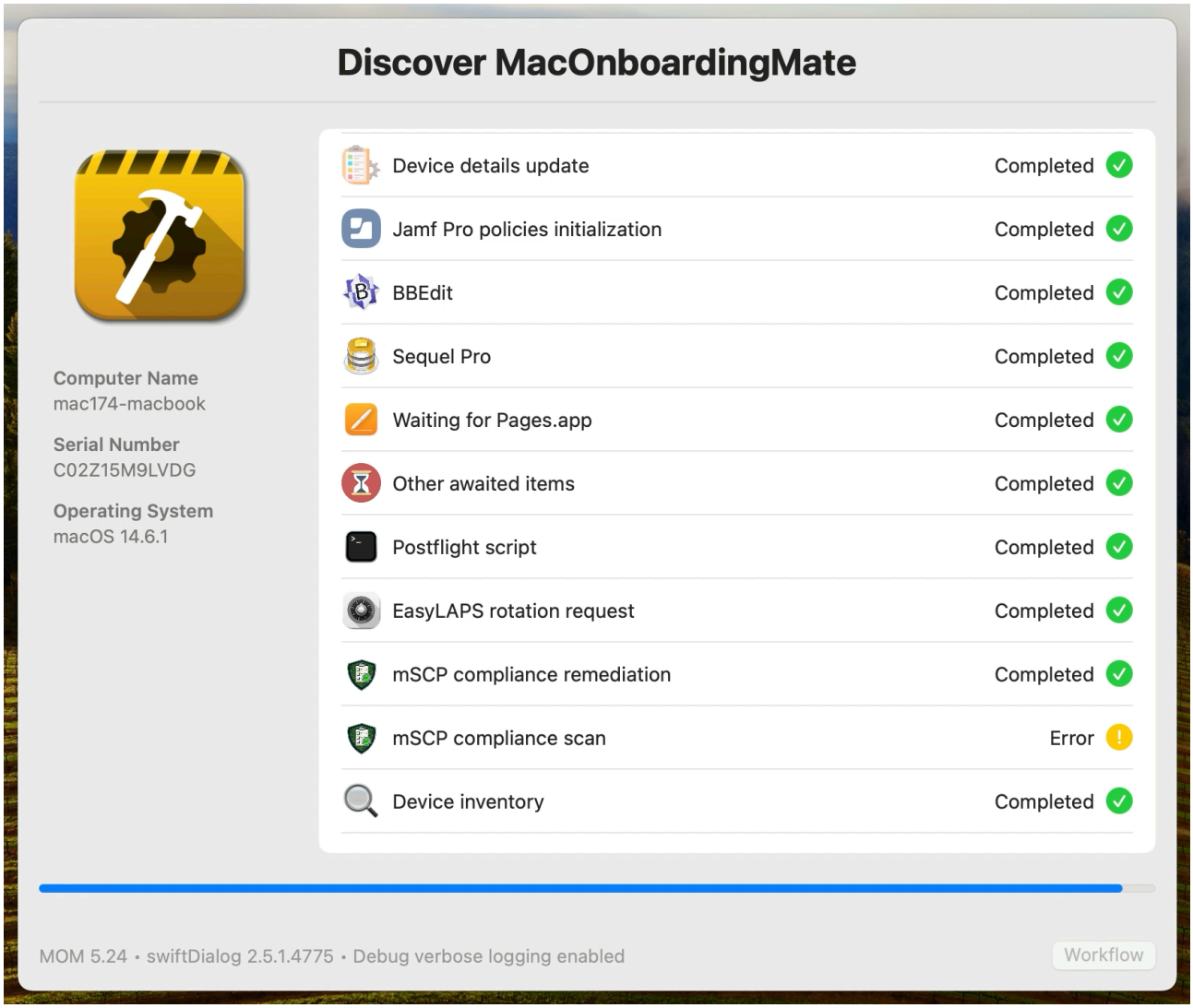
The variable `:mSCPComplianceReport:` is replaced by the report.

• **Key located inside the INTEGRATIONS > TEAMS_CONFIGURATION Dictionary**

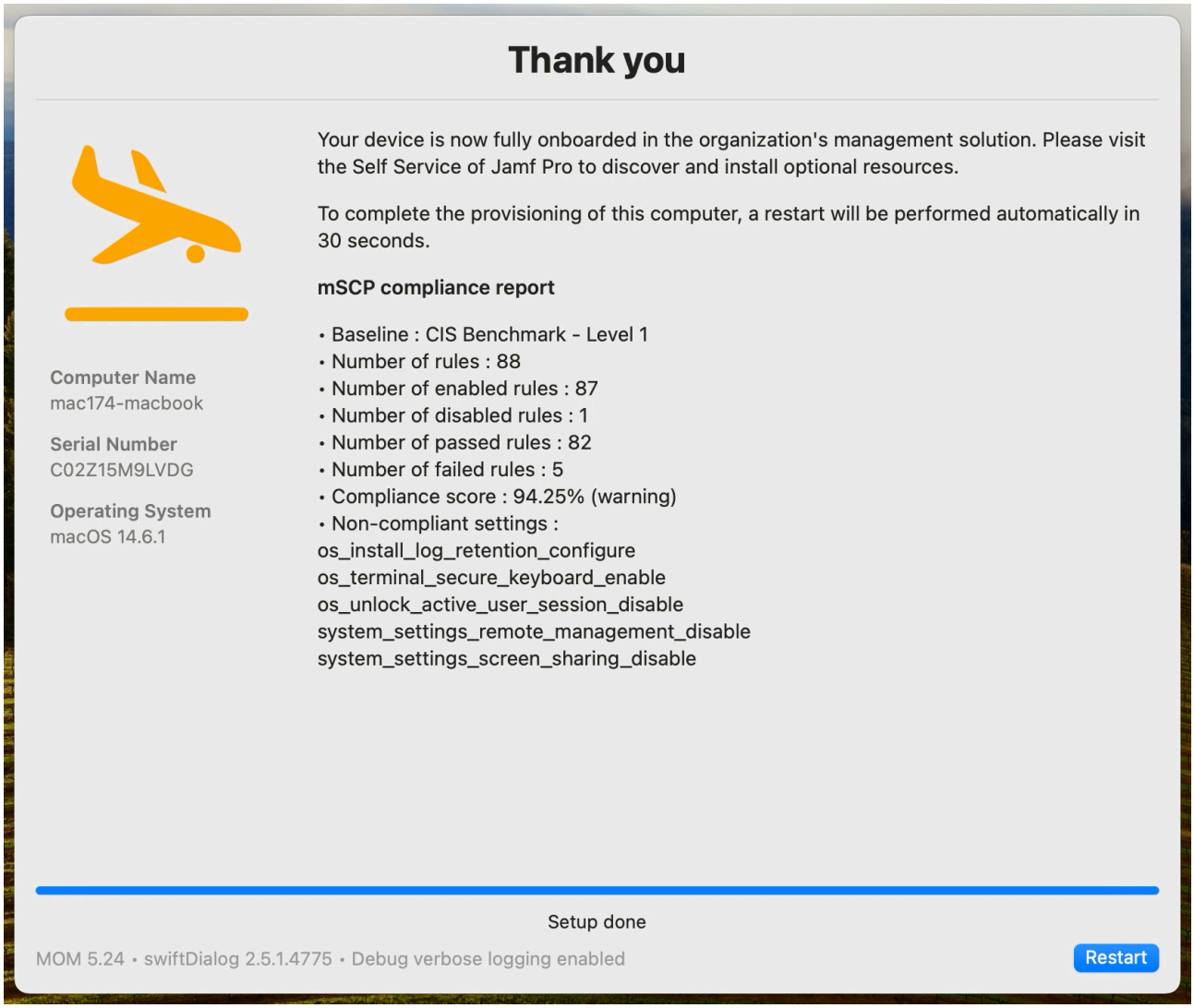
MESSAGE_MSCP_COMPLIANCE : message sent for the compliance report

The variable `:mSCPComplianceReport:` is replaced by the report.

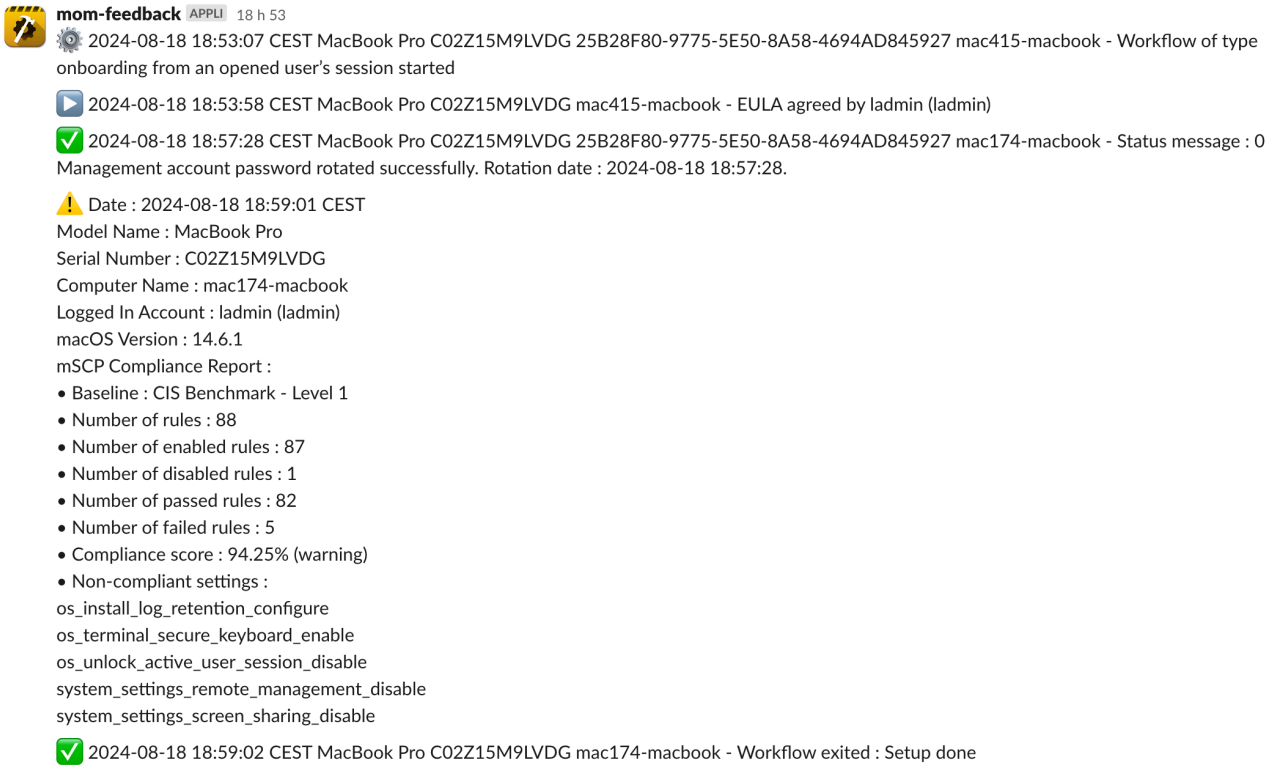
Step 5 : Check the result of the integration



An mSCP compliance remediation has been completed, but the mSCP compliance scan ended with an "error" status because the compliance score is below the value defined for a warning.



The Landing pane displays the mSCP compliance report, including the baseline name and statistics, followed by the list of non-compliant settings.



The mSCP compliance report is included in the webhooks sent by MOM to a dedicated Slack or Microsoft Teams channel for feedback.

Onboarding a Mac using MOM in Launcher mode

MOM orchestrates the onboarding of the device in the management solution from an opened user's session.

Enrollment experience

In the context of an MDM solution, the device is enrolled according :
- Automated Device Enrollment if the device is fully provisioned in AxM and MDM
- Device Enrollment in the opposite situation.

In both contexts, the location (destination point) of the device that determines the workflow to execute is :
- manually selected from a Location Selector when two or more locations are configured in the Launcher configuration file
- automatically selected when only one location is configured in the Launcher configuration file.

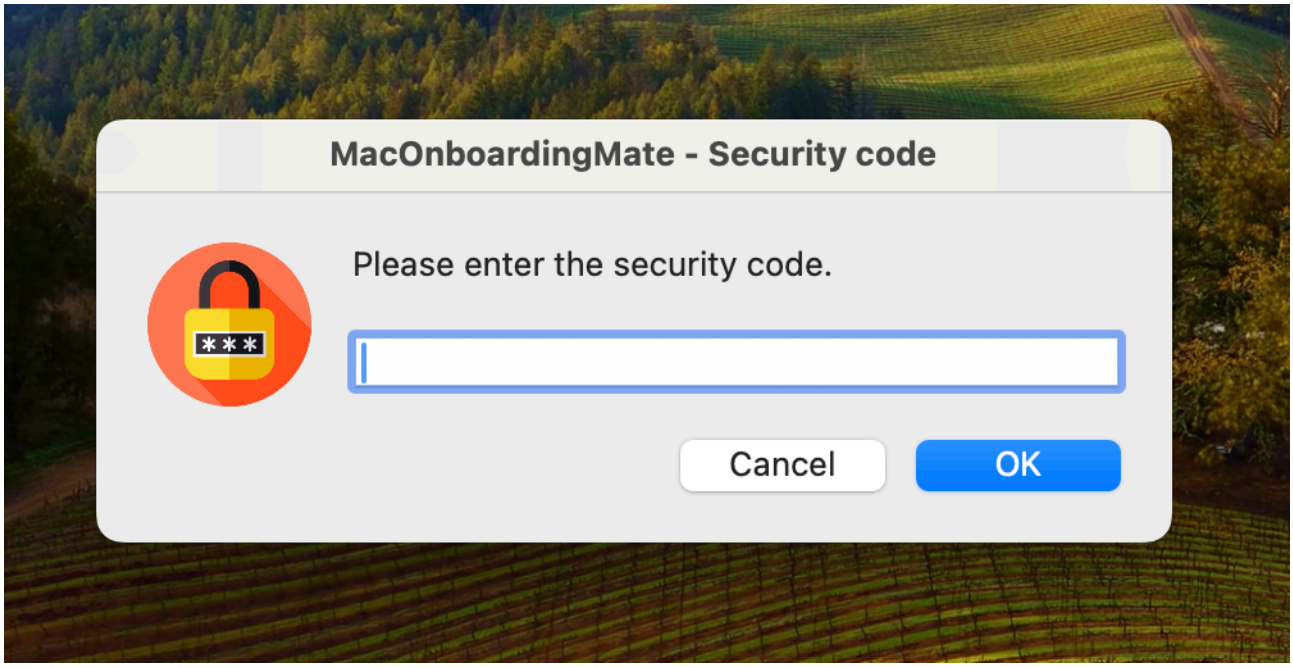
Note : Because calls to AxM are rate limited to once every 23 hours with macOS 12.3.x, and to 10 times every 23 hours with macOS 13 and later, the automated deduction of the workflow to execute in the context of Automated Device Enrollment has been removed in MOM version 5.16.

MOM execution

With macOS Monterey (macOS 12) and later, store together "MOM-Core.pkg" and "MOM-Core-Companion.dmg" in /Users/Shared or a USB key (the mounting of a disk image located in the logged in user home directory is not allowed).

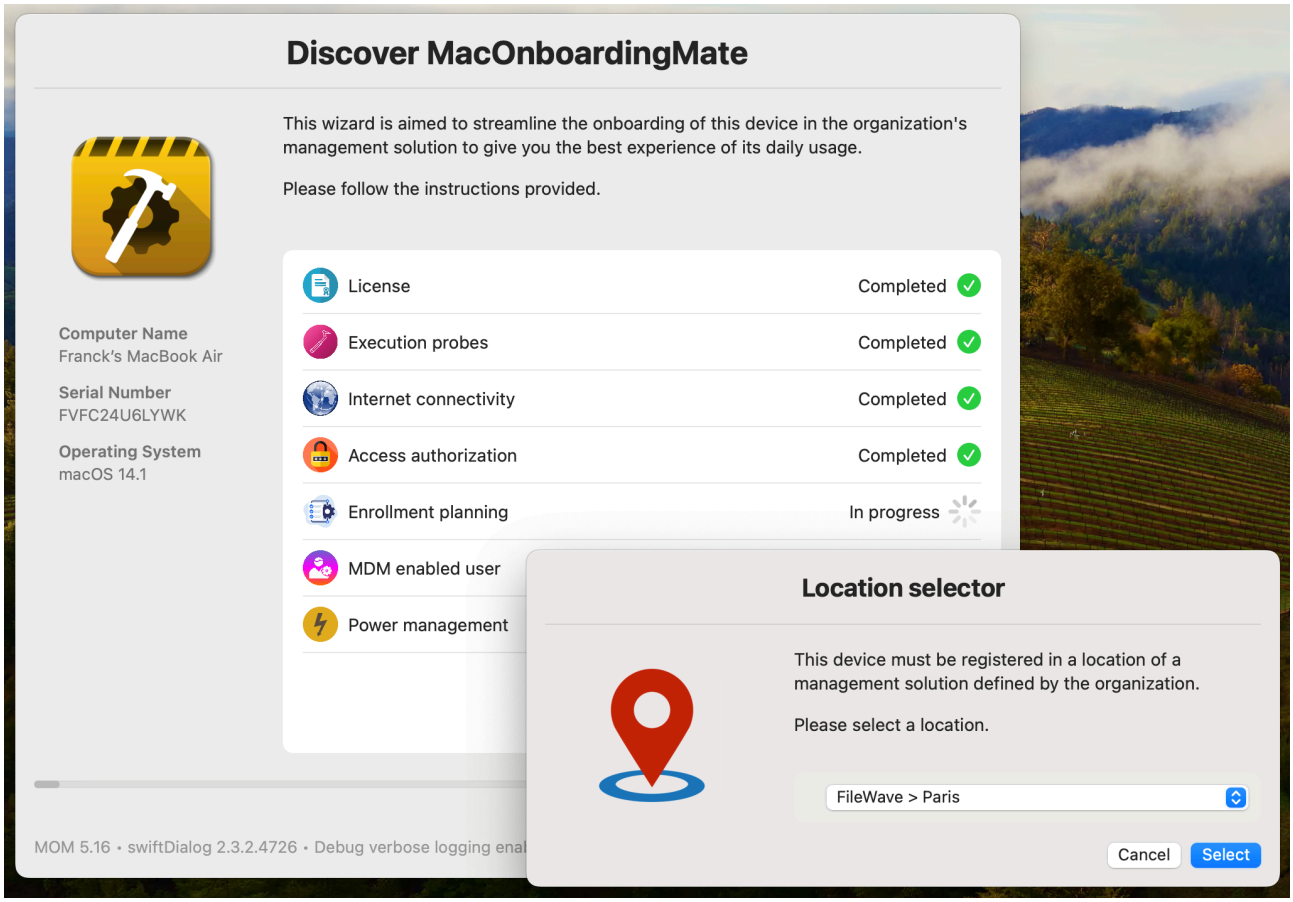
With macOS Big Sur (macOS 11) and earlier, you can also store together "MOM-Core.pkg" and "MOM-Core-Companion.dmg" at the location you prefer (in the logged in user home folder, a USB key, etc.).

Double-click on "MOM-Core.pkg".



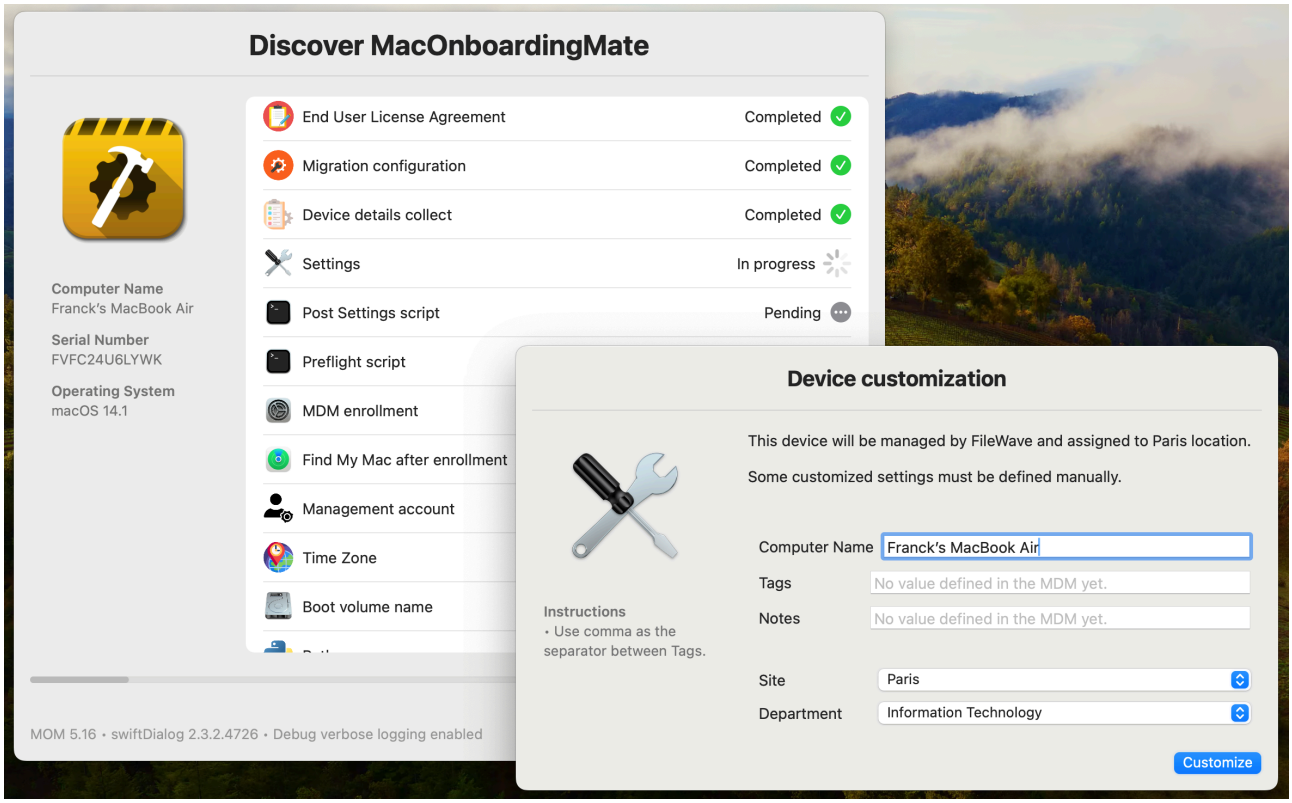
Enter the passphrase used to protect the MOM-Core-Companion disk image from an unauthorized access.

After a couple of seconds, the Welcome pane displays a greeting message and the license status (customer and expiration date).

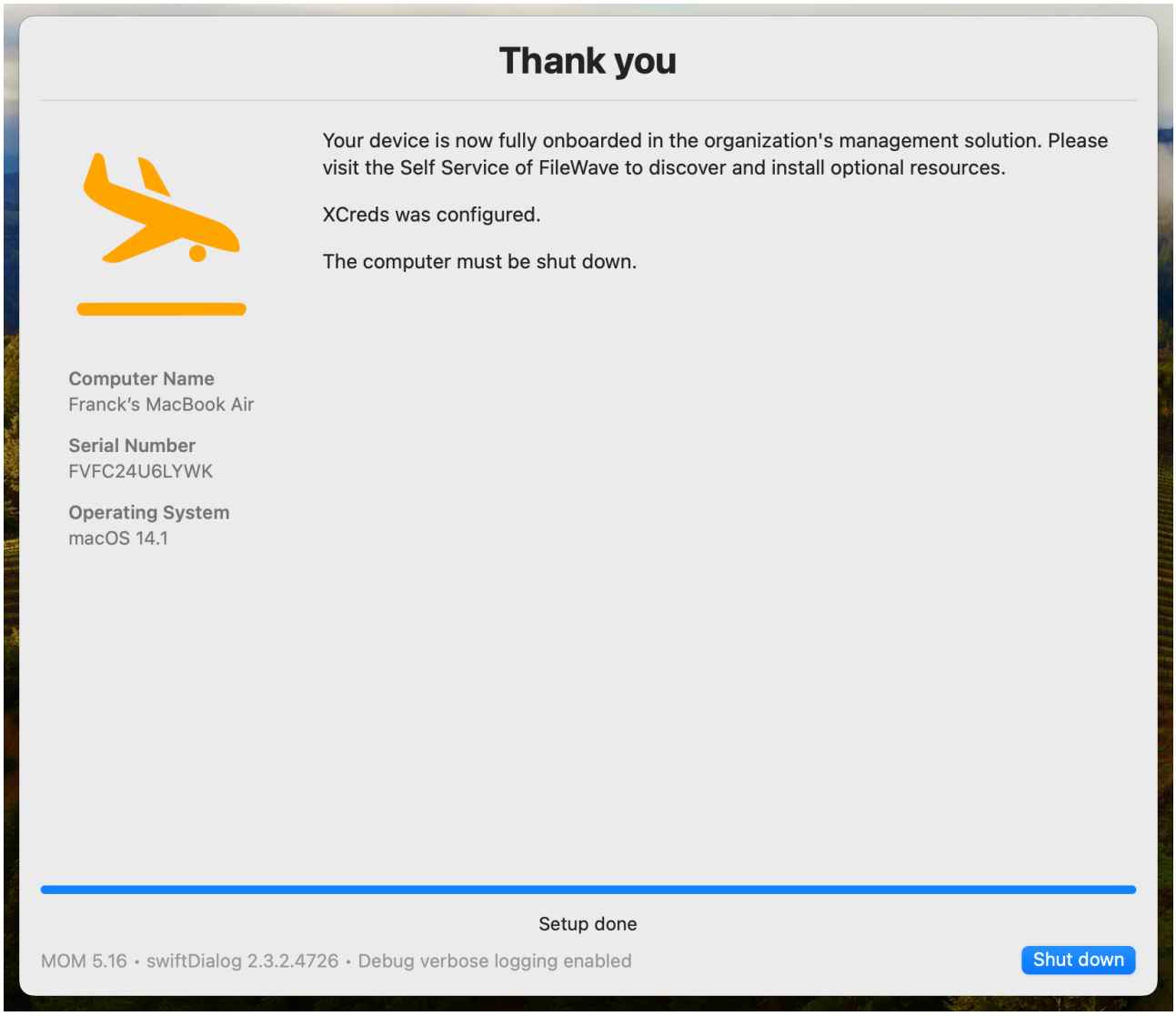


In the context of two or more locations configured in the Launcher configuration file, select a location in the Location selector, then click in "Select".

Outside of the context of mobile accounts, the device should be enrolled from the session of the local account which is aimed to become the MDM enabled (capable) user aka the only user on the device to be able to receive User-level Configuration profiles (User Channel). Check the dialog displayed, then click on "Yes".



Follow the instructions displayed according the planned workflow for the chosen location.



The landing pane confirms that the device was fully onboarded in the management solution.

Onboarding a Mac using MOM in AutoLauncher mode

MOM orchestrates the onboarding of the device in the management solution as soon as possible in the context of Automated Device Enrollment.

Enrollment experience

The device is first enrolled with Automated Device Enrollment.

Then the device retrieves the three required components :
- a Custom configuration profile
- a MOM-Content package
- the MOM-Core package.

The Custom configuration profile is always installed right after the enrollment.

If the MOM-Core package is installed first, MOM waits until the MOM-Content package is installed before proceeding.

MOM is designed to offer a graphical interface that does not interfer with the onboarding.

Depending of the provisioning method, two experiences can be distinguished.

With provisioning over the Setup Assistant or Login Window, all onboarding tasks are performed during these phases. Afterward, the Mac shuts down, restarts, or displays the Login Window, allowing an end user to log in.

With provisioning over the Desktop, non-interactive tasks are started behind the scenes during the Setup Assistant, then interactive tasks are executed over the Desktop of the first logged-in user. Depending of the Finder detection at two key stages of MOM execution, the Welcome pane is displayed earlier or later.

MOM execution with provisioning over the Setup Assistant

Wait for the Setup Assistant to be opened then :
- configure the country or region, the written and spoken languages and the accessibility settings
- continue with "Remote Management" (this step can vary according the MDM configuration).

Then wait for MOM to open on top of the Setup Assistant which should display at this time the "Time Zone" pane. Bear in mind that MOM may take some time to appear on top of the Setup Assistant, so do not click on its interface to risk closing it.

Follow the instructions displayed according the planned workflow.

The landing pane confirms that the device is fully onboarded in the management solution.

MOM execution with provisioning over the Login Window

Wait for the Setup Assistant to be opened then :
- configure the country or region, the written and spoken languages and the accessibility settings
- continue with "Remote Management" (this step can vary according the MDM configuration).

Please note that all the Setup Assistants steps can be automated or bypassed using "Auto Advance for Mac" and an Automated Device Enrollment profile that skips the "Accessibility" pane (Ethernet required).

Then wait for MOM to open on top of the Login Window. Bear in mind that MOM may take some time to appear on top of the Login Window.

Follow the instructions displayed according the planned workflow.

The landing pane confirms that the device is fully onboarded in the management solution.

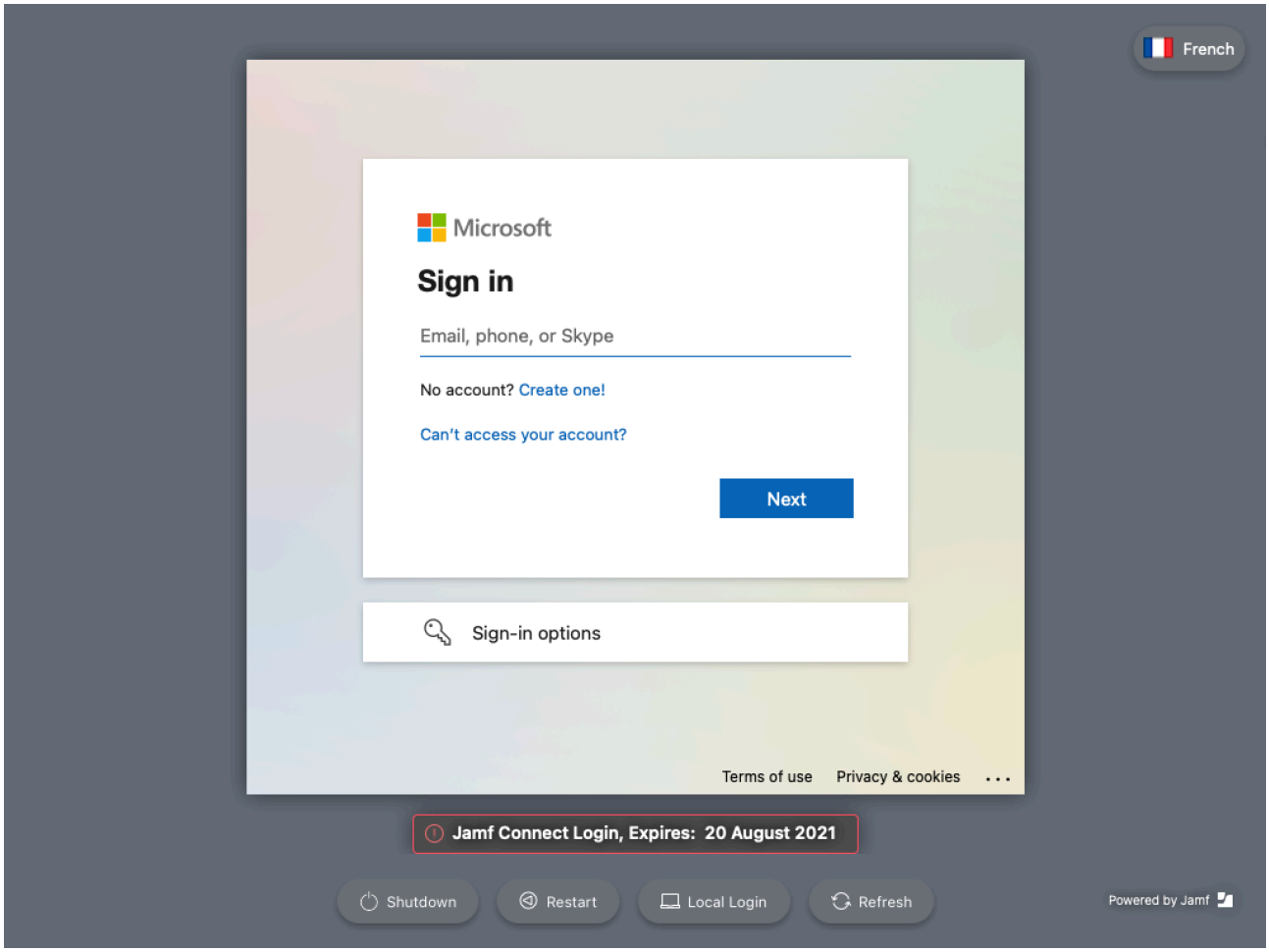
MOM execution with provisioning over the Desktop

Wait for the Setup Assistant to be opened then :
- configure the country or region, the written and spoken languages and the accessibility settings
- continue with "Remote Management" (this step can vary according the MDM configuration).

Please note that all the Setup Assistants steps can be automated or bypassed using "Auto Advance for Mac" and an Automated Device Enrollment profile that skips the "Accessibility" pane (Ethernet required).

Once the enrollment is done, the macOS login window is displayed.

If the "Create a Computer Account" pane is not skipped in the Automated Device Enrollment profile, the macOS login window is not displayed and the session of the created local account is automatically opened.



At this step, a third party login window may appear instead of the macOS login window to propose the creation of a local account based on an existing directory account.

Once a user is logged in, MOM opens over the Desktop of the logged-in user after a few seconds. Follow the instructions displayed according the planned workflow.

The landing pane confirms that the device is fully onboarded in the management solution.

Localizing MOM

MOM 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

If Launcher mode is implemented, open the Launcher configuration file and localize the strings in the UIHELPER section.

For both Launcher and AutoLauncher modes, open the Location configuration file(s) and localize the strings in the UIHELPER and INTEGRATIONS sections.

As indicated in the MOM 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.

The strings in the JAMF_PRO_POLICIES sections offer localizable texts for each policy :
UIHELPER_MAIN_TEXT, UIHELPER_STATUS.

Eventually, other individual keys can be localized :
- EXIT_ACTION > BUTTON_LABEL : the label for the button to exit the workflow
- MIGRATION_POSTPONE : only the label for each defer button, e.g. "1 day", "1 hour".

Localization of the configuration files for multiple languages

In the Launcher configuration file, the following keys can be localized for multiple languages :
- UIHELPER_MAIN_TITLE
- UIHELPER_MAIN_TEXT

In the Location configuration file(s), 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_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_FUTURE
- UIHELPER_MAIN_TEXT_SETTINGS_PRESENT
- UIHELPER_MAIN_TITLE_MUNKICHECKIN
- UIHELPER_MAIN_TEXT_MUNKICHECKIN
- 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

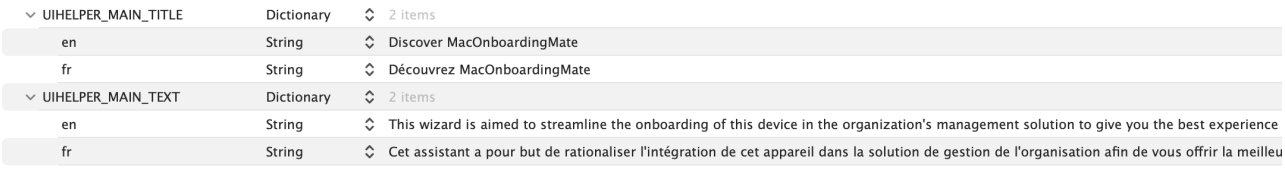
    - type the following command :

```
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 MOM 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 MOM in English to another language, but can also be diverted to just customize those strings in English.

The POT file is provided in the mom_library subfolder of the MOM 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 MOM Toolkit > mom_library > mom.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 "mom_**languagecode**.po" (e.g. "mom_**fr**.po")

9. Add the PO file to the MOM 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 mom.pot file : Translation > Update from POT File

When MOM 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 MOM

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

The components to be updated are respectively :
- MOM Toolkit (Launcher and AutoLauncher modes)
- Launcher configuration file (Launcher mode only)
- Location configuration file(s) (Launcher and AutoLauncher modes)
- Custom configuration profile(s) (AutoLauncher mode only)
- MOM Content package (AutoLauncher mode only)
- MOM Core Companion (Launcher mode only)
- MOM Core package (Launcher and AutoLauncher modes).

MOM Toolkit (Launcher and AutoLauncher modes)

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

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

2. Download and install the updated version of MOM Toolkit

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

4. Copy from the previous folder the **.plist files** stored in mom_configs > locations_plists to the updated folder in mom_configs > locations_plists. Be sure to keep the updated template named "location_1.plist".

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

6. Rename the file mom_configs > launcher.plist, adding a suffix like "_template"

7. Copy from the previous folder **the file** mom_configs > **launcher.plist** to the updated folder in mom_configs

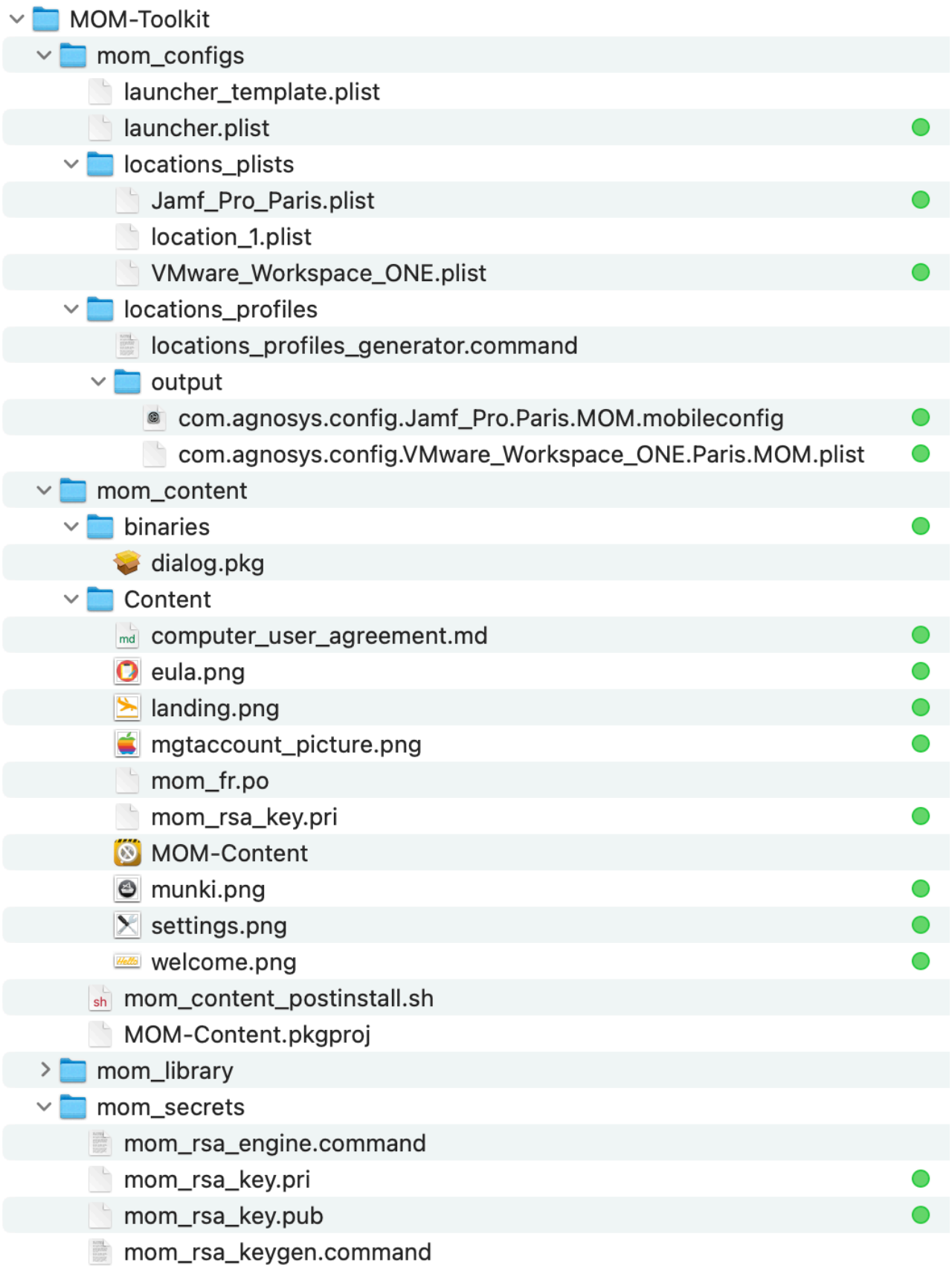
8. Copy from the previous folder **the folder** mom_content > **binaries** to the updated folder in mom_content (.pkg files included)

9. Copy from the previous folder **the content of the folder** mom_content > Content except **MOM-Content.app and original .po files** to the updated folder in mom_content > Content

10. Copy from the previous folder **the following 2 files** stored in mom_secrets to the updated folder in mom_secrets :

- mom_rsa_key.pri
- mom_rsa_key.pub

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


MOM-Toolkit
mom_configs
launcher_template.plist
launcher.plist
locations_plists
Jamf_Pro_Paris.plist
location_1.plist
VMware_Workspace_ONE.plist
locations_profiles
locations_profiles_generator.command
output
com.agnosys.config.Jamf_Pro.Paris.MOM.mobileconfig
com.agnosys.config.VMware_Workspace_ONE.Paris.MOM.plist
mom_content
binaries
dialog.pkg
Content
computer_user_agreement.md
eula.png
landing.png
mgtaccount_picture.png
mom_fr.po
mom_rsa_key.pri
MOM-Content
munki.png
settings.png
welcome.png
mom_content_postinstall.sh
MOM-Content.pkgproj
mom_library
mom_secrets
mom_rsa_engine.command
mom_rsa_key.pri
mom_rsa_key.pub
mom_rsa_keygen.command

Launcher configuration file (Launcher mode only)

Complete your current launcher.plist file to implement as desired new capabilities of MOM, helping you with the updated MOM Dictionary and the updated launcher_template.plist file. Do not hesitate to contact MOM support if you need any clarifications.

Warning : Ensure that your Launcher configuration file contains your current MOM license.

Location configuration file(s) (Launcher and AutoLauncher modes)

Complete your current .plist file(s) to implement as desired new capabilities of MOM, helping you with the updated MOM Dictionary and the updated location_1.plist file. Do not hesitate to contact MOM support if you need any clarifications.

Warning : Ensure that your Location configuration file(s) contain(s) your current MOM license, as it may have been updated directly in the MDM solution, but not in the Location 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 Location 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) (AutoLauncher mode only)

1. Refer in this documentation to the section entitled "Location configuration files to Custom configuration profiles conversion" to convert your updated Location 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).

MOM Content package (Launcher and AutoLauncher modes)

As the private key contained in the file "mom_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 MOM-Content package
- refer to this documentation and the MDM documentation to deploy the updated package.

MOM Core Companion (Launcher mode only)

If something has been updated either in the Launcher configuration file, the Location configuration file(s) or the MOM Content package, refer to this documentation to build an updated MOM-Core-Companion disk image.

MOM Core package (Launcher and AutoLauncher modes)

Download the updated version of MOM Core.

In the context of Launcher mode, execute MOM opening the updated package.

In the context of AutoLauncher mode, refer to this documentation and the MDM documentation to deploy the updated package.

Edge cases

MDM switching / Meraki Systems Manager / Locked Management Profiles

Context of the edge case :

- Migration planned from Meraki Systems Manager to UltimateMDM with AutoLauncher mode
- Device executing any version of macOS 11 and later
- Device enrolled in Meraki Systems Manager with a locked Remote Management profile
- Device assigned to an Automated Device Enrollment Profile :
    - linked to Meraki Systems Manager
    - Removable : No
- Logged in user is a standard account or an admin account

Known macOS limitations :
- the unenrollment must be performed from the same user session as the one used for the enrollment if the associated user account still exists on the device
- calls to AxM are rate limited to once every 23 hours with macOS 12.3.x, and to 10 times every 23 hours with macOS 13 and later ; these limits should be reached when fine-tuning the workflow, but not in production ; when the limitations are reached, wait for 24 hours or use a different test device.

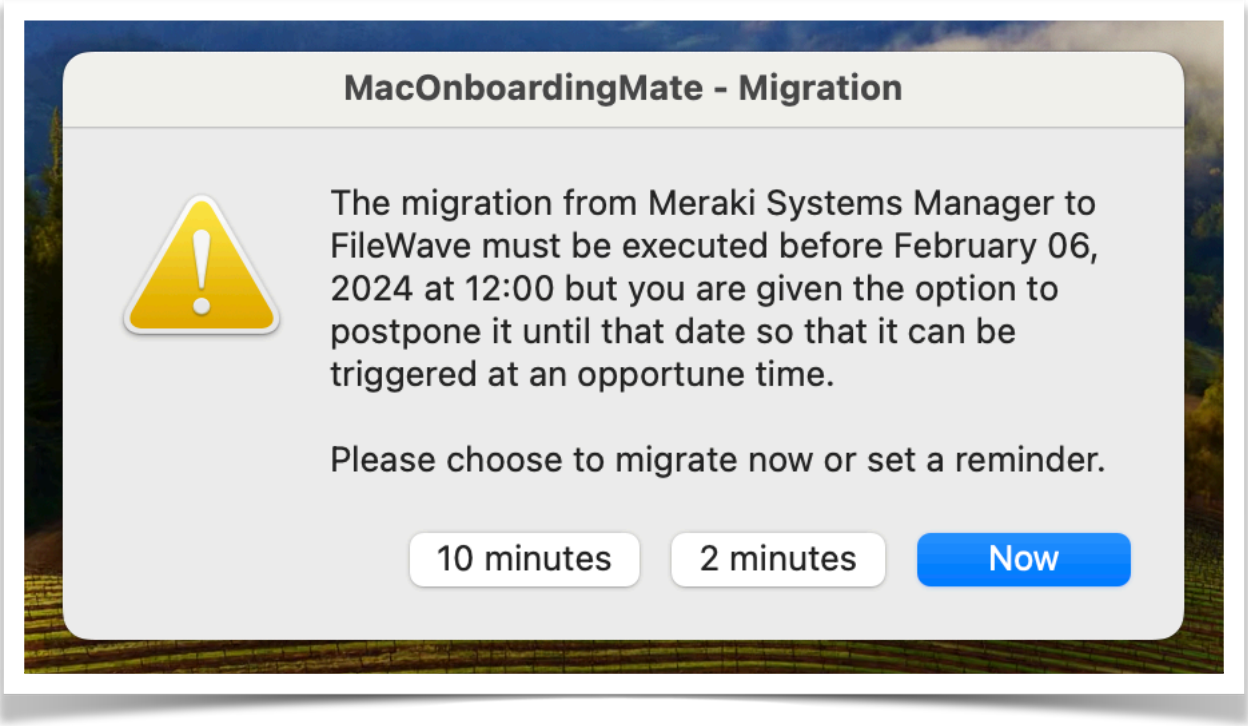
This is the chronology of the required interactions between the IT Support and the End User.

• **IT Support**

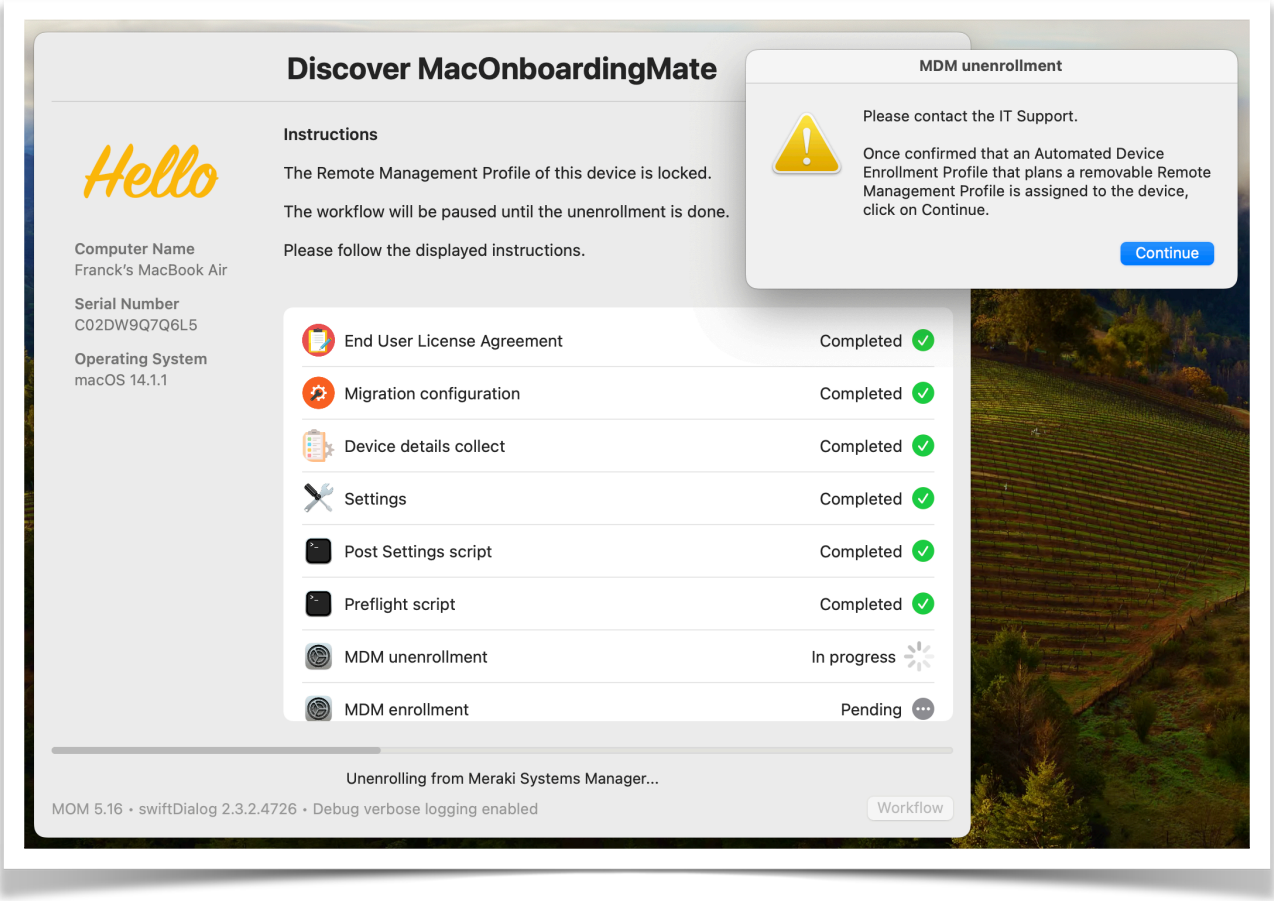
- In Meraki SM :
    - Settings : Custom configuration profile that plans a migration from Meraki Systems Manager to UltimateMDM - Tag : mom
    - Apps : MOM Content and MOM Core packages - Tag : mom
    - Devices : Device selected > Tag > mom
    (Command > Sync apps can help to during testings)
- Webhook message received :
"Workflow of type migration started"

• **End User**

- MOM started



- User chooses to execute the migration now (postpone possible if planned)



- Message displayed :
"The Remote Management Profile of this device is locked. The workflow will be paused until the unenrollment is done. Please follow the displayed instructions."
- Dialog displayed :

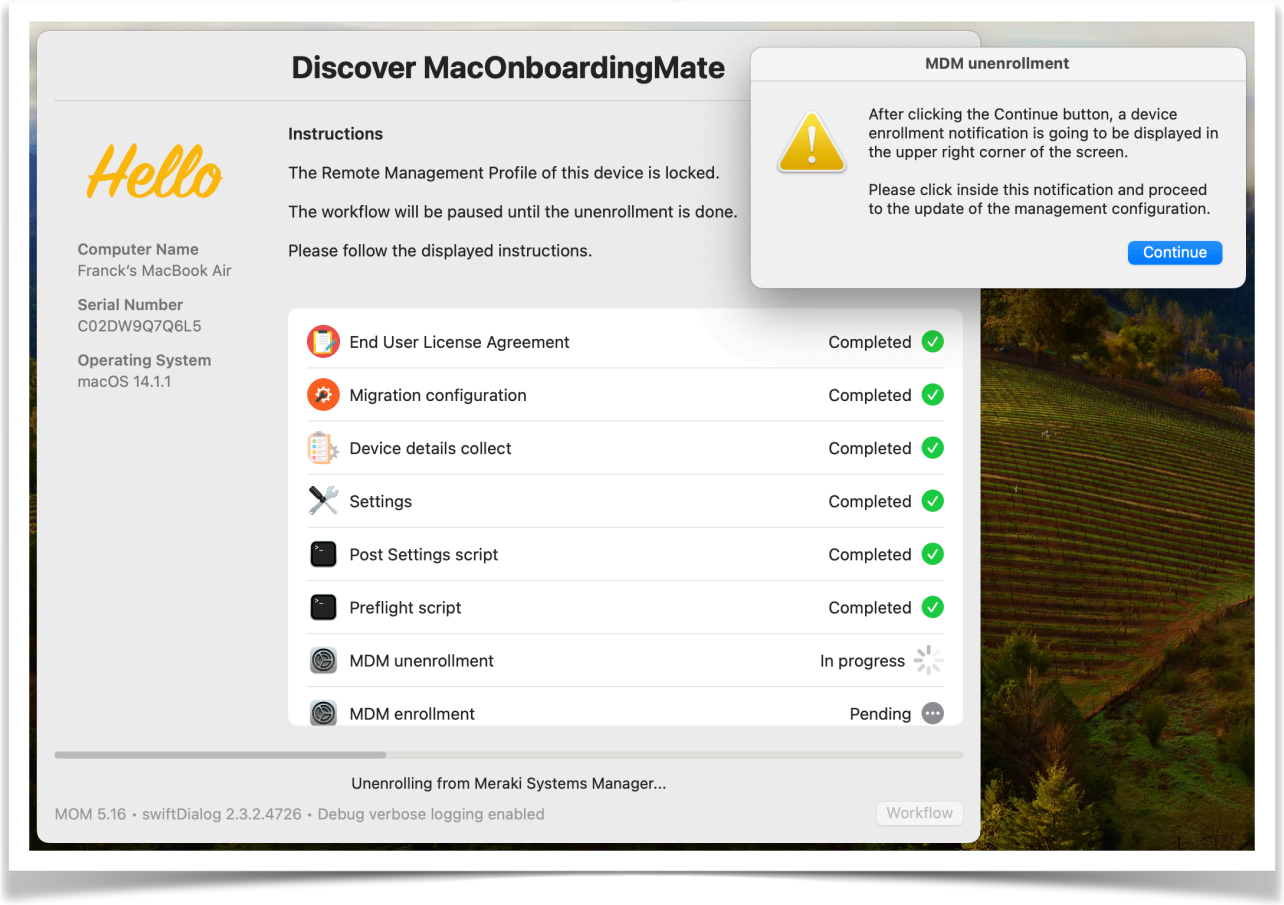
"Please contact the IT Support. Once confirmed that an Automated Device Enrollment Profile that plans a removable Remote Management Profile is assigned to the device, click on Continue."
- User contacts the IT Support

• **IT Support**

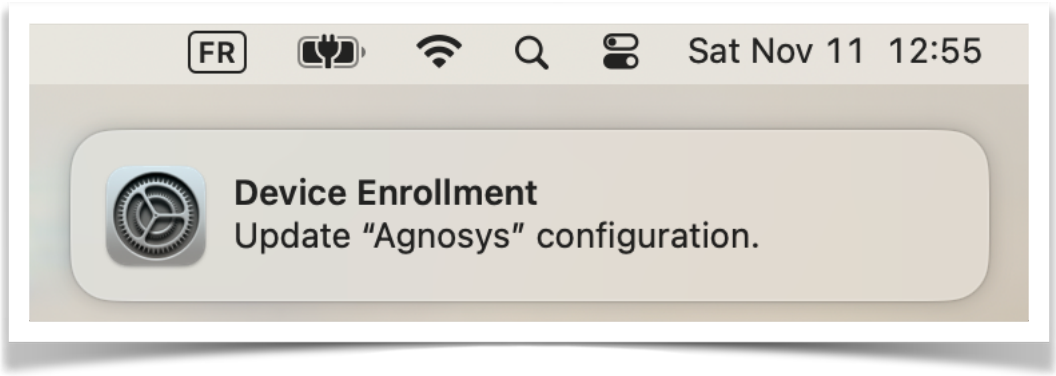
- Webhook message received :
"Device pending unenrollment from Meraki Systems Manager"
- In Meraki SM :
    - Apple Automated Device Enrollment :
        - Device assigned to an Automated Device Enrollment Profile :
            - still linked to Meraki Systems Manager
            - Removable : Yes
        - Full sync
- IT Support confirms to the user that he can click on "Continue"

• **End User**

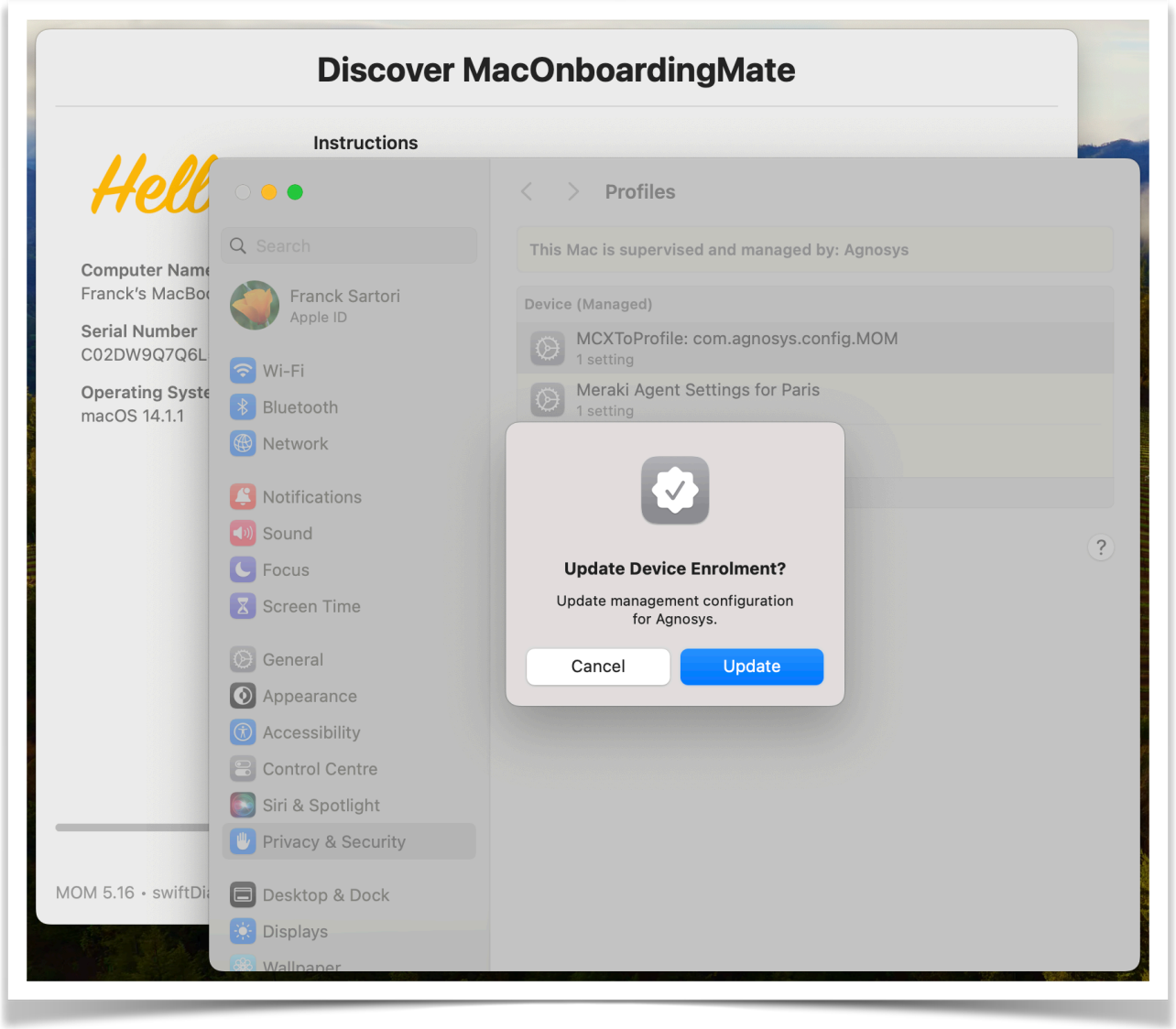
- User clicks on "Continue"



- Dialog displayed :
"After clicking the Continue button, a device enrollment notification is going to be displayed in the upper right corner of the screen. Please click inside this notification and proceed to the update of the management configuration."
- User clicks on "Continue"



- macOS notification displayed :
"Device Enrolment - Update *company name* configuration."
- User clicks inside the notification



- Profiles System Setting (macOS 13 or later) / Profiles System Preference (macOS 12 or earlier) is automatically opened
- macOS dialog displayed :
"Update Device Enrolment? - Update management configuration for *company name*."
- User clicks on "Update"

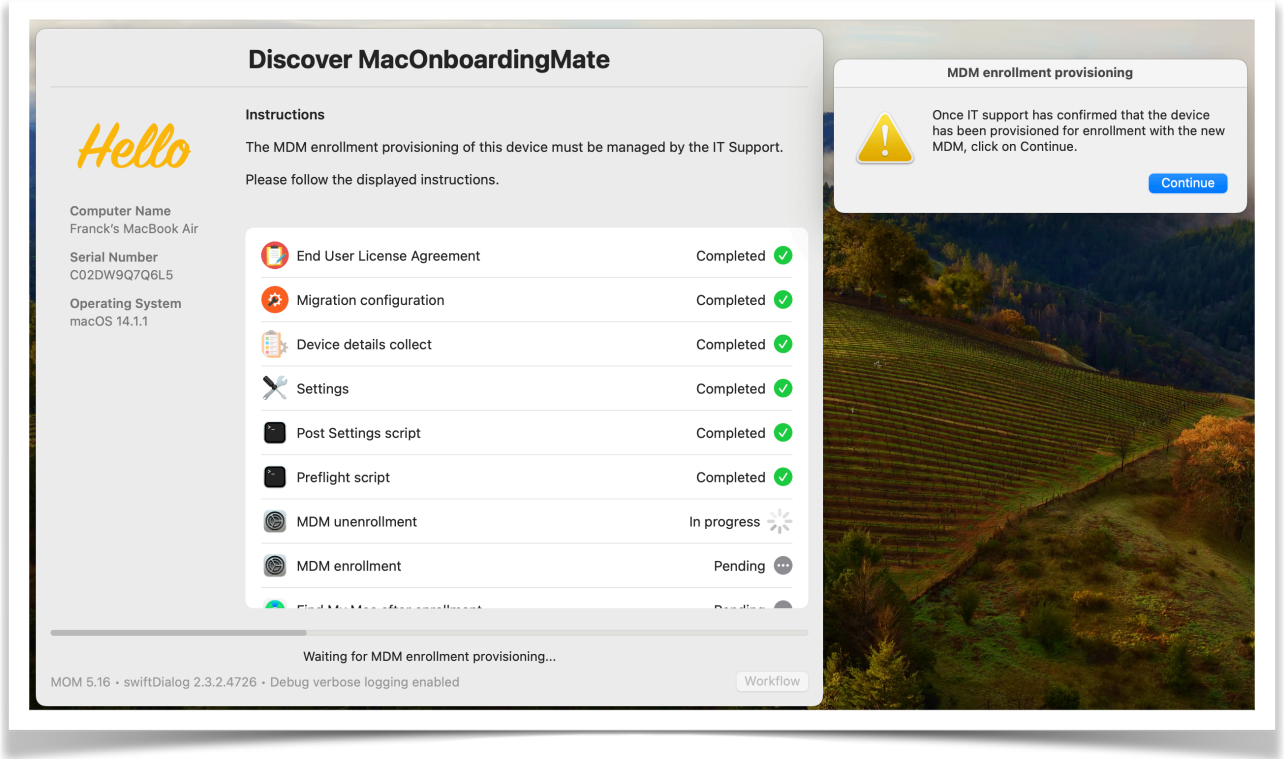
- Depending of how fast the update action is done, reminder dialog may be displayed :
"The Remote Management Profile of this device is still locked. After clicking the Continue button, a device enrollment notification is going to be displayed in the upper right corner of the screen. Please click inside this notification and proceed to the update of the management configuration."
- User clicks on "Continue"
- Once the device enrollment update is done, the Remote Management Profile becomes removable
- MOM deletes locally the unlocked Remote Management Profile

Note : It has been observed that the Remote Management Profile may not become immediately removable ; in this situation, the update process may be triggered several times until the unenrollment can take place.

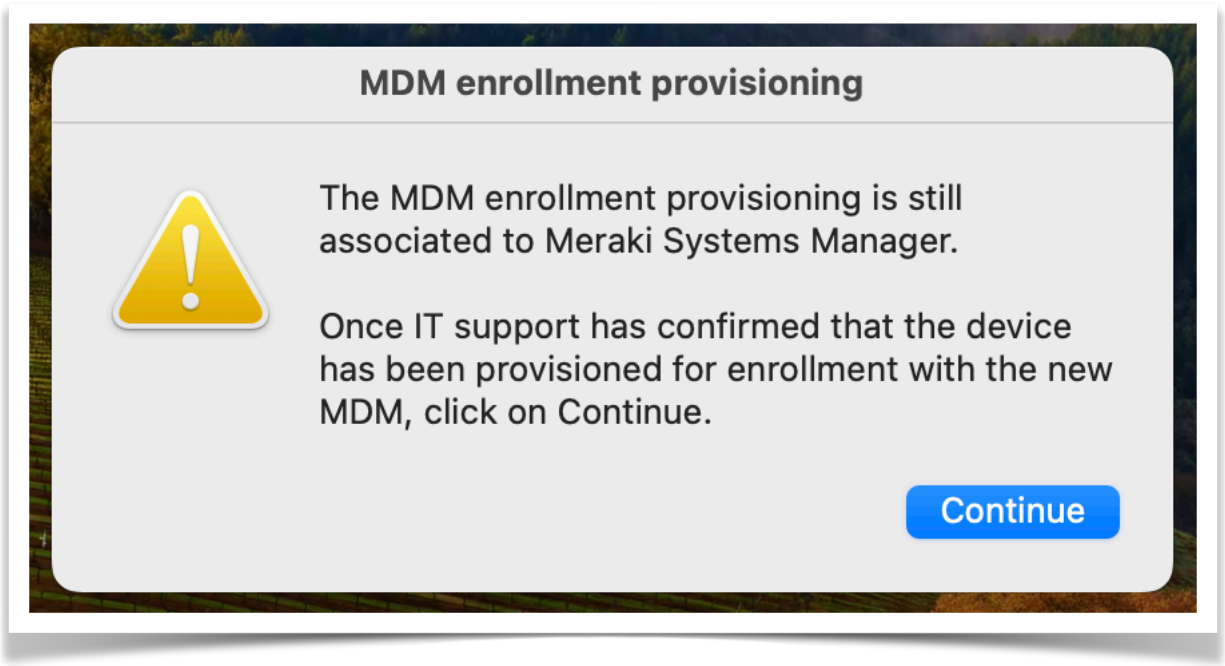
• **IT Support**

- Webhook message received :
"Device unenrolled from Meraki Systems Manager"

• **End User**



- Message displayed :
"The MDM enrollment provisioning of this device must be managed by the IT Support. Please follow the displayed instructions."
- Dialog displayed :
"Once IT support has confirmed that the device has been provisioned for enrollment with the new MDM, click on Continue."



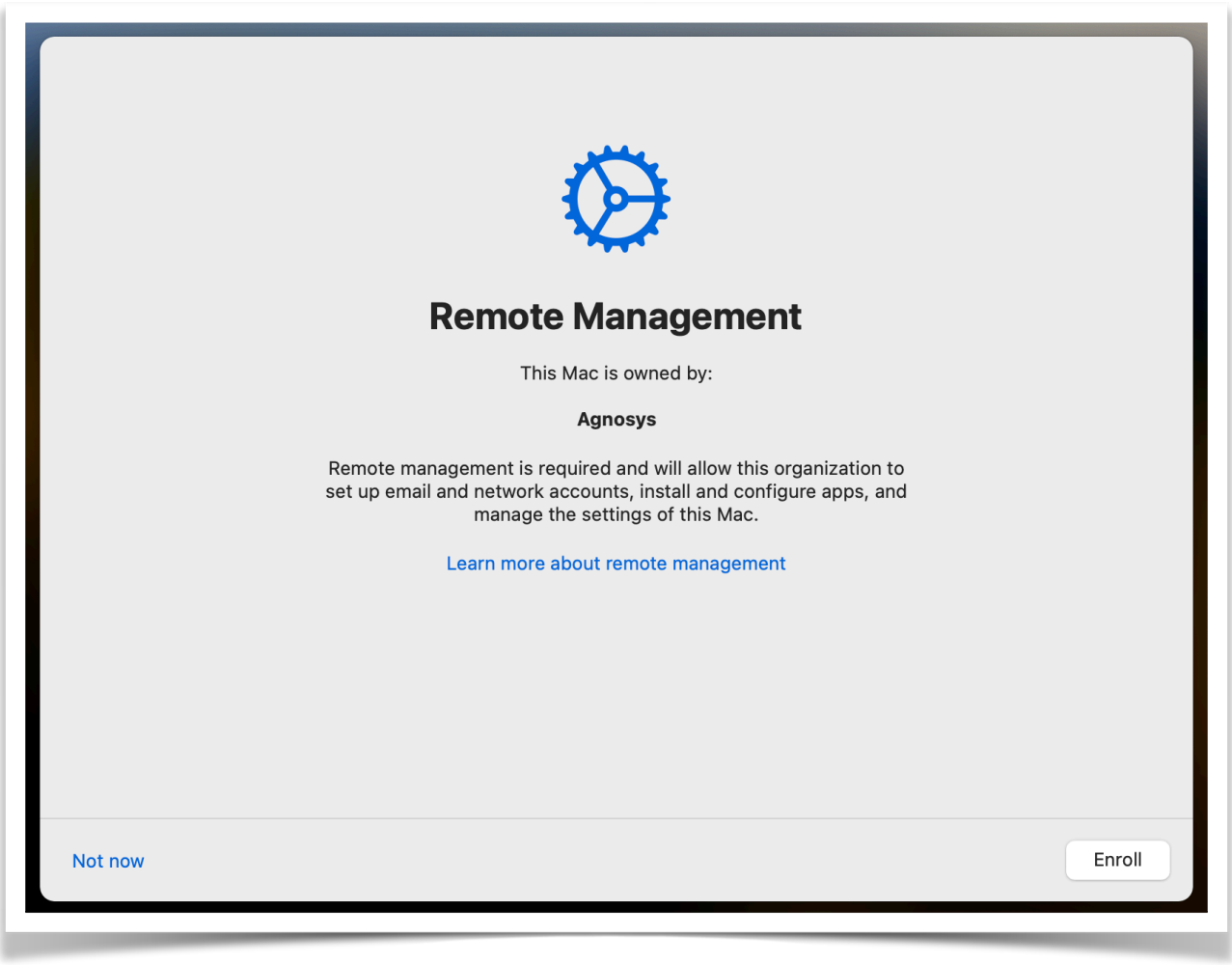
- Message displayed if the "Continue" button is clicked before the next step is done :
"The MDM enrollment provisioning is still associated to Meraki Systems Manager. Once IT support has confirmed that the device has been provisioned for enrollment with the new MDM, click on Continue."

• **IT Support**

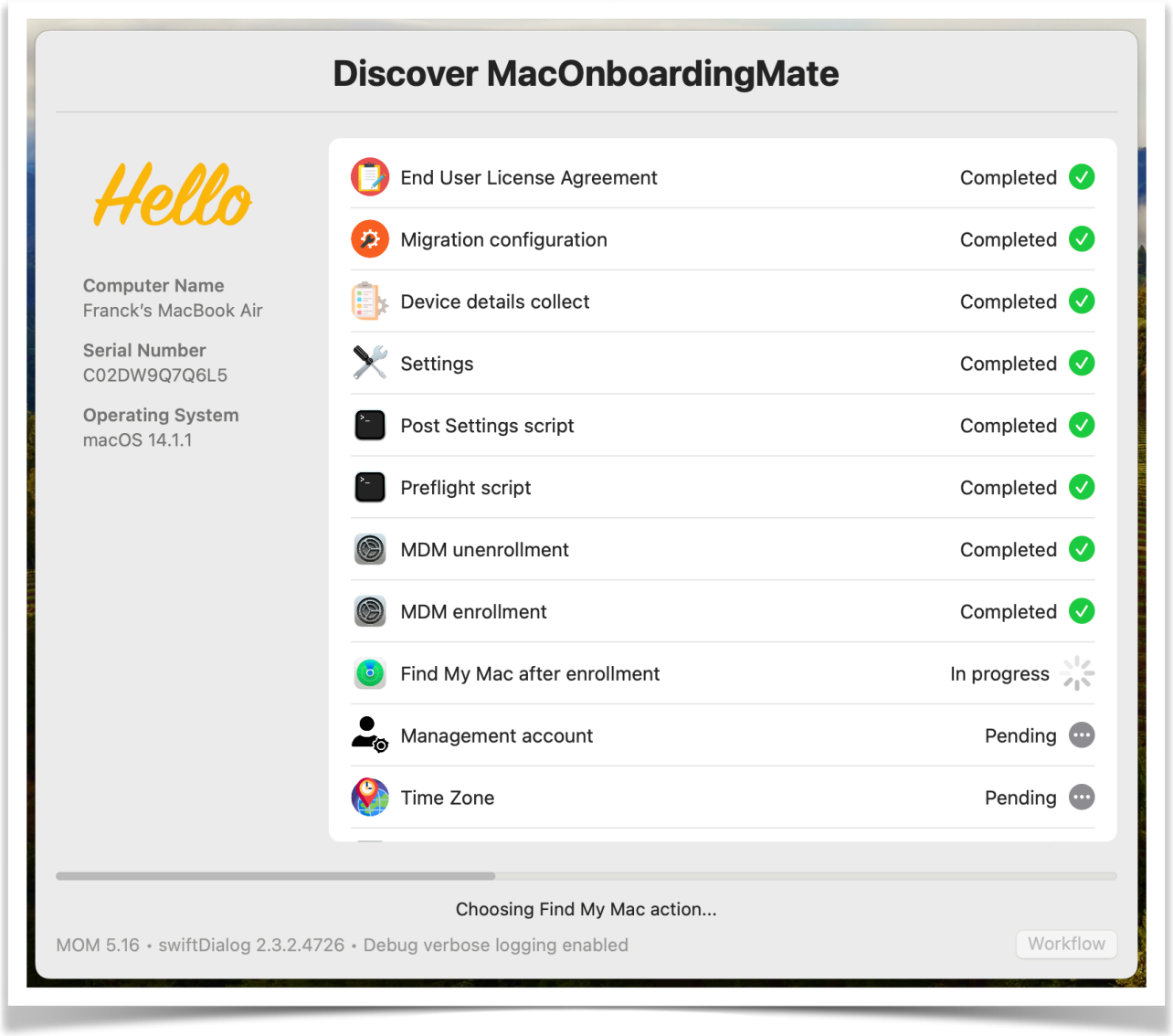
- Webhook message received :
"Device pending provisioning to enroll in UltimateMDM"
- In AxM : device assigned to UltimateMDM
- In UltimateMDM : device assigned to an Automated Device Enrollment Profile
- IT Support confirms to the user that he can click on "Continue"

• **End User**

- User clicks on "Continue"



With macOS 14 or later, a Remote Management pane is displayed in full screen mode. With macOS 13 or earlier, a device enrollment notification is displayed in the upper right corner of the screen. The workflow is paused until the enrollment is done.



The device is enrolled in UltimateMDM and the workflow continues.

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/MOM/debug"
```

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

Enter your password.

Logs are written in /private/var/log.

Warning : Do not forget to delete the MOM 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 MOM 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 "MOM-"

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 "MOM-"

Enter your password.

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

Reset the safeguards that may prevent a MOM workflow to be executed

MOM implements multiple safeguards to prevent the unexpected execution of a MOM workflow :
- detection of a MOM workflow in Launcher mode already executed
- detection of a MOM workflow in AutoLauncher mode already executed
- detection of a running MOM workflow (another one which has not yet ended)
- detection of a postponed MOM workflow (another one which is scheduled to run later).

The counterpart is that these safeguards may prevent a MOM workflow to be executed, specifically during testings.

To defeat the safeguard associated to the "MIGRATION_DISALLOWED_AFTER_WORKFLOW_DONE" key set to "true" :
- open a Terminal Window as an administrator account
- type the following command :

```
rm /Library/Application\ Support/MOM/MOM-*.done
```

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.mom_supervisor
sudo launchctl bootout system/com.agnosys.mom
```

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.

In the context of an MDM switching, mom_supervisor remains bootstrapped after these actions so the migration process is automatically restarted when a user logs in. To terminate an MDM switching, mom_supervisor must be deactivated manually using the launchctl bootout command.

No enrollment notification displayed while recording a screencast

To enable the display of enrollment notifications while recording a screencast :
- macOS 13 and later :
    - open System Settings > Notifications
    - in the "Notification Centre" section, enable "Allow notifications when mirroring or sharing the display"

macOS 12 and earlier :
    - open System Preferences > Notifications & Focus
    - in the "Allow notifications" section, enable "When mirroring or sharing the display".

In the context of a migration, the "screencapture" process can be added to the list of processes that prevent a migration workflow from running when detected ("MIGRATION_DISALLOWED_PROCESSES" key).

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

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

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

Support

Paid support included in MacOnboardingMate offers

Send your support request to mom.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/C01JLJ8S0RW

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.

MacOnboardingMate 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.