

MacOnboardingMate

Integration Guide



Agnosys

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

MOM Integration Guide

v6.06 - 2025/06/18

Introduction	8
Synopsis	10
Implementing Launcher mode	10
Implementing AutoLauncher mode	12
Known issues and limitations	14
Homebrew integration	14
Kandji	14
Software requirements	15
macOS	15
MacOnboardingMate packages	15
Packaging editor	15
Property List editor	15
Omnissa Workspace ONE Admin Assistant	16
Text Editor	16
Automated Device Enrollment	16
MOM Toolkit installation	17
Encryption keys creation	18
Launcher configuration file edition	20
Access to the configuration file template	20
License key	20
Security code	20
Reference for configuration file keys	21
Location configuration files edition	22
Access to the configuration file template	22
Reference for configuration file keys	22
License key	22
Password complexity	23
FileWave : APIAUTHENTICATIONSTRING key	24
Hexnode UEM : APIAUTHENTICATIONSTRING key	26
Jamf Pro - API Roles and Clients : APIAUTHENTICATIONSTRING key	27
Jamf Pro - User account : APIAUTHENTICATIONSTRING key	31
Jamf School : APIAUTHENTICATIONSTRING key	34
JumpCloud : APIAUTHENTICATIONSTRING key	35

Meraki Systems Manager : APIAUTHENTICATIONSTRING key	36
Microsoft Intune : APIAUTHENTICATIONSTRING key	37
Miradore : APIAUTHENTICATIONSTRING key	42
Mosyle Business : APIAUTHENTICATIONSTRING key	43
Mosyle Manager : APIAUTHENTICATIONSTRING key	44
Omnissa Workspace ONE - OAuth authentication : APIAUTHENTICATIONSTRING key	45
Omnissa Workspace ONE - Basic authentication : APIAUTHENTICATIONSTRING key	48
SimpleMDM : APIAUTHENTICATIONSTRING key	54
Microsoft Teams integration	55
Location configuration files to Custom configuration profiles conversion	60
MOM Content building	62
Package signature requirement for AutoLauncher mode	62
Package signature options	64
Content gathering	64
Project opening	65
Signing configuration	66
Project building	67
MOM Core Companion building	70
Configuration profiles requirements	72
Privacy Preferences Policy Control	72
Background Item Management	73
Provisioning FileWave for AutoLauncher mode	75
General configuration	75
Custom Fields	77
Custom configuration profile	78
MOM-Content package	78
MOM-Core package	79
Deployment on the MOM group	79
Provisioning Hexnode UEM for AutoLauncher mode	81
General configuration	81
Custom configuration profile	82
MOM-Content package	82
MOM-Core package	83
Provisioning policy configuration	83

Provisioning Jamf Now for AutoLauncher mode	85
General configuration	85
Custom configuration profile	85
MOM-Content package	85
MOM-Core package	86
Provisioning Jamf Pro for AutoLauncher mode	87
General configuration	87
Custom configuration profile : importing a .plist file	87
Custom configuration profile : importing a .mobileconfig file	88
MOM-Content package	88
MOM-Core package	88
Configuration of the PreStage Enrollment	89
Provisioning Jamf School for AutoLauncher mode	90
General configuration	90
Custom configuration profile	90
MOM-Content package	91
MOM-Core package	91
Configuration of the Automated Device Enrollment profile	91
Provisioning JumpCloud for AutoLauncher mode	93
General configuration	93
Custom configuration profile	94
MOM-Content package	94
MOM-Core package	95
Provisioning Kandji for AutoLauncher mode	96
General configuration	96
Custom configuration profile	96
MOM-Content package	97
MOM-Core package	97
Provisioning Meraki Systems Manager for AutoLauncher mode	98
General configuration	98
Custom configuration profile	99
MOM-Content package	99
MOM-Core package — Via Apps	99
MOM-Core package — Via Provisioning Packages	100

Provisioning Microsoft Intune for AutoLauncher mode	101
General configuration	101
Custom configuration profile	101
MOM-Content package	102
MOM-Core package	103
Provisioning Miradore for AutoLauncher mode	106
General configuration	106
Custom configuration profile	106
MOM-Content package	106
MOM-Core package	106
Provisioning policy configuration	107
Provisioning Mosyle Business for AutoLauncher mode	108
General configuration	108
Custom configuration profile	108
MOM-Content package	108
MOM-Core package — Via Management Profile	109
MOM-Core package — Via InstallApplication	110
Provisioning Mosyle Manager for AutoLauncher mode	111
General configuration	111
Custom configuration profile	111
MOM-Content package	111
MOM-Core package — Via Management Profile	112
MOM-Core package — Via InstallApplication	113
Provisioning Omnissa Workspace ONE for AutoLauncher mode	114
General configuration	114
Custom configuration profile	114
MOM-Content package (signed package)	115
MOM-Content package (unsigned package)	117
MOM-Core package	120
Provisioning SimpleMDM for AutoLauncher mode	121
General configuration	121
Custom configuration profile	121
MOM-Content package	121
MOM-Core package	122

Implementing provisioning over the Setup Assistant or Login Window	123
Requirements for provisioning over the Setup Assistant	123
Requirements for provisioning over the Login Window	124
Location configuration file	124
Implementing MOM for MDM switching	127
MDM switching using Launcher mode	127
MDM switching using AutoLauncher mode	127
Implementing mSCP compliance	130
References	130
Step 1 : Generate compliance assets with Jamf Compliance Editor	130
Step 2 : Provision Jamf Pro	132
Step 3 : Provision another MDM	134
Step 4 : Configure MOM for Jamf Pro or another MDM	139
Step 5 : Check the result of the integration	141
Onboarding a Mac using MOM in Launcher mode	144
Enrollment experience	144
MOM execution	144
Onboarding a Mac using MOM in AutoLauncher mode	150
Enrollment experience	150
MOM execution with provisioning over the Setup Assistant	150
MOM execution with provisioning over the Login Window	151
MOM execution with provisioning over the Desktop	151
Localizing MOM	153
Localization of the configuration files for one language	153
Localization of the configuration files for multiple languages	153
Advanced localization	155
Updating MOM	157
MOM Toolkit (Launcher and AutoLauncher modes)	157
Launcher configuration file (Launcher mode only)	160
Location configuration file(s) (Launcher and AutoLauncher modes)	160
Custom configuration profile(s) (AutoLauncher mode only)	160
MOM Content package (Launcher and AutoLauncher modes)	160
MOM Core Companies (Launcher mode only)	161

MOM Core package (Launcher and AutoLauncher modes)	161
Edge cases	162
MDM switching / Meraki Systems Manager / Locked Management Profiles	162
Troubleshooting	170
Enable the logging manually	170
Enable the logging with Custom configuration profile	170
Display the logs from the Console utility	170
Display the logs from the Terminal utility	171
Reset the safeguards that may prevent a MOM workflow to be executed	171
No enrollment notification displayed while recording a screencast	172
Microsoft Intune - Solve a non-reinstallation issue	172
Support	173
Paid support included in MacOnboardingMate offers	173
Free community support	173
Release notes	173

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



MOM Integration Guide

v6.06 - 2025/06/18

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	Traublachasting				
Reset the safeguards	Iroubleshooting				

Implementing AutoLauncher mode



Step	Chapter in this document				
Get a MacOnboardingMate License Key					
Download the MOM-Core Package					
Download the MOM-Toolkit Package	Software requirements				
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					
Create other Location configuration files if necessary	Location configuration files edition				
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	Traublachesting				
Reset the safeguards	Iroubleshooting				

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.

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.

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.

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).

Omnissa Workspace ONE Admin Assistant

If the MDM solution is Omnissa Workspace ONE and the MOM-Content package cannot eventually be signed, download and install Workspace ONE Admin Assistant :

https://customerconnect.omnissa.com/downloads/details?downloadGroup=WSONE-ADMIN-ASSISTANT&productId=1595&rPId=118941

Text Editor

If the MDM solution is Omnissa 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

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

	😺 Install MOM-Toolkit
	Welcome to the MOM-Toolkit Installer
 Introduction Destination Select Installation Type Installation Summary 	You will be guided through the steps necessary to install this software.
	Go Back Continue

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

• • Iauncher.plist		+ Add	D Edit Value	Duplicate	Delete	XML PLIST Format	٥	∱↓ Sort	Q Find	fill Snippets
Key	Туре	Value								
√ Root	Dictionary	\$ 13 ite	ms							
LICENSE	String	🗘 1HiSG	596c9miEFX	hgpGZagzvPLj	uQ6VOB9RkopsqLl	LSbkMD5ltk7Wv0wFK	+ZZ3trlr	AsdlEE	sMS/Fi	HXIng==

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

• • •	🛅 ladmin — mom_rsa_engine.command — 98×15
Last login: Sat Jul 3 ladmin@MBP-Apple ~ % *** Start : mom_rsa_e Value to encrypt or d Encrypted value : RSA yYut79SpeYt5bdv3KEhT5 SZrgRLtIuR9/z6UpMtESO 1ZZ4fTbZXVhNy4DrcQdju Sanity check - Decryp Saving session copying shared his saving historyt completed.	1 18:46:00 on ttys001 /Users/ladmin/Desktop/MOM-Toolkit/mom_secrets/mom_rsa_engine.command ; exit; engine.command *** lecrypt : SuperSecret -Vu7JDIFzHn2WF01bbdY4g3J19iz7m19V0JQ0rkChDwS1G2ajldqgE5z3JDjK7JVaI+xlAyZT6G9v B2wBjnQXyioKG+vftJwvlbiFo0YjXp5WZJ4QXe7qDAw6mLu7o5+mYLcK0Xd6wpQfMSEW11/XwRb/N XHT3Lqc773WzxdCtsfgZWzrXw5YBVVxM6+tp+apptNdOAnDZ90f3yWo7NUfLqMVXMdPjq5PsU4tRT I+kKbvR4gu4fcPMlb26nQAu7lkVbZC7MmRH9L9h+OGkHqRjCaA== ited value of the encrypted value : SuperSecret tory runcating history files
[Process completed]	

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

• • Iauncher.plist		+ Add	Ø Edit Value	Duplicate	ل Delete	XML PLIST Form	\$ at	↑↓ Sort	Q Find	fill Snippets
Кеу	Туре	Value								
∽ Root	Dictionary	✿ 13 ite	ems							
LICENSE	String	🗘 dft27	tgVCpuRtHt	S7uT7qu+5WD	GMB7MO0YzO7L	03cZdD15zkcPRSES	RDDv1uL	VCEWXQ	mCOa7	7r6Q9
DEBUGMODE	String	disab	led							
DNSCHECKHOSTNAME	String	🗘 dns.g	oogle							
SECURITYCODE	String	YN9S	NTyrNn6Z3×	6d1MxuMwLFz	zB/vnMilEU48gR/	u7hrg6KR+k9lLNBl	ezT8k0kg	chEpytY	K+mTL	.3lhFg==

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

• • Iocation_1.plist			+ Add	Ø Edit Value	Duplicate	Delete	XML PLIST Format	٥	∱↓ Sort	Q Find
Кеу	Туре	Value								
∨ Root	Dictionary	64 items								
LICENSE	String	\$ KOoea9wGElHW	RoXIMM	Oxuk7XdfJrS	mQ+fjto5BZm	ızsOvMRJ9GxQK9	mQEtxK6bT/LxTTZDKH	kZQF1	ihdzkgx	(A==

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

	FileWave Administrators
Account Name Phone Email	User details Permissions VPP tokens Application tokens TeamViewer User Details
<pre>svc_telepod</pre>	
L svc_easylaps	Login Name: svc_mom
fwsupport help@filewave.com	Long Name:
💄 fwadmin	
	Phone:
	Email:
	Password: 💿 No change 💿 Set password 💿 Generate and email password
	Comments:

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

ccount Name	Phone Email	User detail	s Permissions VPP tokens Application	tokens TeamViewer
svc_mom		Server/Model		
svc_telepod		V Update Model	Activation Keys	
svc_easylaps		Revert Model	Auditing	
fwsupport	help@filewave.com	General		
fwadmin		Can Administer Users		
		Preferences		
		Change Preferences	Configure User Enrollment	
		Configure Server Settings	Download DEP Certificate	Configure EMM Default Policy
		Upload Server Certificate	Configure DEP Accounts	
		Configure Chromebooks	Configure VPP Tokens	
		Configure Google Firebase	Configure SIS Settings	
		Upload MDM Client Packages	Configure Classroom	
		Clients and Groups		
		Modify Clients/Groups Clear Fileset Status	Set Permissions Change Enrollment Username	View Location Information
		Wipe Devices	Manage Automatic Enrollment	
		Filesets and Groups		
	Manage VPP Tokens	Check LDAP/IDP user permissions	LDAP/IDP user application tokens	Apply Cancel OK

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 :

ccount Name	Phone Email	Oser details Permissions VPP tokens Application tokens Teamviewer
svc_mom		1 token(s) Q. Search
svc_telepod		Non Teles
svc_easylaps		Name A 10ken Default Taken F00.060ff0.05d7.4bf1.00f0.08064b88019b1
fwsupport	help@filewave.com	
fwadmin		
		•
		Token name: Default Takan
		Description: This default token is required for FileWave Admin and cannot be deleted.
		Token: {8e069ff0-e5d7-4bf1-a0fe-e8964b68e18b}
		Regenerate token
		Token (base64): ezhIMDY5ZmYwLWU1ZDctNGJmMS1hMGZILWU4OTY0YjY4ZTE4Yn0=
		Script example: curl -s -k -H "Authorization: ezhIMDY5ZmYwLWU1ZDctNGJmMS1hMGZILWU4OTY0YjY4ZTE4Yn0=" https:// agnosys.filewave.net:20445/inv/api/v1/component/
-	Manage VPP Tokens	Check LDAP/IDP user permissions LDAP/IDP user application tokens Apply Cancel OK

- 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).

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).

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.

Settings : System > API roles and clients
← MOM
Display Name Display name for the API Role.
мом
Required
Privilege documentation Find out which privileges are required for each API endpoint. Jamf Pro API documentation Classic API documentation
Privileges Privileges to be granted for Jamf Pro objects, settings, and actions
Read Computers X Read Sites X Create Computer Extension Attributes X Send Computer Remote Desktop Command X
Read Departments X View Local Admin Password X Send Computer Unmanage Command X Update Computers X ×
View Disk Encryption Recovery Key 🗙 Update User 🗙 Read Computer Extension Attributes 🗙 Create Computers 🗙 Read Buildings 🗙

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).

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).

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).

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).

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).
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.

Microsoft Entra admin center		$\mathcal P$ Search resources, services,	and docs (G+/)	Ф (\$ @ ~	admin.office365@agnos AGNOSYS (AGNOSYS.FR)
 A Home X Diagnose & solve problems 		Home > Agnosys > Manage tenants > Custom domain name Agnosys	es			×
★ Favorites	\sim	« Custom domain names	+ Add custom domain To Diagnose and solve problems Control Refresh Control Co	; A Got feedback?		
Identity Overview	^	Custom url domains (Preview) Troubleshooting + Support	Search Y	Add filter		
8 Users	\sim	New support request	Name Status		Federa	ted Primary
☆ Groups む Devices	~		agnosys.eu Verified agnosys.fr Verified	Т		~
 Applications Roles & admins 	\sim		agnosys.onmicrosoft.com	le		
Billing	\sim					
 Preview hub Domain names 	~					

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.

м	icrosoft Entra admin center			Q	ŝ	୭ ନ	admin.office365@agnos AGNOSYS (AGNOSYS.FR)
^	Home		Home > App registrations > Jamf School Agnosys Demo Branding & properties > App registrations				×
* *	Diagnose & solve problems Favorites	~	+ New registration 🌐 Endpoints 🗙 Troubleshoot 🖒 Refresh 🞍 Download 🗟 Preview features 🖗 Got feedback?				
4	Identity	^	Starting June 30th 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn n	will continu ore	e to pro	vide technical su	oport and security updates $ imes$
()	Overview						
8	Users	\sim	All applications Owned applications Deleted applications				
	All users		P Start typing a display name or application (client) ID to filter these r ⁺				
	Deleted users		5 applications found				
	User settings		Display name 1 Application (client) ID			Created on ↑	U Certificates & secrets
^A Q ^A	Groups	\sim	Jamf School Agnosys Training a7f1b824-1026-4cf8-9de3-e0c3f7b33	93		3/20/2024	🛇 Current
B	Davisas	\sim	Jamf Connect 7593f7dc-e727-4eaf-a2e5-fbc4f20829	5e		12/31/2020	-
40	Devices	~	Jamf School Agnosys Demo 2271eddc-4e0d-4241-81de-39916500	40ec		10/10/2020	🛇 Current
₿,	Applications	\sim	xc XCreds b1e8f52b-e4f9-4b6e-8507-a98d8cd9e	4ec		10/8/2023	-
	Enterprise applications		ZMS b2ae9eaa-68c1-4250-a8b5-2e1d8e97	b4a		2/25/2020	🛇 Current
1	App registrations						
දී	Roles & admins	\sim					

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

Microsoft Entra admin center	\wp Search resources, services, and docs (G+/)	Ф © (D R	admin.office365@agnos AGNOSYS (AGNOSYS.FR)
Home	Home > App registrations > Jamf School Agnosys Demo Branding & properties > App registrations >			
	Register an application			×
X Diagnose & solve problems				
★ Favorites	* Name			
	The user-facing display name for this application (this can be changed later).			
Identity	Mac_API_calls			
(i) Overview				
A Users	Supported account types			
All users	Who can use this application or access this API?			
Deleted users	Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)			
Lies estime	Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Yhov)			
oser settings	Personal Microsoft accounts only			
ገጽ Groups	✓ Help me choose			
E Devices				
Applications	Redirect URI (optional)			
Enterprise applications	We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be channed later, but a value is required for most authentication scenarios.			
App registrations	Select a platform v/ en http://wample.com/auth			
😋 Roles & admins	vegi nepozytowanyouconyoucon vegi nepozytowanyouconyoucon			
B) Billing	register on opp you re working on nere, integrate gainery opps one other opps from outside your organization by adding from citterprise applications.			
 Loons & commont 	By proceeding, you agree to the Microsoft Platform Policies 🖓			
Learn & support	Register			

Enter a name for the application.

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

Click on "Register".

Home > App registrations > Jamf School Agnosys Demo Branding & properties > App registrations >						
👪 Mac_API_calls 🖈 …						×
₽ Search «	📋 Delete Endpoir	nts 💀 Preview features				
Solution Overview	Got a second? We we	ould love your feedback on Microsoft ide	ntity platform (previously Azu	ure AD for developer). $ ightarrow$		
🍊 Quickstart						
🚀 Integration assistant	∧ Essentials					
🗙 Diagnose and solve problems	Display name	: Mac_API_calls	Copy to clipboard	Client credentials	: Add a certificate or secret	
Manage	Application (client) ID	: 80a68fd0-d040-44aa-a0fe-4326	o62219b5 🗋	Redirect URIs	: Add a Redirect URI	
Branding & properties	Object ID	: 4c0cb9a2-8e18-4144-a263-a4d1	8eb3b45d	Application ID URI	: Add an Application ID URI	
	Directory (tenant) ID Supported account typ	: 5af9425b-19f9-47e4-a654-b6eft bes : <u>My organization only</u>	7ae0416	Managed application in I	: <u>Mac_API_calls</u>	
📍 Certificates & secrets						
Token configuration	Get Started Docur	mentation				
-> API permissions						

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

Home > App registrations > Jamf Scho	ool Agnosys Demo Branding & properties > App registrations > Mac_API_ca	Add a client secret		×
Mac_API_calls Cert	tificates & secrets 👒 🖤	Provincian (
Q Search ((Got feedback?	Description	Client secret for Mac_API_calls	
v Search		Expires	730 days (24 months)	\sim
Overview	Cradentials enable confidential applications to identify themselves to the authent	ic.		
Quickstart	scheme). For a higher level of assurance, we recommend using a certificate (inste	ac		
🚀 Integration assistant				
X Diagnose and solve problems	Certificates (0) Client secrets (0) Federated credentials (0)			
Manage	A secret string that the application uses to prove its identity when requesting a	0		
Branding & properties	A secret string that the application uses to prove its harning when requesting a			
Authentication	+ New client secret			
📍 Certificates & secrets	Description Expires Value)		
Token configuration	No client secrets have been created for this application.			
API permissions				
Expose an API				
🙇 App roles				
A Owners				
Roles and administrators				
10 Manifest				
Support + Troubleshooting				
2 New support request				
		Add Cancel		

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

Enter a description and select a life time.

Click on "Add".			
Certificates (0) Client secrets (1) Fee	derated credentials (0)		
A secret string that the application uses to pro	ove its identity when req	uesting a token. Also can be referred to as applica	tion password.
+ New client secret			
Description	Expires	Value 🕕	Secret ID
Client secret for Mac_API_calls	9/13/2026	VIs8Q~Elf7T1wqErgbNSW0sS8XSSgPzwl	c3f33d70-e61e-4bda-9b00-9c12913e3316 🗈 🧵

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.

Home > App registrations > Jamf School Agnosys Demo Branding & properties > App registrations > Mac_API_calls 							
✓ Search «	🖒 Refresh 🛛 🔗 Got feedba	ck?					
Overview							
🗳 Quickstart	Configured permissions						
🚀 Integration assistant	Applications are authorized to call all the permissions the application	Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include					
🔀 Diagnose and solve problems	an the permissions the appreciation	an the permissions the application needs, team more about permissions and consent					
Manage	Add a permission	t admin consent	t for Agnosys	Admin consent requess Status			
Branding & properties	> (Microsoft Craph (1)	ijpe	Description	Autorite Conserve equilibrium status			
Authentication	V Microsoft Graph (1)	Delegated	Circuite and see down and file				
📍 Certificates & secrets	User.Read	Delegated	Sign in and read user profile	NO			
Token configuration							
API permissions	To view and manage consented pe	ermissions for ine	dividual apps, as well as your tenant's co	onsent settings, try Enterprise applications.			
🙆 Expose an API							

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

Request API permissions × Image: Select permission solution to filter these results Application runs as a background service or daemon without a signed-in user.

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".

🕐 Refresh 🔰 🔊 Got feedback?							
A You are editing permission(s) to your application, users will have to consent even if they've already done so previously.							
Configured permissions							
Applications are authorized to call A all the permissions the application n	Pls when they eeds. Learn mo	are granted permission of the second se	sions by users/admins as part of the consent process. The list of configured permissions should include ns and consent				
+ Add a permission 🗸 Grant admin consent for Agnosys							
API / Permissions name	Туре	Description	Admin consent requ Status				
V Microsoft Graph (3)							

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,2β5c8367-328a-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).

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).

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).

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).

Omnissa Workspace ONE - OAuth authentication : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Omnissa 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.omnissa.com/bundle/WorkspaceONE-UEM-Console-BasicsVSaaS/page/UsingUEMFunctionalityWithRESTAPI.html

Create a new role with limited API privileges.

Go to Accounts > Administrators > Roles.

Click on	"Add	Role".
----------	------	--------

Create Role

Name *	MacOnboar	dingMate						
Description *	Limited API	privileges						
Categories		REST					Search Resources	
All		Read	Edit	Category	Name	D	escription	
➤ Accounts				DECT	Admins			Details
MPI				REST	Apps			Details
REST				REST	Compliance	e Policy		Details
SOAP				REST	Custom Att	tributes		Details
Apps & Books				REST	Devices			Details
Assist				REST	REST Enter Integration	prise		Details
Pluoprints				REST	Groups			Details
bideprints				REST	Products			Details
Configurations	\bigcirc			DECT	B (1			B (1)



×

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".

Register a New Clien	t	\times
Name *	MOM-OAuth	
Description *	MOM OAuth Client	
Organization Group *	Agnosys	
Role *	MacOnboardingMate	
Status	Enabled This client will not be able to receive, refresh or create new tokens or make REST API calls to Workspace ONE UEM when disabled.	
	CANCEL	VE

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".

Register a New Client

Name	MOM-OAuth	Organization Group	Agnosys					
Description	MOM OAuth Client	Role	MacOnboardingMate					
		Status	Enabled					
(i) Below is the client ID and se	(1) Below is the client ID and secret for MOM-OAuth.							
Client ID:	a2406ea96bf841788d73b8e64d4fca1e							
Client Secret:	6340B341EBD0C15314D83E0904BC5737 💿 🖺							
This client ID and secret will be used to authenticate Workspace ONE UEM API calls.								
The secret access key displayed on this screen will not be saved in the Workspace ONE UEM console. Please copy it and save to a secure location to authenticate your API client.								
			_					
			CLOSE					

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

Token URL Client ID Client Secret	:	https://uat.uemauth.vmwservices.com/connect/token 3c46dbb9377c4491896989ea2fdae1f0 9A78D983F619CB7873A90908F6AA1409
https://uat.ue	ema	auth.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).

Omnissa Workspace ONE - Basic authentication : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Omnissa 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".

Create Role

Name *	MacOnboard	dingMate						
Description *	Limited API	privileges						
Categories		REST					Search Resources	
All		Read	Edit	Category	Name	D	escription	
➤ Accounts				REST	Admins			Details
₩API		0		REST	Apps			Details
REST				REST	Compliance Po	licy		Details
SOAP				REST	Custom Attribu	ites		Details
Apps & Books				REST	Devices			Details
Assist				REST	REST Enterpris Integration	e		Details
Blueprints				REST	Groups			Details
bideprints				REST	Products			Details
Configurations	\cap	\cap	\cap	DECT	a (1			B (1)

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

CANCEL

×

- 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".

Add Admin

1 Definition	Define and select your ad	min.
	Admin Type	Basic
2 Roles	Username	svc_mom
3 Details	Password	
4 Settings	Confirm Password	
	Require password change at next login	
	First Name	МОМ
	Middle Name	
	Last Name	Service
	Email address	technique@agnosys.fr
	Time Zone	(GMT+01:00) Brussels, Copenhage 🗸
	Locale	English (United States) [English (U \smallsetminus
	Initial Landing Page	Q Devices > Dashboard
		CANCEL

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.

Settings	Agnosys					×
 System Getting Started Branding Enterprise Integration 	System > Advanced > REST API ②	API				
> Security	General Aut	hentication				
Help						
> Localization	Current Setting		Inherit Override			
Terms of Use						
S/MIME	REST API URL					
~ Advanced	5 11 10 1					
~ API	Enable API Access		ENABLED DISABLED			
Event Notifications						
REST API	Service	Account Type	API Key	Description	Allow List	Admin Generated? (1)
Device Root Certificate	Air/March ADI	Admin	zMj+ul/8tDRG7HVdnOPP2M5Q8 Sv5/ogiM=	HGxuhdB8J3		Yes
Site URLs	ALMONDY I	Awridt	-yr-m			

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).

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).

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).

•••	₩	Q. Search (Cmd+E)	··· FS
Q Activity	Teams ··· ≡ +	A mom_feedback Posts Files Notes ⊕	_1 ∨ ··· €
(E) Chat	🗞 Discover		
Calendar Calis Calis OneDrive Admin Bookings	Your teams Agnosys General easylaps-feedback mom_feedback telet	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><text><text></text></text></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	

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

Workflows Save time with automations	>	<
Select the workflow you want to set up for Agnosys > mon	n_feedback.	
webhook		×
Templates		
Post to a channel when a webhook request is received		Ü
铰 Manage	More workflows	;
	·	

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

Post card to channel in Microsoft Teams	Name		
when webhook request is received	Post to a channel wh	nen a webhook request is received	
	Connections *		
	For this workflow to ru	un, all apps must have a valid conn	ection.
	Microsoft Tea	ms sartori.f@agnosys.fr	⊘ ·

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

Post to a channel when a webhook re Workflows via Power Automate See all	quest is received templates	×
Post card to channel in Microsoft Teams when webhook request is received	 Details Microsoft Teams Team Agnosys Microsoft Teams Channel mom_feedback 	~
< Back		Add workflow

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

Post to a channel when a webhook request is received Workflows via Power Automate See all templates	×
Workflow added successfully! Your workflow has been created. Run it by making a POST reguest to	
https://prod-220.westeurope.logic.azure.com:443/workflows/c88838d1dd194c139e11e601af6a6d09/trigger	rs/ 🗈
Want to make changes? <u>Manage your workflow</u>	Done

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.

	riti		1	O Search (Cmd+E)			All and the second second		··· ES
	NEW			Search (Chiute)					So
Q Activity	م م	Workflows Home	Create C	Chat About					0 C
(=) Chat					∑ M	licrosoft Team	ns flows $ \smallsetminus $	$ \mathcal{P} $ Search flows	+ New flow
COS Teams		Flow name			Status	Modified	Co-owners	Тур	be Team an
Calendar		🕫 Post to a channel v	vhen a webh	nook request is received	On 🕐	39 sec ago	FS	Inst	ant N/A
Calls							•		
OneDrive									
Workflows									
+ Apps									
	7 4					and the second second	State States		

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).

~		?
IC .		
"Terminal" would files in your Des	like to access ktop folder.	
Don't Allow	ОК	

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

~ 🛅 MOM-Toolkit
✓
🔚 launcher.plist
Iocations_plists
location_1.plist
location_2.plist
Iocations_profiles
locations_profiles_generator.command
✓ i output
com.agnosys.config.Jamf_Pro.Paris.MOM.mobileconfig
com.agnosys.config.VMware_Workspace_ONE.Paris.MOM.plist

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 Omnissa 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.

Omnissa 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.

SimpleMDM

Signature required.

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 titled "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

√ 🚞 MOM-Toolkit
> 🚞 mom_configs
√
√ 🛅 Content
mom_rsa_key.pri
MOM-Content
mom_content_postinstall.sh
MOM-Content.pkgproj

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.

Project	Settings	Pavload	Scripts
	octango	i dyiodd	Compto
Packages	Settings		
🥪 MOM-Content			
	Default Destination: /	Set	
	Contents	Type: Internal	
		1960	
	Name	Owner Group Permissions	
	~ 👜 /	root wheel drwxr-xr-x	
	> 🔤 Applications	root admin drwxrwxr-x	
	V 🛅 Library	root wheel drwxr-xr-x	
	Application Support	root admin drwxr-xr-x	
	~МОМ	root admin drwxrwxr-x	Empty Selection
	binaries	root wheel drwxr-xr-x	
	Content	root admin drwxr-xr-x	
	> Automator	root wheel drwxr-xr-x	
	> Documentation	root wheel drwxr-xr-x	
	> Extensions	root wheel drwxr-xr-x	
	> Frameworks	root wheel drwxr-xr-x	
	> Input Methods	root wheel drwxr-xr-x	
	> Internet Plug-Ins	root wheel drwxr-xr-x	
	> 📄 LaunchAgents	root wheel drwxr-xr-x	
	> TaunchDaemone	root wheel drawr-vr-v	
	+ -		
+			

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.

•••			🧾 MOM-Content.pkgproj
Project		Settings	Presentation
Packages 🍓 MOM-Content	Build	Name: MOM-Content	

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

Ú.	Packages	File	Edit	View	Presentation	Hierarchy	Project	Build	Window	Help
							Project			¥0
							New Pac	kage		ЖN
							New Pac	kage Ref	erence	₹ ₩N
							Import Pa	ackage		
							Upgrade	to Distri	bution	
							Set Certi	ficate		
							Remove	Certifica	te	

Select Project > Set Certificate.

Draigat Fold	~	
	Choose the certificate to be u	used for signing the distribution.
	Signing Installer packages or dist certificate lets Gatekeeper verify not known malware and has not b	tributions with a Developer ID Installer that a downloaded package or distribution is been tampered with.
🛅 Develop	er ID Installer: AGNOSYS FRANC	E (WDLELDR2B7) (Developer ID C
	Show Cartificate	
	Show Certificate	Cancer

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

•••		MOM-Content.p	MOM-Content.pkgproj					
Project Packages	Settings Build	Presentation		Requirements & Resources		Comments	HENTIGHT	

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

Project building

É	Packages	File	Edit	View	Presentation	Hierarchy	Project	Build	Window	Help	
								Build R	esults	ΰжВ	
								Build		₩В	
								Build a	nd Run	ЖR	
								Build a	nd Debug	ЖY	

Select Build > Build.



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

	e MOM-Content.pkgproj - Build Log
, 4	Suild MOM-Content.pkgproj Project MOM-Content.pkgproj
	📀 Create build folder
~	Create package MOM-Content
>	 Create payload Assemble payload files Unable to copy item at path '/Users/ladmin/Desktop/MOM-Toolkit/mom_content/binaries' because the item could not be found Split forks Create bill of materials Create payload Create pax archive Scripts payload Create distribution script Distribution script and other resources
	Oreate xar archive
	Build Succeeded 01/08/2021 15:11 No issues 01/08/2021 15:11
В	Build succeeded

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.

	Packages wants to sign using key " your keychain.	privateKey" in				
	To allow this, enter the "login" keychain password.					
	Password:					
?	Always Allow Deny	Allow				

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".

~ 🚞 MOM-Toolkit
> 🚞 mom_configs
✓
∨ 🚞 build
🥪 MOM-Content.pkg
> 🚞 Content
📗 mom_content_postinstall.sh
🛄 MOM-Content.pkgproj

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).

	ladmin — mom_core_companion_factory.command — 118×49
Last login: Fri May 24 20 /Users/ladmin/Desktop/MOM ladmin@MacBook-Air ~ % /L *** Start : mom_core_comp Current Path : /Users/lad New launcher.plist file f Disk Image Password : suy Content package size : 16 Read/write disk image siz created : /Users/ladmin/DC /dev/disk4s1 // "disk4" ejected. Prépartion du moteur d'i Lecture de Protective Mas (CRC32 \$F4037986 : Pro Lecture de GPT Header (Pr (CRC32 \$7AB3A946 : GPT Lecture de GPT Partition (CRC32 \$39A16713 : GPT Lecture de (Apple_Free : (CRC32 \$00000000 : (/L	<pre>2:47:19 on ttys000 A-Toolkit/mom_core_companion/mom_core_companion_factory.command ; exit; Jsers/ladmin/Desktop/MOM-Toolkit/mom_core_companion/mom_core_companion_factory.command ; exit; Janion_factory.command *** Jmin/Desktop/MOM-Toolkit/mom_core_companion Found. Jersecret 3 Mo te : 28 Mo sektop/MOM-Toolkit/mom_core_companion/output/MOM-Core-Companion_RW.dmg SUID_partition_scheme Volumes/MOM-Core-Companion imagerie ster Boot Record (MBR : 0) otective Master Boot Record (MBR : 0)) timary GPT Header : 1) 7 Header (Primary GPT Table : 2) 7 Partition Data (Primary GPT Table : 2) ; 3) kple_Free : 3)) pole HFS : 4)</pre>
(CRC32 \$A0F7B535 : dis Lecture de (Apple_Free : (CRC32 \$000000000 : (A	<pre>sk image (Apple_HFS : 4)) : 5) Apple_Free : 5)) Data (Backun GPT Table : 6)</pre>
(CRC32 \$39A16713 : GPT Lecture de GPT Header (Ba	<pre>F Partition Data (Backup GPT Table : 6)) ackup GPT Header : 7)</pre>
(CRC32 \$E7FC11E6 : GPT Ajout de ressources…	Header (Backup GPI Header : 7))
Temps écoulé : 2.481s Taille du fichier : 18005 Secteurs traités : 57344, Vitesse : 7.5 Mo/s Compression : 38.7% created: /Users/ladmin/De	5168 octets, Somme de contrôle : CRC32 \$D1BFA64B . 38276 comprimés esktop/MOM-Toolkit/mom_core_companion/output/MOM-Core-Companion.dmg
Saving session copying shared history saving historytrunc completed.	/ cating history files
[Opération terminée]	

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".

Name: MOM Comment:	
Comment: All 📀 of the expressions below must be true	
All 📀 of the expressions below must be true	
- Inventory Query 📀 in 😒 Mac enrolled using ADE	
+ Cancel	ОК

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

	QueryBuilder - Mac enro	olled using ADE
۹ 🛛	Name: Mac enrolled using ADE	Main Component: All Devices 😋
Component ActivationLock Bypass Code	Include Archived Clients	
 All Devices Apple Media Booster 	All of these expressions must be true	Criteria Fields Clients
DEP Account DEP Device	Not Operating System / OS Type	is 😧 macOS 😧
DEP Profile Fileset Fileset deployment status	Not Security Settings / Enrolled via DEP	equals 🕤 true 📀
nformation related to ActivationLock 3ypass code (supervised iOS devices only)	* - Add Group	Move up Move down Move in next group Move before parent
		Cancel Save

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

		Custom Fields
Custom Fields	Q Search	Field Details
Display Name 🔹	Internal Name	Name
Asset Lag	asset_tag	Asset Tag
Noom	loom	Internal Name
		Using internal name the field can be referenced in other parts of FileWave
		asset_tag
		Description
		Provided By
		Defines how the field value shall be populated
		Administrator
		Assigned to all devices
		Values
		Data Type
		String
		Restrict allowed values
		Use a default value
+ - Ir	nport Export Duplicate	Cancel

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".

• • •					Cre	Create New Association(s)						
Associate MOM with MOM							2 Clients (8 C	lones) 10 G	roups, 2 Mobile	Devices Q Sea	arch clients or group	
Search: Everyth	ing Clients	Mobile	Groups	Clear	r all filters							
Name -		D	Model	IP	Last Connect	Lock	Free Space	Platform	Comment	Serial/MAC	Imaging MAC Address	
Enrollment	20	1										
Platform	20	4										
Software	21	0										
🕨 🖿 EasyLA.	20	9										
MOM 💿	25											
🕨 🖿 Telepod	21	2										
										Cancel	Create Association	
										Gancer	Create Association	

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



In the toolbar, click on "Update Model".

	Update Server Model
V	Do you really wish to update the FileWave serve model?
	Update Model Cancel

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

hexnode mdm Enroll Manage	Policies Apps Content Re	eports Admin Get Start	red Q Search Devices, User	s or Policies	A ? 🔕
General Settings	Apple DEP				
Enrollment	Apple's Device Enrollment Program lets y	ou enroll your corporate Apple dev	rices and have it fully configured o	out-of-the-box.	
APNs					? ▷
✓ Apple Business/School Manager	DEP Devices DEP Configuratio	n Profiles DEP Accounts			
Apple DEP	From here, you can manage the devic	es associated with your DEP accou	nts. View device details and assoc	iate configuration profiles	with the
Apple VPP	devices.				
Configurator Enrollment		Add DEP Account	Sync with DEP 🥲		
Android Enterprise	Select DEP Account 👻	Associate DEP Profile		Search	Q
SCCM	Serial Number	Model	Profile	Profile Status	Last A
G Suite		IMAC 21 5"/6770M	Shared Mac	Assigned	
Okta					
Android ROM/OEM Enrollment					
Email	Page size 10 🔻				1-1 of 1

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

	115			
Group Name * Mac	enrolled using ADE			?
Description				⊳
	B			
Choose Geofences/Loc	ation filters		 Inclu 	de O Exclude
Bay Area	LA County	Sydney	London	
Dubai	Berlin	Singapore	Hong Kong	
Washington				
Create New Geofences				
T create new Georenices				

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

hexnode mdm Enroll Manage F	Policies Apps	Content Reports	Admin 0	Get Started		Q Searc	h Devices, Users or Policies	ф 👩
My Files Kiosk File Shortcuts Documents	My Files Distribute files fr Add	om Hexnode MDM portal I	to a designated	space within an er	rolled device.		Search here	?
Media		File Name com.agnosys.config.Hexr is.MOM.mobileconfig	node_MDM.Par	Version 1	File Format	Added On 04/09/2022 21:19	Last Modified 04/09/2022 21:19 🚯 🕹	3 Ŵ

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

he>	knode mdm	Enroll	Manage	Policies	Apps	Content	Reports	Admin	Get Started	Q Search Devices, Users or Policies		A : 🕲
App Add E	Settings nterprise and Store apps	to the list,	to push them la	ater to device	es directly o	r through polic	ies.					
Apps	App groups Ap	p catalog	s Store La	ayouts							Filter Appr	
+A	App 🔺		Publisher		Category	Plat	form	Price	License Type No of Devices	Upload Status	All Categories	\$
	MOM-Conter	ıt	Enterprise	e	Utilities	6		Free	0	Success	App Type Store app Enterprise app	
										1-1 of 1	 Web app Android Enterprise 	2

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

hexnode mdm Enroll	Manage Policies	Apps Con	tent Reports	Admin	Get Started	Q Search Devices, Users	or Policies 🗘 ? 👰
App Settings Add Enterprise and Store apps to the list, to	push them later to dev	ices directly or throu	gh policies.				
Apps App groups App catalogs	Store Layouts						
+ Add Apps - Delete					МОМ	×Q	Filter Apps
П Арр 🔺	Publisher	Category	Platform	Price	License Type No of Devices	Upload Status	All Categories \$
MOM-Content	Enterprise	Utilities	<u>(6)</u>	Free	0	Success	App Type Store app Enterprise ann
MOM-Core	Enterprise	Utilities	(6)	Free	0	Success	Web app Android Enterprise
						1-2 of 2	License Type Free Paid

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

⊒ jamf NOW	< Automa Device	ated Device Enrollment S		Ó	Sync Devices
Devices Apps		IMAC 21.5"/6770M Serial Number: C02GD7ADDHJN	Paris A Unassigned	Not Managed	
Blueprints					
C APNs	\odot				
//→ Auto-Enrollment	\odot				

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

7	School					Agnosys Demo	~ \$	8 P
888	Dashboard	Shared M	Лас		Jamf School / Profiles	/ Automated Device E	nrollment Profile	s / Shared Mac
D	Devices	~						
8	Users		Shared Mac macOS					
ш	Classes		🗍 1 device					
Ø	Incidents	Genera	macOS Settings Onboardin	Profiles and packages	s			
8	Profiles	^						
	Overview		Profile scope To ensure the selected profile	es remain installed on devices	s after enrollment, en	sure the scope		
	Automated Device Enrollment Profiles		of the profile includes the dev	vices in the scope of the Auto	omated Device Enrollr	nent profile.		
	Apps	~	Profiles	MOM-Custom configura	tion profile	× •		
۵	Documents	~						
8	Scripts			+ Add				
Þ	Wallpapers		In-house macOS packages	MOM-Content		× •) (×		
Ø	Organisation	~						
				MOM-Core-6.02		× ·		
API	2.0 Documentation			+ Add				
Lice	ense Management	Remove Pro	ofile				Cance	I Save

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

•7	jumpcloud	d Device Groups ©			S Pricing	4 Alerts	Resource	es 💿 Sup	port FS	
G	Home	+	Q Se	arch					2 groups	delete
✓ USE	R MANAGEMENT									
8	Users		Туре	Group 🔺						
#fk	User Groups		ŦŦ	Onboarding Group of Devices						>
✓ USE	R AUTHENTICATION									
60	LDAP		Ŧ	Paris						>
C	RADIUS		-	Group of Devices						
	sso									
✓ DE\	/ICE MANAGEMENT									
Ģ	Devices									
•	Device Groups									
0	Policy Management									

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

Automated Device Enrollment Complete	Renew Token
Automated Device Enrollment (formerly DEP) allows for your organization's devices to automatically enroll into Kandji when they are first unboxed and connected to the internet.	
DEFAULTS	Ø Edit
Device Enrollment 🥑 MOM	
Support Phone Number +33 6 82 59 37 04	
Support Email Address technique@agnosys.fr	
AUTOMATED DEVICE ENROLLMENT DEVICES Last fetch 3 minutes a	go 🖉 Fetch now
1 device assigned to Kandji:	
🖵 1 Macs	
. O iPhones	
O Apple TVs	
[] O iPods	
View more details on the Automated Device Enrollment Devices page.	

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

cisco Meraki	Q Search Dashboard 🕫 Announcements ▾ . ⑦ Help ▾ sartori.f@agnosys.fr ▾					
ORGANIZATION	New in Dashboard: Mobile App Update -	Version 4.5.0 and 10 other features. Read more.		×		
Agnosys - Meraki Enterprise	nosys - Meraki terprise Apple Device Enrollment Program					
NETWORK	Managa profiles Assign partings Domain pattings Tag - Mayo - Astigns - Domain davias - Court					
Paris				Faitial synce		
	DEP	del Terre Naturado Cadal - Acalana des	Settings assign	Settings push +		
	Status enrollment Name Mod	del Tags Network Serial Assigned by	Assigned date time	time Settings		
Custome Manager	Assigned macOS iMa	c mom Paris C02GD7ADDHJN itunesvpp@agnos	Aug 06 2021, 11:27 Aug 06 2021, 11:27 CEST CEST CEST	- Shared Mac v1		
Systems Manager						
Organization						

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 Program	3 Requirements 4 Detection rules 5 Assignments 6 Review + create				
Select file * i	MOM-Content.pkg				
Name * 🛈	MOM-Content.pkg				
Description * (i)	MOM-Content.pkg Agnosys 0 selected Enter a valid url Enter a valid url				
Publisher * 🕕					
Category 🛈					
Information URL (i)					
Privacy URL ①					
Developer (i)					
Owner 🛈					
Notes ①					
Logo ①	Select image				
Previous Next App information - Select file > Select ap - App package file > Se - Publisher : Agnosys	p package file elect a file > MOM-Content.pkg > OK				
Program : no scripts need to	be configured				
App information Program	3 Requirements (4) Detection rules (5) Assignments (6) Review + create				
Minimum operating system * \bigcirc	macOS High Sierra 10.13 V				

- Requirements

Previous

_

_

- Minimum operating system : macOS High Sierra 10.13

Next

📀 App information 🛛 🤡 Program 🔗 Requirem	ents Oetection rules (5) Assignments (6) Review + create					
Ignore app version ① Yes						
Configure the app bundle identifiers and version numbers to be used to detect the presence of the app.						
Included apps						
Provide the list of apps included in the uploaded file. The app list is case-sensitive. The app listed first is used as the primary app in app reporting. Learn more about included apps.						
App bundle ID (CFBundleIdentifier)	App version (CFBundleShortVersionString)					
App bundle ID (CFBundleIdentifier) com.agnosys.MOM-Content	App version (CFBundleShortVersionString)					
App bundle ID (CFBundleIdentifier) com.agnosys.MOM-Content Enter bundle ID	App version (CFBundleShortVersionString) 1.0 Enter app version					

- 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 Program	③ Requirements ④ Detection rules ⑤ Assignments ⑥ Review + create				
Select file * ①	MOM-Core-6.02.pkg				
Name * 🕕	MOM-Core-6.02.pkg				
Description * ()	MOM-Core-6.02.pkg				
Publisher * ①	Agnosys				
Category (i)	0 selected Enter a valid url Enter a valid url				
Information URL ①					
Privacy URL (i)					
Developer (i)					
Owner (i)					
Notes ①					
Logo (i)	Select image				
Previous Next - 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					
📀 App information 🛛 📀 Program	3 Requirements (4) Detection rules (5) Assignments (6) Review + create				
Minimum operating system * 🕕	macOS High Sierra 10.13 V				
Previous Next					

- Requirements

- Minimum operating system : macOS High Sierra 10.13

App information 🛛 Program 🔇 Requirement	nts					
Ignore app version ① Yes No						
Configure the app bundle identifiers and version numbers to be used to detect the presence of the app.						
Included apps						
i Provide the list of apps included in the uploaded file. The app list is case-sensitive. The app listed first is used as the primary app in app reporting. Learn more about included apps.						
App bundle ID (CFBundleIdentifier)	App version (CFBundleShortVersionString)					
com.agnosys.MOM-Core	6.02					
Enter bundle ID	Enter app version					
Previous Next						

- 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.

	Dashboard (Organization	Management S	ecurity DNS Filtering	Support *	Session expires in: 00:05	Franck Sartori 5 🖒 Logout
				Your Trial end	s in 213 day(s). <u>Click here</u> to upgrade no	ow.	
é	Apple Basic Set	up 🔻		Enrollment (DEP)		Automated Device Enrollment Profile	×
64	Push Certificate	0	All your Apple accounts an "Apple Integration" on the	nd its profiles are listed below. To a e left menu.	dd a new one or to edit click at	Options during the enrollment	
•	Apple Business Ma	anager 🥑	iOS r	macOS tvOS		You can also upload any signed PKG from other management software as Munki).	re (such
	Users & Group	DS ►	Q Search by name Mosyle Business		View devices · New profile	▲ MOM-Core.pkg MOM-Core.pkg 3.03 MB (remove)	
۲	Integrations	•	Shared Mac (default) View device list				
	Preferences	Þ				Important Note: If the devices are still boxed, they will receive this Automated Device Enrollin configuration during the Setup Assistant steps on the device (first steps). If the devices have already been used, they must be formatted to receive this Auto Device Enrollment configuration. If your devices are running macOS 10.12.4 or later, and you don't want to for them, you can use the Terminal to apply this Automated Device Enrollment configuration profile running the command below. For Mac OS 10.12.4 through 10.13.4 use: "sudo profiles -N" For Mac OS 10.13.4 and later use: "sudo profiles renew -type enrollment" *Note: You must have Admin rights to the Mac in order to run this command Save	ment the omated rmat

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 Omnissa 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 Omnissa 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 Omnissa Workspace ONE. Please refer to Omnissa 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 Omnissa 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".

Resou Pro	rrces > Profiles & Baselines						
Filters » ADD V EXPORT Search List							
	Profile Details	Payloads	Managed By	Assignment Type	Assigned Groups	Installed Status	Status
_ ♪	MOM Apple macOS - Device Custom Settings	1	Agnosys	Auto	Agnosys	View	0

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 Omnissa Workspace ONE console.

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

Add Application

Organization Group ID *	Agnosys	
Application File *	MOM-Content.pkg	UPLOAD

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".

Add Application

Application File

MOM-Content.pkg

Deploy this file as a Bootstrap Package for Expedited Delivery or manage the complete lifecycle with Full Software Management.

Select how you want to deploy this file below.

Deployment Type	EXPEDITED DELIVERY	FULL SOFTWARE MANAGEMENT
Deployment Type	EXPEDITED DELIVERY	FULL SOFTWARE MANAGEMEN

Deploy as a Bootstrap Package, without advanced deployment options, for rapid delivery of high-priority signed distribution packages (.pkg) immediately after enrollment. This option is optimal for open-source or home-grown tools necessary for baseline configuration. Traditional software for end user productivity must not be distributed via this method Click here for more info

Select "Expedited Delivery".

Click on "Continue".

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

istribution	Distribution			
	Name *	MOM-Content		
	Description	Assignment Description	n	
	Assignment Groups *	To whom do you want t	o assign this app?	
	App Delivery Method *	• Auto	On Demand	١
	Display in App Catalog			١

CANCEL

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".

•	macOS	MOM-Content Bootstrap Package Agnosys	Not Applicable	Apple macOS/All/MacBook P		Not Applicable
	⊖ 🖌 max05	MOM-Content Bootstrap Package	Not Applicable		Not Applicable	Not Applicable

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.

	Parsing completed	
MOM-Content.pkg	Reveal in Finder Done	
		Add More

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

•••	C / Boodinents		· v	000		
Favourites	Name	 Date Modified 	Size		Kind	
AirDrop	🗸 🚞 Workspace ONE Admin Assistant	Today at 19:45			Folder	
Recents	✓	Today at 19:44			Folder	
	😻 MOM-Content-1.0.pkg	Today at 19:44		54,7 MB	Installer package	
	MOM-Content-1.0.plist	Today at 19:44		2 KB	property list	
Desktop						
🕒 Documents						

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

Open the Omnissa Workspace ONE console.

Go to Resources > Apps > Native.

Click on "Add" > "Application File".

Add Appli	cation				
Organization	Group ID *	Agnosys			
Application Fi	le *				UPLOAD
Select the Organ	nization Group the	at encompasses the device	es that ar	e to be prepared wi	ith MOM.
Click on "Uploa	d" and upload MC	OM-Content.pkg (Type : Lo	cal File).		
Click on "Contin	ue".				
Add Applicatio	'n				×
Application File					
Deploy this file as a B	ootstrap Package for Expedite	ed Delivery or manage the complete lifecycle w	ith Full Softwar	e Management.	
Select how you want	to deploy this file below.				
Deployment Type	EXPEDITED	D DELIVERY FULL SOFTWARE MAN	AGEMENT		
Configure advanced o	leployment options to manage	e the complete software lifecycle for macOS fil	e types such as	.dmg, .pkg, and .mpkg. Click here	for more info
(i) Additional metad	ata is required to configure ful	Il software lifecycle management for this file.			
Download and Ins here for more info	itall the VMware AirWatch Adn ว	min Assistant Tool to generate a metadata file	.plist), then upl	oad the metadata file once compl	lete. Click
Generate Metadata	🛨 Workspace	ONE Admin Assistant for macOS			
Metadata File *			UPLOAD]	

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".

MOM-Content - Assignment

Distribution		Distribution				
Restrictions	<a>	Distribution				
		Name *	MOM-Content			
		Description	Assignment Description			
		Assignment Groups *	To whom do you want to assign this ap	p?		
		Deployment Begins *	12/31/2021 📋 12:00	AM ~ (GMT+01:00) Brussels, Copenhagen, Madrid, Paris		
		App Delivery Method	 Auto 	On Demand		(j)
		Display in App Catalog				(j)
					CANCEL	CREATE

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".

•	macOS	MOM-Content Agnosys	1 version(s)	Apple macOS/All/MacBook P			12/31/2021 7:53:28 PM
	⊖ 🖉 mac05	MOM-Content 会会会会会	1.0.0.0	Not Applicab	e View	0	12/31/2021 7:53:28 PM

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".

•	macOS	MOM-Core Bootstrap Package Agnosys	Not Applicable	Apple macOS/All/MacBook P		Not Applicable		12/31/2021 6:01:02 PM
	○ 🖋 mecOS	MOM-Core Bootstrap Package	Not Applicable	Ν	Not Applicable	Not Applicable	0	12/31/2021 6:01:02 PM

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

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

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, 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.

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

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.

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 2.5.2 and later.

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.

TIMEZONE : set to the name of a time zone from among those returned by the systemsetup -listtimezones command ; when Location Services cannot be enabled during the Setup Assistant, 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)

- PRIVACY_CONTROL (list of privacy settings that must be enabled by the user before the workflow can proceed)

- KERBEROS_SSO_EXTENSION_INTEGRATION (wait for a Kerberos ticket to be acquired, wait until password synchronization between the local and network accounts is complete).

• 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 :

- this key is ignored on macOS 15.4 and later, as onboarding over the Setup Assistant must occur before the "Create a Computer Account" pane is displayed

- set to "true" to display MOM after the end-user account is created via the "Create a Computer Account" pane, or set to "false" to display MOM before that pane

- setting this key to "true" only makes sense if the Automated Enrollment profile is configured to show the "Create a Computer Account" pane.

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", "shutdown" and "undefined" are supported; "logout" causes the Mac to display the Login Window once provisioning is complete ; when appropriate, "undefined" is automatically converted to "logout".

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

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".

CIS Benchmark - Level 1 macOS 15.0	Rules 95 Rules, 95 included, 95 found Sort - ID				
Sections	☑ 3.5 Configure Audit Log Files to Not Contain Access Control Lists				
All Sections	✓ 3.5 Configure Audit Log Folder to Not Contain Access Control Li				
	3.1 Enable Security Auditing				
Auditing	✓ 3.5 Configure Audit_Control to Not Contain Access Control Lists				
macOS	✓ 3.5 Configure Audit_Control Group to Wheel				
	 3.5 Configure Audit_Control Owner to Mode 440 or Less Permis 3.5 Configure Audit_Control Owner to Root 				
Password Policy					
	✓ 3.5 Configure Audit Log Files Group to Wheel				
System Settings	✓ 3.5 Configure Audit Log Files to Mode 440 or Less Permissive				
Supplemental	✓ 3.5 Configure Audit Log Files to be Owned by Root				
	3.5 Configure Audit Log Folders Group to Wheel				

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 Omnissa 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 titled "MOM Content Building" and specifically the section titled "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/ Omnissa 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.

✓
> 🚞 mom_configs
> 🚞 mom_content
✓
> 🚞 mSCP_audit_files
Workspace_ONE_plists_converter
✓
🔝 com.apple.applicationaccess.plist
com.apple.controlcenter.plist
🔚 com.apple.loginwindow.plist
com.apple.MCX.plist
🔚 com.apple.mobiledevice.passwordpolicy.plist
com.apple.Safari.plist
🔚 com.apple.screensaver.plist
com.apple.security.firewall.plist
🔚 com.apple.SoftwareUpdate.plist
com.apple.systempolicy.control.plist
🔜 com.apple.Terminal.plist
com.apple.timed.plist
v ists_formatted_for_custom_settings
✓ i output
Workspace_ONE_plists_converter.command

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".

~		Workspace_	ONE_	_plists_	_converter
---	--	------------	------	----------	------------

🗸 🚞 plists

- com.apple.applicationaccess.plist
- com.apple.controlcenter.plist
- com.apple.loginwindow.plist
- com.apple.MCX.plist
- com.apple.mobiledevice.passwordpolicy.plist
- com.apple.Safari.plist
- com.apple.screensaver.plist
- com.apple.security.firewall.plist
- com.apple.SoftwareUpdate.plist
- com.apple.systempolicy.control.plist
- 🔝 com.apple.Terminal.plist
- com.apple.timed.plist
- plists_formatted_for_custom_settings

output

- com.apple.applicationaccess.plist
- com.apple.controlcenter.plist
- com.apple.loginwindow.plist
- com.apple.MCX.plist
- com.apple.mobiledevice.passwordpolicy.plist
- com.apple.Safari.plist
- com.apple.screensaver.plist
- com.apple.security.firewall.plist
- com.apple.SoftwareUpdate.plist
- com.apple.systempolicy.control.plist
- 📄 com.apple.Terminal.plist
- com.apple.timed.plist
- Workspace_ONE_plists_converter.command

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 titled "Custom configuration profile" included in the chapter titled "Provisioning Omnissa 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 titled "Custom configuration profile" included in each chapter titled "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".

✓
> 🚞 mom_configs
> 🚞 mom_content
✓
✓
✓ audit_files_plists
📗 org.cis_lvl1.audit.plist
audit_files_profiles
📄 audit_files_profiles_generator.command
✓ i output

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.

• • • org.cis_lvl1.audit.plist Edited	+ 🖉 🕞 Add Edit Value Duplicate	☐ XML ≎ Delete PLIST Format	↑↓ Q Sort Find Snippets
Кеу	Туре	~ Value	
∼ Root	Dictionary	88 items	
✓ audit_acls_files_configure	Dictionary	2 items	
exempt	Boolean	true	\$
exempt_reason	String	Enter a reason for disabling this rule	
v audit_acls_folders_configure	Dictionary	1 item	
exempt	Boolean	\$ false	\$
> audit_auditd_enabled	Dictionary	✿ 1 item	

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".

✓
∨ 🚞 audit_files_plists
org.cis_lvl1.audit.plist
✓
audit_files_profiles_generator.command
✓ i output
org.cis_lvl1.audit.mobileconfig
🛄 org.cis lvl1.audit.plist

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 Omnissa 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 titled "Custom configuration profile" included in each chapter titled "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.





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.

Thank you



MOM 5.24 • swiftDialog 2.5.1.4775 • Debug verbose logging enabled

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

Restart

mom-feedback APPLI 18 h 53

1

🐞 2024-08-18 18:53:07 CEST MacBook Pro C02Z15M9LVDG 25B28F80-9775-5E50-8A58-4694AD845927 mac415-macbook - Workflow of type onboarding from an opened user's session started

下 2024-08-18 18:53:58 CEST MacBook Pro C02Z15M9LVDG mac415-macbook - EULA agreed by ladmin (ladmin)

2024-08-18 18:57:28 CEST MacBook Pro C02Z15M9LVDG 25B28F80-9775-5E50-8A58-4694AD845927 mac174-macbook - Status message : 0 Management account password rotated successfully. Rotation date : 2024-08-18 18:57:28.

▲ Date : 2024-08-18 18:59:01 CEST Model Name : MacBook Pro Serial Number : C02Z15M9LVDG Computer Name : mac174-macbook Logged In Account : ladmin (ladmin) macOS Version : 14.6.1 mSCP Compliance Report :

- Baseline : CIS Benchmark Level 1
- Number of rules : 88
- Number of enabled rules : 87
- Number of disabled rules : 1
- Number of passed rules : 82
 Number of failed rules : 5
- Compliance score : 94.25% (warning)
- Non-compliant settings :

os_install_log_retention_configure

os_terminal_secure_keyboard_enable

os_unlock_active_user_session_disable

system_settings_remote_management_disable

system_settings_screen_sharing_disable

V 2024-08-18 18:59:02 CEST MacBook Pro C02Z15M9LVDG mac174-macbook - Workflow exited : Setup done

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".

MacOnboardingMate - Security code	
Please enter the security code.	
Cancel OK	

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).

	D: M D H		
	Discover MacOnboarding	gMate	
	This wizard is aimed to streamline the onboard management solution to give you the best exp	ling of this device in the organization's erience of its daily usage.	R
1	Please follow the instructions provided.		
	License	Completed <	
Computer Name Franck's MacBook Air	Execution probes	Completed <	
Serial Number FVFC24U6LYWK	Internet connectivity	Completed 🕢	
Operating System macOS 14.1	Access authorization	Completed 🗸	
	Enrollment planning	In progress	
	3 MDM enabled user	Location selector	
	Power management		
		This device must be registered in a location of a management solution defined by the organization.	
		Please select a location.	
		FileWave > Paris	(
DM 5.16 • swiftDialog 2.3.2	.4726 • Debug verbose logging enal	Cancel	Sele

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".

	Discover MacOnboard	lingMate
	This wizard is aimed to streamline the on management solution to give you the bes Please follow the instructions provided.	boarding of this device in the organization's t experience of its daily usage.
	License	MDM enabled user
Computer Name Franck's MacBook Air	Execution probes	The MDM enabled user is basically the logged in user during the enrollment and the only user on
Serial Number FVFC24U6LYWK	Internet connectivity	Configuration profiles afterwards.
Operating System	Access authorization	Do you agree that the user account Franck (franck) becomes the MDM enabled user ?
	Enrollment planning	No Yes
	MDM enabled user	In progress
	Power management	Pending
MOM 5.16 • swiftDialog 2.3.2.	4726 • Debug verbose logging enabled	Initialization

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".

	D End User License Agreement		Completed 🧹	English and the second
2	Migration configuration		Completed 🥑	Carllen Standard
	Device details collect		Completed 🥑	
	X Settings		In progress	A COMPANY
Computer Name Franck's MacBook Air	Post Settings script		Pending	
Serial Number FVFC24U6LYWK	Preflight script		Device	
Operating System macOS 14.1	MDM enrollment		Device	
	Find My Mac after enrollment		This device will b	e managed by FileWave and assigned to Paris location
	Anagement account	No.	Some customized	a settings must be defined manualiy.
	Yime Zone		Computer Name	e Franck's MacBook Air
			Tags	No value defined in the MDM yet.
	Boot volume name	Instructions Use comma as the 	Notes	No value defined in the MDM yet.
		separator between Tags.		
			Site	Paris
			Department	Information Technology

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

	Thank you
\$	Your device is now fully onboarded in the organization's management solution. Please visit the Self Service of FileWave to discover and install optional resources. XCreds was configured. The computer must be shut down.
Computer Name Franck's MacBook Air Serial Number FVFC24U6LYWK Operating System macOS 14.1	
014 5 40	Setup done

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. Bear in mind that MOM may take some time to appear, 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 Assistant steps can be automated or bypassed using "Auto Advance for Mac" (Power and 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.

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).



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.

	French
Microsoft	
Sign in	
Email, phone, or Skype	
No account? Create one!	
Can't access your account?	
Next	
ିର୍ବ୍ଦ Sign-in options	
Terms of use Privacy & cookies •••	
Jamf Connect Login, Expires: 20 August 2021	
🖒 Shutdown 🔞 Restart 🖵 Local Login 🗘 Refresh	Powered by Jamf 🎽

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 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 guickly 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.

en String Discover MacOnboardingMate fr String Découvrez MacOnboardingMate	✓ UIHELPER_MAIN_TITLE	Dictionary	٥	2 items
fr String String Découvrez MacOnboardingMate	en	String	٥	Discover MacOnboardingMate
	fr	String	٥	Découvrez MacOnboardingMate
VUHELPER_MAIN_TEXT Dictionary C 2 items	✓ UIHELPER_MAIN_TEXT	Dictionary	٥	2 items
en String 🗘 This wizard is aimed to streamline the onboarding of this device in the organization's management solution to give you the best experienc	en	String	٥	This wizard is aimed to streamline the onboarding of this device in the organization's management solution to give you the best experience
fr String 🗘 Cet assistant a pour but de rationaliser l'intégration de cet appareil dans la solution de gestion de l'organisation afin de vous offrir la meille	fr	String	٥	Cet assistant a pour but de rationaliser l'intégration de cet appareil dans la solution de gestion de l'organisation afin de vous offrir la meilleu

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 :

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	
✓	
launcher_template.plist	
launcher.plist	
Iocations_plists	
Jamf_Pro_Paris.plist	
location_1.plist	
VMware_Workspace_ONE.plist	
Iocations_profiles	
locations_profiles_generator.command	
✓ in output	
com.agnosys.config.Jamf_Pro.Paris.MOM.mobileconfig	
com.agnosys.config.VMware_Workspace_ONE.Paris.MOM.plist	
~ 🚞 mom_content	
🗸 🚞 binaries	
💝 dialog.pkg	
🗸 🚞 Content	
discomputer_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	
sh mom_content_postinstall.sh	
MOM-Content.pkgproj	
> 🚞 mom_library	
✓	
mom_rsa_engine.command	
mom_rsa_key.pri	
🔄 mom_rsa_key.pub	
(201). ·	

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 titled "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 titled "Custom configuration profile" included in each chapter titled "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

MacOnboardingMate - Migration
The migration from Meraki Systems Manager to FileWave must be executed before February 06, 2024 at 12:00 but you are given the option to postpone it until that date so that it can be triggered at an opportune time.
Please choose to migrate now or set a reminder.
10 minutes 2 minutes Now

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

	Discover MacOnboardingMate	MDM unenrollment
Hello Computer Name Franck's MacBook Air	Instructions The Remote Management Profile of this device is locked. The workflow will be paused until the unenrollment is done. Please follow the displayed instructions.	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.
Serial Number C02DW9Q7Q6L5	D End User License Agreement	Completed 📀
macOS 14.1.1	Migration configuration	Completed <
	Device details collect	Completed <
	X Settings	Completed 🕑
	Post Settings script	Completed 🕗
	Preflight script	Completed 📀
	MDM unenrollment	In progress
0M 5.16 • swiftDialog 2.3.2	Unenrolling from Meraki Systems Manager .4726 • Debug verbose logging enabled	Workflow

- 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"

	Discover MacOnboardingMate	MDM unenrollment	
Hello Computer Name Franck's MacBook Air	Instructions The Remote Management Profile of this device is locked. The workflow will be paused until the unenrollment is done. Please follow the displayed instructions.	After clicking the Continue button, a device enrollment notification is going to be displayed the upper right corner of the screen. Please click inside this notification and procee to the update of the management configuratio	
C02DW9Q7Q6L5	D End User License Agreement	Completed 📀	
macOS 14.1.1	Ø Migration configuration	Completed 🗸	
	Device details collect	Completed 🗸	
	X Settings	Completed 🥑	
	Post Settings script	Completed 🗸	
	Preflight script	Completed 🗸	
	MDM unenrollment	In progress 🔆	
	MDM enrollment	Pending 😳	
OM 5.16 • swiftDialog 2.3.2	Unenrolling from Meraki Systems Manager .4726 • Debug verbose logging enabled	Workflow	

- 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

11 00	Instructions		
Hell	○ ● ●	< > Profiles	
	Q Search	This Mac is supervised and managed by: Agnosys	
Computer Name	Franck Sartori		
Sorial Number	Apple ID	Device (Managed)	
C02DW9Q7Q6L		MCXToProfile: com.agnosys.config.MOM	
Operating Syste	WI-FI	Meraki Agent Settings for Paris	
macOS 14.1.1	Bluetooth	1 setting	
	Wetwork		
	Notifications		
	Sound		
	Focus	Update Device Enrolment?	?
	Screen Time	Update management configuration	
	General		
	Appearance		
	Accessibility		
	Control Centre		
	Siri & Spotlight		
	Privacy & Security		
10M 5.16 • swiftDia	Desktop & Dock		
	🔅 Displays		
	- Wallpaper		

- 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

	Diccorol macon scalanginato		MDM enrollment provisioning
Hello Computer Name	Instructions The MDM enrollment provisioning of this device must be m Please follow the displayed instructions.	naged by the IT Support.	Once IT support has confirmed that the device has been provisioned for enrollment with the ne MDM, click on Continue.
Franck's MacBook Air Serial Number C02DW9Q7Q6L5	D End User License Agreement	Completed 📀	
Operating System nacOS 14.1.1	🤣 Migration configuration	Completed <	
	Device details collect	Completed 🗸	
	X Settings	Completed 🥑	
	Post Settings script	Completed 🗸	
	Preflight script	Completed 🗸	
	MDM unenrollment	In progress	
	MDM enrollment	Pending 😁	
		Dan dian	
	Waiting for MDM enrollment provisioning	So alle	

- 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."

MDM enrollment provisioning			
	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.		
	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"

\mathbf{O}	
Remote Management	
This Mac is owned by:	
Agnosys	
Remote management is required and will allow this organization to set up email and network accounts, install and configure apps, and manage the settings of this Mac.	
Learn more about remote management	
Not now	Enroll

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.