MacOnboardingMate Dictionary : Launcher Configuration File
Version 6.06 — Updated on June 18, 2025

The following keys apply to both versions of MacOnboardingMate.

Key	Type	Example
LICENSE	String	MacOnboardingMate license key
The MacOnboardingMate license key.		
DEBUGMODE	String	disabled
Set to "debug" or "debugverbose" (exactly) to enable MOM logging in /var/log as soon as the key is read and to create the debug flag accordingly.		
The setting is ignored if the logging has been already enabled by the manual creation of a debug flag.		
DNSCHECKHOSTNAME	String	dns.google
The hostname to be tested with the "dig" command line tool to check Internet connectivity.		
SECURITYCODE	String	RSA-encrypted_security_code
MOM Essential : the passphrase used to protect the MOM-Core-Companion disk image from an unauthorized access.		
MOM Premium : the code to enter when MOM is executed from the session of a user account with administrative privileges.		
RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.		
MDMENABLEDUSERVALIDATION	Boolean	true
Set to "true" to be asked to validate that MOM is executed from the session of the targeted MDM enabled user.		
The option should be set to "true" in 1:1 deployments and to "false" in Shared devices deployments.		
UIHELPER	String	swiftdialog
To enable an improved interface, set to "swiftdialog" (preferred) or "depnotify". To enable the legacy interface, set to "applescript".		
As swiftDialog requires macOS 11 or later, a fallback to DEPNotify is automatically triggered when macOS 10.15 or earlier is detected.		
UIHELPER_PICTURE	String	welcome.png
The picture to be displayed in the welcome pane (.png file expected).		
UIHELPER_MAIN_TITLE	String	Welcome To ACME !
The title to be displayed in the welcome pane.		
UIHELPER_MAIN_TEXT	String	This wizard is aimed to streamline the onboarding of this device in the organization's management solution to give you the best experience of its daily usage.\r\rPlease follow the instructions provided.
The text to be displayed in the welcome pane.		
Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).		
DEPNOTIFY_URL	String	https://files.nomad.menu/DEPNotify.pkg
The URL used to download the DEPNotify package (DEPNotify*.pkg file expected).		
SWIFTDIALOG_URL	String	https://github.com/swiftDialog/swiftDialog/releases/download/v2.5.6/dialog-2.5.6-4805.pkg
The URL used to download the swiftDialog package (dialog*.pkg file expected).		
When macOS 11 is detected, the URL is forcibly set to https://github.com/swiftDialog/swiftDialog/releases/download/v2.2.1/dialog-2.2.1-4591.pkg as version 2.2.1 is the newest version compatible.		
When macOS 12 is detected, the URL is forcibly set to https://github.com/swiftDialog/swiftDialog/releases/download/v2.4.2/dialog-2.4.2-4755.pkg as version 2.4.2 is the newest version recommended.		
LOCATIONS > LIST	Array	Jamf School Paris,location_1.plist

List of the locations (destination points) of enrolled devices in their management solution.
These locations are displayed in the Location Selector when two or more locations are configured.
Add one array item per location in the form of Location name,Property List filename.

LOCATIONS > DEFAULT_LOCATION	Integer	0

swiftDialog and AppleScript interfaces only : the location selected by default in the Location Selector when displayed.
The value must be the number of the item in the LIST array (starting with "0").

MacOnboardingMate Dictionary : Location Configuration File

The following keys apply to both versions of MacOnboardingMate.

Key	Context	Launcher	AutoLauncher	Type	Example
LICENSE	Licensing	N/A	Supported	String	MacOnboardingMate license key
The MacOnboardingMate license key.					
DEBUGMODE	Debug	N/A	Supported	String	disabled
Set to "debug" or "debugverbose" (exactly) to enable MOM logging in /var/log as soon as the key is read and to create the debug flag accordingly.					
The setting is ignored if the logging has been already enabled by the manual creation of a debug flag.					
DNSCHECKHOSTNAME	Enrollment	N/A	Supported	String	dns.google
The hostname to be tested with the "dig" command line tool to check Internet connectivity.					
POWER_MANAGEMENT	Enrollment	Supported	Supported	String	battery:75%
By default, the workflow execution requires the device to be connected to AC Power.					
Add "battery" (only) to allow the workflow to be executed while the device is on Battery Power.					
Add "battery:[0-100]%" to require that the device is connected to AC Power if the battery charge is less than the percentage specified.					
MDMSOLUTION	Enrollment	Supported	Supported	String	Jamf Pro
The management solution in which the device enrolls : "FileWave", "Hexnode UEM", "Jamf Now", "Jamf Pro", "Jamf School", "JumpCloud", "Kandji", "ManageEngine MDM", "Meraki Systems Manager", "Microsoft Intune", "Miradore", "Mosyle Business", "Mosyle Manager", "Omnissa Workspace ONE", "SimpleMDM" (exact name from this list with case-sensitivity respected).					
This string is recorded in the location file saved as /Library/Application Support/MOM/location.plist					
MDMLOCATION	Enrollment	Supported	Supported	String	Paris
The name of the location (destination point) of the device once enrolled in the management solution.					
For clarity, the name of the location is supposed to be the same as the one used in the setup.plist file (see LOCATIONS > LIST).					
Meraki Systems Manager : the name of the location must be the exact name of a Network defined inside the Organization for the API calls to be functional.					
This string is recorded in the location file saved as /Library/Application Support/MOM/location.plist					
AUTOMATED_DEVICE_ENROLLMENT	Enrollment	Supported	Supported	Boolean	false
Set to "true" to attempt to enroll the device using Automated Device Enrollment.					
AUTOMATED_DEVICE_ENROLLMENT_REQUIRED	Enrollment	Supported	Supported	Boolean	false
Set to "true" to enforce the use of Automated Device Enrollment. Should Automated Device Enrollment fail, the only option is to retry.					
Set to "false" to enable fallback from Automated Device Enrollment to Account-Driven Enrollment or Device Enrollment if Automated Device Enrollment fails.					
ACCOUNT_DRIVEN_ENROLLMENT	Enrollment	Supported	Supported	Boolean	false
Set to "true" to enroll the device using Account-Driven Enrollment.					
Account-Driven Enrollment can be Account-Driven Device Enrollment or Account-Driven User Enrollment, depending on the MDM configuration.					
The key will be ignored if the device is not installed with macOS 14 and later.					
When Account-Driven Enrollment is enabled, other Device Enrollment methods are ignored.					
ENROLLMENT_PROFILE	Enrollment	Supported	Supported	String	profile_jc.mobileconfig
The name of the Enrollment profile to enroll the device using Device Enrollment (.mobileconfig file expected).					
This setting only applies to JumpCloud.					
JumpCloud : Device Management > MDM > MDM Configuration > download profile					
ENROLLMENT_URL	Enrollment	Supported	Supported	String	https://hostname.jamfcloud.com/enroll

The URL for downloading the Enrollment profile to enroll the device using Device Enrollment.

This URL should ideally point to the location targeted.

FileWave : FileWave Admin > Assistants > Enroll iOS Device > Manual Enrollment > Enrollment URL > https://hostname.filewave.net:20443/ios

Hexnode UEM : Enroll > Platform-Specific > macOS > Email or SMS > Open Enrollment > Enrollment URL > https://hostname.hexnodemdm.com/enroll

Jamf Now : Blueprints > Name of Blueprint (square) > Name of Blueprint (upper left) > Enrollment > Permanent Link

Jamf Pro : https://hostname.jamfcloud.com/enroll

Jamf School : School > Location > Devices > Enroll Device(s) > On-device enrollment (iOS & macOS) > URL + Network ID + Location Code

JumpCloud : use "undefined" as the enrollment is performed by a profile (see ENROLLMENT_PROFILE)

Kandji : https://hostname.kandji.io/enroll

Meraki Systems Manager : Organization > Network > Systems Manager > Monitor > Devices > Add devices > macOS > https://m.meraki.com/?enrollment_code=Network_ID

Miradore : https://online.miradore.com/enrollnow

Microsoft Intune : use "undefined" as the URL is defined automatically by Microsoft Company Portal

Mosyle Business : Management > Device Groups > Targeted group > Enrollment URL (alternative : generic enrollment URL for your instance)

Mosyle Manager : My School > Enrollment > Manual enroll via Safari (URL) > Enrollment URL

Omnissa Workspace ONE : https://hostname.awmdm.com/enroll ; use "undefined" to manage the enrollment from Intelligent Hub

Simple MDM : Account > Devices > Enrollments > Targeted group > Enrollment Link

APIURL		Extra informations	Supported	Supported	String	https://hostname.jamfcloud.com

The URL to make API calls with the management solution.

FileWave : https://hostname.filewave.net (API v1 and v2 usage)

Hexnode UEM : https://hostname.hexnodemdm.com/api

Jamf Pro : https://hostname.jamfcloud.com (Classic API and Jamf Pro API usage)

Jamf School : https://hostname.jamfcloud.com/api

JumpCloud : https://console.jumpcloud.com/api

Kandji : https://hostname.api.kandji.io (US) or https://hostname.api.eu.kandji.io (EU) ; refer to https://support.kandji.io/api

Meraki Systems Manager : https://api.meraki.com/api/v1

Microsoft Intune : https://graph.microsoft.com/Beta (API 1.0 is not supported)

Miradore : https://online.miradore.com/sitename (API v1 and v2 usage)

Mosyle Business : https://businessapi.mosyle.com/v1

Mosyle Manager : https://managerapi.mosyle.com/v2

Omnissa Workspace ONE : Groups & Settings > All Settings > System > Advanced > API > Rest API — General > REST API URL : https://asX.awmdm.com/api

SimpleMDM : https://a.simplemdm.com/api/v1

APIAUTHENTICATIONSTRING		Extra informations	Supported	Supported	String	RSA-encrypted_authentication_string

The string to be used to authenticate API calls with the management solution.

FileWave : FileWave Admin > Assistants > Manage Administrators > + Local Account > User details : Login Name - Set password / Permissions / Application tokens : Token (base64)

Hexnode UEM : Admin > API > Configure API > Enable > padlock

Jamf Pro (API Roles and Clients) : concatenation of those 2 values separated with a colon : Client ID:Client Secret (refer to the Integration Guide for the details)

Jamf Pro (User account) : concatenation of those 2 values separated with a colon : apisvcaccount:apisvcaccountpassword

Jamf School : Network ID:API Key (School > Devices > Enroll Device(s) > On-device enrollment > Network ID / School > Organisation > Settings > API > Add API Key > Name + Key > Apply)

JumpCloud : API Key (Account > API Settings)

Kandji : API Token ; refer to https://support.kandji.io/api

Meraki Systems Manager : Organization > Configure > Settings > Dashboard API access > Enable access to the Cisco Meraki Dashboard API + Account > My Profile > API access > Generate new API key

Microsoft Intune : concatenation of those 3 values separated with commas : tenant_domain,application_(client)_id,client_secret_value

Miradore : API key (Infrastructure diagram > API > Create key > Name > API key > Create key)

Mosyle Business : concatenation of those 3 values separated with commas : apisvcaccountemail,apisvcaccountpassword,accesstoken

- API Service Account : Organization > Administrators > Add Administrator > Name / User ID / Email / Send welcome e-mail : unchecked / Password / Account type : Administrator > Save

- Access Token : Organization > Integrations > Mosyle API Integration > Add new token > Profile name / Access Method : Public / Allowed Endpoint : Devices > Save > Access Token

Mosyle Manager : concatenation of those 3 values separated with commas : apisvcaccountemail,apisvcaccountpassword,accesstoken

- API Service Account : MySchool > Administrators > Add new administrator > Name / User ID / Email / Send welcome e-mail : unchecked > Save > Edit > Password / Account type : Leader > Save

- Access Token : MySchool > Integrations > Mosyle API Integration > Enable API Integration > Access Token

Omnissa Workspace ONE (OAuth2 authentication) : concatenation of those 3 values separated with commas : Token URL,Client ID,Client Secret

- Token URL : refer to https://docs.omnissa.com/bundle/WorkspaceONE-UEM-Console-BasicsVSaaS/page/UsingUEMFunctionalityWithRESTAPI.html

- Groups & Settings > Configurations > OAuth Client Management > Name, Description, Organization Group, Role : Console Administrator / Custom Role, Status : Enabled > Client ID, Client Secret

Omnissa Workspace ONE (Basic authentication) : concatenation of those 3 values separated with commas : username,password,API Key

- Accounts > Administrators > List View > Username — Roles > Organization Group : Console Administrator / Custom Role — API > Authentication : User Credentials

- Groups & Settings > All Settings > System > Advanced > API > Rest API — General > Enable API Access : Enabled / Service : AirWatchAPI | Account Type : Admin | API Key — Authentication > Basic : Enabled

SimpleMDM : API Key (Account > API > Add API Key > name > Save > Secret Access Key > reveal)

RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.

JSON_PARSER		Extra informations	Supported	Supported	String	plutil

To enable JSON parsing with plutil, set the key to "plutil" (preferred method).

To enable JSON parsing with JavaScript, set the key to "javascript".

To enable JSON parsing with jq, set the key to "jq". When jq cannot be installed correctly, plutil is used as the fallback.

When macOS 11 and earlier is detected, JavaScript is used as the fallback of plutil.

When Jamf Pro API is enabled, API calls are forcibly made using plutil (macOS 12 and later), JavaScript (macOS 10.15 and macOS 11) and jpt (https://github.com/brunerd/jpt).

JQ_URL		Extra informations	Supported	Supported	String	https://github.com/jqlang/jq/releases/download/jq-1.7.1/jq-macos-arm64

Since MOM 4.24, JSON parsing with JQ is deprecated but is still supported.

When jq is enabled, set the key to this download URL : https://github.com/jqlang/jq/releases/download/jq-1.7.1/jq-macos-arm64

The URL for the arm64 or the x86_64 architecture is automatically derived from any given URL.

NETWORKQUALITY		Installation	Supported	Supported	Boolean	true

Set to "true" to initiate a download speed check at intervals of no less than 5 minutes, with the results shown under the device details.

PROMOTION_ALLOWED		Configuration	Supported	Supported	Boolean	true

Set to "true" to grant a standard user the administrative privileges required by macOS for the MDM enrollment using Device Enrollment, or the SecureToken grant to the management account.

During MDM enrollment, the grant occurs after the display of the enrollment Web page or the opening of the enrollment application, until the enrollment is done.

Once the targeted action is done, the granted administrative privileges are revoked.

In the context of Automated Device Enrollment with macOS 14 and earlier, the elevation of privileges is forced regardless of this setting so that macOS can display the mandatory enrollment notification :

- with macOS 14, the grant occurs just before the display of the enrollment pane, until the enrollment is done

- from macOS 11 to macOS 13 : the grant occurs just before the display of the enrollment notification, until the enrollment is done

- with macOS 10.15 and earlier : the grant occurs only at the time the enrollment notification is displayed.

Automated Device Enrollment with macOS 15 and later allows standard users to enroll their device, so no elevation of privileges is triggered.

Key					
PROVISIONING	Configuration	N/A	Supported	Dictionary	OVER_SETUP_ASSISTANT — Dictionary -- -- ATTEMPT — Boolean — true -- -- FOCUS — Boolean — false -- -- WAIT_LOCAL_ACCOUNT_CREATION — Boolean — false OVER_LOGIN_WINDOW — Dictionary -- -- ATTEMPT — Boolean — true -- -- FOCUS — Boolean — false OVER_DESKTOP — Dictionary -- -- FOCUS — Boolean — false

Configuration of the provisioning experience in the context of Automated Device Enrollment.

OVER_SETUP_ASSISTANT
- 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.
This feature is only supported when the UI Helper is swiftDialog.
OVER_LOGIN_WINDOW
- 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
This feature is only supported when the UI Helper is swiftDialog.
OVER_DESKTOP
- FOCUS : set to "true" to blur the background while MOM is running during onboarding over the Desktop
This feature is only supported when the UI Helper is DEPNotify.
Capacities forcibly disabled when the onboarding occurs over the Setup Assistant or over the Login Window
Interactive tasks : FileVault enablement (MGTACCOUNTFILEVAULT), SecureToken granting (MGTACCOUNTSECURETOKEN), Inventory source (MIGRATION_CHOOSE_INVENTORY_SOURCE), Privacy Control (PRIVACY_CONTROL), Kerberos SSO Extension Integration (KERBEROS_SSO_EXTENSION_INTEGRATION).
Fallbacks
• When onboarding over the Setup Assistant is attempted while the Mac is no longer in Setup Assistant, the fallback is onboarding over the Login Window if this option is enabled. Otherwise, onboarding over the Desktop of the first logged-in user will be enabled.
• When onboarding over the Login Window is attempted while the Mac is no longer in Login Window, onboarding over the Desktop of the first logged-in user will be enabled.

Key					
MGTACCOUNT	Configuration	Supported	Supported	String	ladmin

The management account name.
The setting only applies if the management account is detected as missing when MOM is executed.

MGTACCOUNTFULLNAME	Configuration	Supported	Supported	String	Local Administrator

The management account full name.

MGTACCOUNTUID	Configuration	Supported	Supported	Integer	600

The management account UID.

MGTACCOUNTSHELL	Configuration	Supported	Supported	String	/bin/zsh

The management account Shell.

MGTACCOUNTHOME	Configuration	Supported	Supported	String	/Users/ladmin

The management account home folder.

MGTACCOUNTPASSWORD	Configuration	Supported	Supported	String	RSA-encrypted_mgt_account_password

The management account password.
RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.

MGTACCOUNTPICTURE	Configuration	Supported	Supported	String	mgtaccount_picture.png

The management account picture (.png file expected).

MGTACCOUNTHIDDEN	Configuration	Supported	Supported	Boolean	false

Set to "true" to hide the management account.

MGTACCOUNTFILEVAULT	Configuration	Supported	Supported	String	required

This key only applies to devices configured with FileVault enabled. Set to "required" to add the management account to the list of users allowed to unlock the device. Set to "optional" for the same action but with the possibility to skip it when a password must be entered interactively. The methods used are in this order : - Automated enablement with credentials escrowed during SecureToken granting - Interactive enablement with credentials entered by a user (who holds a SecureToken with APFS Boot Volume). Set to "disabled" to remove the management account from the list of users allowed to unlock the device. Set to "undefined" to ignore the key.					
MGTACCOUNTSECURETOKEN	Configuration	Supported	Supported	String	required
Set to "required" to prompt a user who holds a SecureToken and whose password must be entered interactively to grant a SecureToken to the management account. Set to "optional" for the same action but with the possibility to skip it. Set to "undefined" to ignore the key.					
AWAITED_ITEMS	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary
List of items awaited before the workflow can proceed. WAITING : Set to "true" to wait for the listed items DISPLAY : Set to "compact" to display the wait for all awaited items as a single stage in the stages list, or set to "expanded" to display each awaited item as a separate stage in the stages list LIST : Add one array item for each awaited item Item > TYPE : Set to "app", "CFBundleIdentifier", "path" or "Wi-Fi" For an item of type "app", "CFBundleIdentifier" or "path" : - ITEM : the app name, the bundle name or the full pathname (no space escaping required) - NAME : the name displayed in the stages list for this item - TIMEOUT : the maximum wait time in seconds before waiting is interrupted - ICON : the icon displayed for the item when the "expanded" display is enabled (.png file expected) ; if the icon is not available, a default app icon or hourglass icon is displayed For an item of type "Wi-Fi" : - SSID : the SSID that the workflow is waiting for the device to connect to - SECURITY : the security protocol configured for this SSID ; the supported values are "WPA" (WPA Personal), "WPAE" (WPA Enterprise), "WPA2" (WPA2 or WPA3 Personal) and "WPA2E" (WPA2 or WPA3 Enterprise) - NAME : the name displayed in the stages list for this SSID - TIMEOUT : the maximum wait time in seconds before waiting is interrupted - ICON : the icon displayed for the item when the "expanded" display is enabled (.png file expected) ; if the icon is not available, a default Wi-Fi icon is displayed The "expanded" display is only supported when the UI Helper is swiftDialog. The timeout is calculated from the time when the awaited items step is triggered.					
BOOTVOLUMENAME	Configuration	Supported	Supported	String	Macintosh HD
The name of the Boot Volume.					
COMPUTERNAME_CONFIG_LAUNCHER	Configuration	Supported	N/A	String	prompt
Pick a renaming method in this list : "prompt", "template", "csv". prompt : computer name entered manually in the Computer name field of the Settings pane. template : computer name derived from a template (see COMPUTERNAMETEMPLATE). csv : computer name retrieved from a CSV file (see COMPUTERNAMECSV).					
COMPUTERNAME_CONFIG_AUTOLAUNCHER	Configuration	N/A	Supported	String	template
Pick a renaming method in this list : "prompt", "template", "csv". prompt : computer name entered manually in the Computer name field of the Settings pane. template : computer name derived from a template (see COMPUTERNAMETEMPLATE). csv : computer name retrieved from a CSV file (see COMPUTERNAMECSV).					
COMPUTERNAME_CSV	Configuration	Supported	Supported	String	computernames.csv
The CSV file that dictates the computer name (*.csv file expected). A template for the CSV file is available : MOM-Toolkit > mom_library > computernames.csv					
COMPUTERNAME_TEMPLATE	Configuration	Supported	Supported	String	MAC:Random[digits:3][padding:true]:-:ModelName:-:SerialNumber:

The template that dictates the computer name.

:ModelName: is a variable substituted by the Model Name visible in System Information > Hardware > Model Name.

:Random[digits:*n*][padding:true|false]: is a variable substituted by a number composed of a maximum of *n* digits ; when padding is set to "true", this number is preceded by zeros to have a length of *n* characters.

:SerialNumber: is a variable substituted by the Serial Number visible in System Information > Hardware > Serial Number.

:SerialNumber[length:*n*][truncate:start|end]: limits the Serial Number to *n* characters, any extra characters being removed at the start or at the end.

COMPUTERNAME_CASE	Configuration	Supported	Supported	String	lower

Set to "lower" to enforce lower case characters.
Set to "upper" to enforce upper case characters.

COMPUTERNAME_CHARACTERS_ALLOWED	Configuration	Supported	Supported	String	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 .-_'

List of characters allowed in the Computer name field of the Settings pane when DEPNotify is used.
The character comma is forcibly disallowed.

COMPUTERNAME_MAX_LENGTH	Configuration	Supported	Supported	Integer	15

Set to the maximum number of characters authorized for a computer name (computer name shortened from the beginning to this number of characters).
Set to "0" to ignore the policy.

CONFIGURATIONPROFILESCRIPTS	Configuration	Supported	Supported	Boolean	true

Set to "true" to authorize the execution of loginhook and/or logouthook scripts embedded in the Login Window payload of a Configuration profile.

DOCKUTIL_INSTALL	Installation	Supported	Supported	String	enabled

Set to "enabled" to install the Dockutil Tool used by Agnosys Login script to configure the Dock (see SCRIPTS > LOGINUSERSCRIPT).

DOCKUTIL_URL	Installation	Supported	Supported	String	https://github.com/kcrawford/dockutil/releases/download/3.1.3/dockutil-3.1.3.pkg

The URL used to download the Dockutil Tool for macOS 11 and later (dockutil*.pkg file expected).

DOCKUTIL_URL_V2	Installation	Supported	Supported	String	https://github.com/kcrawford/dockutil/releases/download/2.0.5/dockutil-2.0.5.pkg

The URL used to download the Dockutil version 2 for macOS 10.15 and earlier (dockutil*.pkg file expected).

EXIT_ACTION	Configuration	Supported	Supported	Dictionary	COMMAND — String — undefined
					COMMAND_DELAY — Integer — 60
					APP_PATH — String — /Applications/Managed Software Center.app
					WEB_URL — String — https://www.agnosys.com
					BUTTON_LABEL — String — Open Managed Software Center

Set the COMMAND key to a supported command from this list (exactly) :
- logout : triggers a log out and the display of the login window
- restart : triggers a restart
- restart_delete_local_accounts_except_management_account : triggers a restart followed by the irreversible deletion of all local accounts except the management account (mobile accounts are preserved) ; this command is executed via the MOM Privileged Helper on macOS 12 and later (see the Integration Guide for implementation details) ; this command is reverted to "restart" if FileVault is enabled or if the management account does not exist or if the management account does not have a SecureToken (APFS Boot Volume only) or if the management account password is not the one defined by the MGTACCOUNTPASSWORD key (APFS Boot Volume only)
- shutdown : triggers a shut down.
- undefined : no specific action is triggered after MOM is closed.
Provisioning over the Setup Assistant : "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 : "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".
Provisioning over the Desktop : "logout", any "restart", "shutdown" and "undefined" are supported ; when Jamf Connect or NoMAD Login AD or XCreds is configured by the workflow, "undefined" is automatically converted to "logout".
When EXIT_ACTION is eventually set to "logout", any "restart" or "shutdown", the COMMAND_DELAY key defines the time in seconds after which the action is automatically triggered once the Landing pane is displayed (set to "0" to disable the automation).
The following three keys are only used during Provisioning over the Desktop when the COMMAND key is set to "undefined" :
- APP_PATH : Full path to the app that must be opened once the Landing pane is closed
- WEB_URL : Web URL to a Web page opened in the logged-in user's default Web browser once the Landing pane is closed
- BUTTON_LABEL : customized text displayed in the button instead of the default text "Quit" ; this text should indicate the app and/or the Web page that is/are going to be opened.

FIND_MY_MAC_DISABLED_BEFORE_ENROLLMENT	Enrollment	Supported	Supported	String	required-ActivationLockEnabled

Set to "required" to wait for the disablement of "Find My Mac" before the device is enrolled (regardless Activation Lock status).

Set to "required-ActivationLockEnabled" to wait for the disablement of "Find My Mac" before the device is enrolled if an Activation Lock is enabled (Apple silicon or an Apple T2 Security Chip required).

This action involves that the Personal Apple ID used to enable "Find My Mac" is configured in the logged-in user's session otherwise the workflow is prevented to be run.

Set to "undefined" to ignore the key.

FIND_MY_MAC_ENABLED_AFTER_ENROLLMENT	Enrollment	Supported	Supported	String	optional

Set to "required" to wait for the enablement of "Find My Mac" after the device is enrolled.

Set to "optional" to offer the enablement of "Find My Mac" after the device is enrolled.

This action involves that "Find My Mac" is enabled with the Personal Apple ID configured in the logged-in user's session.

In the context of a device equipped with an Apple silicon or an Apple T2 Security Chip, refer to the MDM documentation to learn how to reveal the Activation Lock Bypass Code the MDM should escrow at enrollment and the steps required to allow the enablement of an Activation Lock afterwards.

Set to "undefined" to ignore the key.

FIRMWAREPASSWORD	Configuration	Supported	Supported	String	RSA-encrypted_firmware_password

The string to use as the firmware password.

This setting only applies if the host is an Intel Mac (no Virtual Machine, no Apple silicon Mac).

RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.

Set to "undefined" to ignore the firmware password configuration.

PRIVACY_CONTROL	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

List of privacy settings that must be enabled by the user before the workflow can proceed.

This feature ensures that the user enables the settings but does not automatically add an item to the Privacy & Security pane.

ACTIVATION : Set to "true" to enable this feature

PANEPOSITIONANCHOR : Set to "topleft", "left", "bottomleft", "top", "center", "centre", "bottom", "topright", "right", or "bottomright" to anchor the displayed pane at a specific position, overriding the default centered anchor.

PANEPOSITIONOFFSET : Set to an integer that adjusts the pane's position slightly towards the center, relative to its anchor point.

PRIVACYSETTINGSOPENING : Set to "auto" to open the Privacy & Security pane automatically, or to "manual" to open it only after the "Next" button in the displayed pane is clicked.

LIST : Add one array item for each privacy setting, defined by the following keys :

- TYPE : Set to "CFBundleIdentifier"

- ITEM : The bundle name

- SERVICE : Set to "kTCCServiceScreenCapture" (open a support ticket for any additional privacy services required)

- REQUIRED : Set to "true" to ensure that granting cannot be skipped

- NAME : The name of the app expected to be associated with the privacy setting (or any other relevant text)

- ICON : The icon displayed for the privacy setting (.png file expected) ; if the icon is not available, a default padlock icon is displayed

- PICTURE : The picture displayed to show the expected outcome (or any other relevant image) ; if the picture is not available, a default padlock icon is displayed

- TEXT : The instructions displayed under the picture (or any other relevant text)

This feature is only supported when the UI Helper is swiftDialog.

This feature depends on the MOM Privileged Helper (see the Integration Guide for implementation details).

PYTHON_INSTALL	Installation	Supported	Supported	String	enabled

Set to "enabled" to install Python 3 Recommended that contains the Docklib Tool.

PYTHON_URL	Installation	Supported	Supported	String	https://github.com/macadmins/python/releases/download/ v3.12.1.80742/python_recommended_signed-3.12.1.80742.pkg

The URL used to download Python 3 Recommended (python_recommended_signed*.pkg file expected).

REMOTEMANAGEMENT	Configuration	Supported	Supported	Boolean	true

Set to "true" to enable the Remote Management service and allow access for the management account with all privileges.

This capability is only supported with Jamf Pro and SimpleMDM that offer to send an Enable Remote Desktop MDM command performed by an API call before the service is configured.

With other MDM, the service is configured but not enabled and an Enable Remote Desktop MDM command received afterwards will cancel the configuration.

ROSETTA_INSTALL	Installation	Supported	Supported	Boolean	true

Set to "true" to install Rosetta 2.

This setting only applies if the host is an Apple silicon Mac (macOS 11 and later) and Rosetta 2 is not already installed.

LOGINUSERSCRIPT (inside SCRIPTS Dictionary)	Configuration	Supported	Supported	Dictionary	LOGINUSERSCRIPT — Dictionary -- FILENAME — String — login_user.sh

FILENAME : the name of the script that is executed when a user logs in (i.e. Desktop Picture and Dock configurations)

A template for the Login User script is available : MOM-Toolkit > mom_library > login_user.sh

PREFLIGHTSCRIPT **(inside SCRIPTS Dictionary)**	Configuration	Supported	Supported	Dictionary	PREFLIGHTSCRIPT — Dictionary -- FILENAME — String — preflight.sh -- PARAMETERS — String — -a 10 -- PREFER_PRIVILEGED_HELPER — Boolean — false -- TIMEOUT — Integer — 60 -- ICON — String — preflight_icon.png -- STEPS — Integer — 3

FILENAME : the name of the Preflight script that is run at the beginning of the workflow ; set to "undefined" to ignore the script

PARAMETERS : the parameters (options and arguments) passed to the script upon execution

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

TIMEOUT : the maximum wait time in seconds before waiting is interrupted

ICON : the icon which is displayed for the script in the stages list

STEPS : number of steps planned in the Preflight script

A template for the Preflight script is available : MOM-Toolkit > mom_library > placeholder.sh

To ensure that the progress bar reflects accurately the workflow, the value must match the exact number of times the command "uihelper progress_forward" is used in the script.

When the script terminates with a zero exit code, the Flight Recorder reports the string that the script sends to standard output, which is enclosed within tags of any name, following the structure <tag>string</tag> (i.e. <result>Printer management privileges granted</result>).

When the script terminates with a non-zero exit code, the Flight Recorder reports the exit code.

When the script terminates due to a timeout, the Flight Recorder reports the message "Timeout exceeded".

POSTSETTINGSSCRIPT **(inside SCRIPTS Dictionary)**	Configuration	Supported	Supported	Dictionary	POSTSETTINGSSCRIPT — Dictionary -- FILENAME — String — post_settings.sh -- PARAMETERS — String — -b 20 -- PREFER_PRIVILEGED_HELPER — Boolean — false -- TIMEOUT — Integer — 60 -- ICON — String — post_settings_icon.png -- STEPS — Integer — 3

FILENAME : the name of the Post Settings script that is run after the device customization pane is closed ; set to "undefined" to ignore the script

PARAMETERS : the parameters (options and arguments) passed to the script upon execution

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

TIMEOUT : the maximum wait time in seconds before waiting is interrupted

ICON : the icon which is displayed for the script in the stages list

STEPS : number of steps planned in the Post Settings script

A template for the Postflight script is available : MOM-Toolkit > mom_library > placeholder.sh

To ensure that the progress bar reflects accurately the workflow, the value must match the exact number of times the command "uihelper progress_forward" is used in the script.

When the script terminates with a zero exit code, the Flight Recorder reports the string that the script sends to standard output, which is enclosed within tags of any name, following the structure <tag>string</tag> (i.e. <result>Printer management privileges granted</result>).

When the script terminates with a non-zero exit code, the Flight Recorder reports the exit code.

When the script terminates due to a timeout, the Flight Recorder reports the message "Timeout exceeded".

POSTFLIGHTSCRIPT **(inside SCRIPTS Dictionary)**	Configuration	Supported	Supported	Dictionary	POSTFLIGHTSCRIPT — Dictionary -- FILENAME — String — postflight.sh -- PARAMETERS — String — -c 30 -- PREFER_PRIVILEGED_HELPER — Boolean — false -- TIMEOUT — Integer — 60 -- ICON — String — postflight_icon.png -- STEPS — Integer — 3

FILENAME : the name of the Postflight script that is run at the end of the workflow ; set to "undefined" to ignore the script
PARAMETERS : the parameters (options and arguments) passed to the script upon execution
PREFER_PRIVILEGED_HELPER : set to "true" to delegate the execution of the script to the MOM Privileged Helper
TIMEOUT : the maximum wait time in seconds before waiting is interrupted
ICON : the icon which is displayed for the script in the stages list
STEPS : number of steps planned in the Postflight script.
A template for the Postflight script is available : MOM-Toolkit > mom_library > placeholder.sh
To ensure that the progress bar reflects accurately the workflow, the value must match the exact number of times the command "uihelper progress_forward" is used in the script.
When the script terminates with a zero exit code, the Flight Recorder reports the string that the script sends to standard output, which is enclosed within tags of any name, following the structure <tag>string</tag> (i.e. <result>Printer management privileges granted</result>).
When the script terminates with a non-zero exit code, the Flight Recorder reports the exit code.
When the script terminates due to a timeout, the Flight Recorder reports the message "Timeout exceeded".

SETDESKTOPSPY_INSTALL	Installation	Supported	Supported	String	enabled
Set to "true" to install the script used by Agnosys Login script to configure the Desktop Picture on a device installed with macOS 10.4.3 and earlier (see SCRIPTS > LOGINUSERSCRIPT).					
SETDESKTOPSPY_URL	Installation	Supported	Supported	String	https://raw.githubusercontent.com/grahamgilbert/macscripts/master/set_desktops/set_desktops.py
The URL used to download the set_desktops.py script (set_desktops.py file expected).					
SETTINGS_PANE (part 1/5) **Base configuration**	Extra informations	Supported	Supported	Dictionary	DISPLAY — Boolean — true CHARACTERS_ALLOWED — String — abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 .-_'
DISPLAY : set to "true" to enable the display of the text field(s) and/or the menus in the Settings pane CHARACTERS_ALLOWED : list of the characters allowed in the text field(s) (DEPNotify only) With Meraki Systems Manager, Mosyle Business and Mosyle Manager, the symbol comma is automatically added to this list when the "Tags" attribute is enabled.					
SETTINGS_PANE (part 2/5) **Declaring Text fields**	Extra informations	Supported	Supported	Dictionary	LIST — Array -- Item 0 — Dictionary -- -- ATTRIBUTE — String — Asset Tag -- -- TYPE — String — textfield -- -- REGEX — String — ^\d{6}$ -- -- REGEX_ERROR — String — Asset Tag must be a six-digit number. -- -- REQUIRED — Boolean — true

List of the text fields displayed in the Settings pane.
ATTRIBUTE :
- FileWave : enter "Building", "Comment", "Department", "Enrollment Username", "Location" or a Custom Field name ; the Custom Field will be created if missing
- Hexnode UEM : enter "Asset Tag", "Department", "Description" or "Notes" ; known limitation : all attributes are writable but only the "Description" value can be retrieved to pre-fill the text field
- Jamf Pro : enter "Asset Tag", "Building", "Department", "Room", "Site", "Username" or an Extension Attribute name ; the Extension Attribute will be created if missing
- Jamf School : "Asset Tag" or "Notes"
- JumpCloud : enter "Description"
- Meraki Systems Manager : enter "Tags" or "Notes"
- Microsoft Intune : enter "Notes"
- Miradore : enter "Category", "Location", "Organization", "Tags", "Email", "FullName[FML]" or a Custom Attribute name ; the Custom Attribute will be created if missing ; the letters FML, for First name, Middle initial and Last Name, define the strings separated with spaces that must be interpreted, and in what order, to build the full name read from an MDM or written to Miradore
- Mosyle Business : enter "Asset Tag" or "Tags"
- Mosyle Manager : enter "Asset Tag" or "Tags"
- Omnissa Workspace ONE : enter "Asset Number" or "Notes" or a Custom Attribute name ; the Custom Attribute will be created if missing
- SimpleMDM : enter a Custom Attribute name ; spaces and hyphens in the name are converted to underscores ; the Custom Attribute will be created if missing
TYPE : set to "textfield"
REGEX : set the regular expression used to validate the input
REGEX_ERROR : set the message to display when the input fails validation
REQUIRED : set to "true" to make filling out the field mandatory
About regular expressions :
- testing can be conducted using https://regex101.com
- example : ^\d{6}$ validates a six-digit number (exactly)
- example : ^[\w\.-]+@([\w-]+\.)+[\w]{2,4}$ validates an email address (e.g., user@example.com).
Notes :
- with DEPNotify and Jamf School, Meraki Systems Manager, Mosyle Business and Mosyle Manager : only the first two text fields listed are managed
- with DEPNotify and another MDM Solution : only the first text field listed is managed
- the REGEX, REGEX_ERROR and REQUIRED keys are only supported when the UI Helper is swiftDialog.

SETTINGS_PANE (part 3/5)	Extra informations	Supported	Supported	Dictionary	LIST — Array
Declaring Menus - Manual Filling - All MDM Solutions					-- Item 0 — Dictionary
					-- -- ATTRIBUTE — String — Department
					-- -- TYPE — String — menu
					-- -- TITLE — String — Department
					-- -- BUBBLE_TITLE — String — Title
					-- -- BUBBLE_TEXT — String — Informative Text
					-- -- CONTENT — Array
					-- -- -- Item 0 — Dictionary
					-- -- -- -- VALUE_DISPLAYED — String — Information Technology
					-- -- -- -- VALUE_STORED — String — Information Technology
					-- -- -- Item 1 — Dictionary
					-- -- -- -- VALUE_DISPLAYED — String — Sales
					-- -- -- -- VALUE_STORED — String — Sales

List of the menus displayed in the Settings pane.
ATTRIBUTE : name of the attribute to populate (refer to the list of supported attributes for each MDM solution above)
TYPE : set to "menu"
TITLE : the menu title
BUBBLE_TITLE and BUBBLE_TEXT : the title and text for the Help bubble associated with the menu (DEPNotify only)
CONTENT : VALUE_DISPLAYED is a selectable value, while VALUE_STORED is the corresponding value written in the MDM Solution, and both can differ
Notes :
- with DEPNotify : only the first four menus listed are managed
- with AppleScript : no menu is managed.

SETTINGS_PANE (part 4/5) **Declaring Menus - Automated Filling - Jamf Pro**	Extra informations	Supported	Supported	Dictionary	LIST — Array -- Item 0 — Dictionary -- -- ATTRIBUTE — String — Department -- -- TYPE — String — menu -- -- TITLE — String — Department -- -- BUBBLE_TITLE — String — Title -- -- BUBBLE_TEXT — String — Informative Text -- -- CONTENT — String — network_organization:departments|ignore case

With Jamf Pro, MOM offers an automation to dynamically populate the content of a menu.

Instead of manually completing the selectable values via the CONTENT array, define the CONTENT key of type "string" with one the following values :

- network_organization:buildings

- network_organization:departments

- network_organization:sites

The menu is automatically populated with the values retrieved from Jamf Pro and the selected value is eventually stored in the corresponding device attribute.

To enable sorting options, add a "|" directly after one of the above values then add the below options separated with commas (exact name from this list with case-sensitivity respected) :

- reverse : descending order (ascending order is enabled unless this option is added)

- ignore case : ignore case-sensitivity

SETTINGS_PANE (part 5/5) **Declaring Menus - Automated Filling - Miradore**	Extra informations	Supported	Supported	Dictionary	LIST — Array -- Item 0 — Dictionary -- -- ATTRIBUTE — String — Organization -- -- TYPE — String — menu -- -- TITLE — String — Organization -- -- BUBBLE_TITLE — String — Title -- -- BUBBLE_TEXT — String — Informative Text -- -- CONTENT — String — attributes:organizations|ignore case

With Miradore, MOM offers an automation to dynamically populate the content of a menu.

Instead of manually completing the selectable values via the CONTENT array, define the CONTENT key of type "string" with one the following values :

- attributes:categories

- attributes:locations

- attributes:organizations

- users:emails

The menu is automatically populated with the values retrieved from Miradore and the selected value is eventually stored in the corresponding device attribute.

To enable sorting options, add a "|" directly after one of the above values then add the below options separated with commas (exact name from this list with case-sensitivity respected) :

- reverse : descending order (ascending order is enabled unless this option is added)

- ignore case : ignore case-sensitivity

TIMEZONE	Configuration	Supported	Supported	String	Europe/Paris

The name of a time zone from among those returned by the systemsetup -listtimezones command.

Set to "undefined" to ignore the key.

WALLPAPER_INSTALL	Installation	Supported	Supported	String	enabled

Set to "true" to install the script used by Agnosys Login script to configure the Desktop Picture on a device installed with macOS 10.4.4 and later (see SCRIPTS > LOGINUSERSCRIPT).

WALLPAPER_URL	Installation	Supported	Supported	String	https://github.com/sindresorhus/macos-wallpaper/releases/download/v2.3.2/wallpaper.zip

The URL used to download the wallpaper binary (wallpaper.zip file expected).

UIHELPER	Interface	N/A	Supported	String	swiftdialog

To enable an improved interface, set to "swiftdialog" (preferred) or "depnotify". To enable the legacy interface, set to "applescript".

As swiftDialog requires macOS 11 or later, a fallback to DEPNotify is automatically triggered when macOS 10.15 or earlier is detected.

DEPNOTIFY_URL	Interface	N/A	Supported	String	https://files.nomad.menu/DEPNotify.pkg

The URL used to download the DEPNotify package (DEPNotify*.pkg file expected).

SWIFTDIALOG_URL	Interface	N/A	Supported	String	https://github.com/swiftDialog/swiftDialog/releases/download/v2.5.6/dialog-2.5.6-4805.pkg

The URL used to download the swiftDialog package (dialog*.pkg file expected).
When macOS 11 is detected, the URL is forcibly set to https://github.com/swiftDialog/swiftDialog/releases/download/v2.2.1/dialog-2.2.1-4591.pkg as version 2.2.1 is the newest version compatible.
When macOS 12 is detected, the URL is forcibly set to https://github.com/swiftDialog/swiftDialog/releases/download/v2.4.2/dialog-2.4.2-4755.pkg as version 2.4.2 is the newest version recommended.
Provisioning over the Login Window is supported with swiftDialog 2.5.2 and later.

UIHELPER_PICTURE_WELCOME	Interface	N/A	Supported	String	welcome.png
The picture to be displayed in the welcome pane (.png file expected).					
UIHELPER_MAIN_TITLE_WELCOME	Interface	N/A	Supported	String	Welcome to ACME !
The title to be displayed in the welcome pane.					
UIHELPER_MAIN_TEXT_WELCOME	Interface	N/A	Supported	String	This wizard is aimed to streamline the onboarding of this device in the organization's management solution to give you the best experience of its daily usage.\r\rPlease follow the instructions provided.
The text to be displayed in the welcome pane. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).					
UIHELPER_PICTURE_HELP **QR code - except mailto URI scheme**	Interface	N/A	Supported	Dictionary	TYPE — String — qrcode QRCODE_DATA — String — http://www.maconboardingmate.com QRCODE_COLOR — String — rgb(159,73,190)
• TYPE : set to "qrcode" • QRCODE_DATA : the string to encode within the QR code, such as a URL beginning with "http(s)://" (see below for an email address using "mailto:") • QRCODE_COLOR : the QR code's color in RGB format, for example, rgb(0,0,0) for black This feature is only supported when the UI Helper is swiftDialog 2.5.3 and later, and requires a text display in the help pane.					
UIHELPER_PICTURE_HELP **QR code - mailto URI scheme**	Interface	N/A	Supported	Dictionary	TYPE — String — qrcode QRCODE_DATA — String — mailto:mom.support@agnosys.fr QRCODE_COLOR — String — rgb(159,73,190) MAILTO — Dictionary -- SUBJECT — String — Help Request -- BODY — String — Please provide assistance with the following issue: -- PLACEHOLDERS — Array -- -- Item 0 — String — Workflow : Discover MacOnboardingMate -- -- Item 1 — String — Computer Name : :ComputerName: -- -- Item 2 — String — Serial Number : :SerialNumber: -- -- Item 3 — String — Model Name : :ModelName: -- -- Item 4 — String — Hardware UUID : :HardwareUUID: -- -- Item 5 — String — macOS Version : :macOSVersion:
• TYPE : set to "qrcode" • QRCODE_DATA : an email address using "mailto:" to encode within the QR code • QRCODE_COLOR : the QR code's color in RGB format, for example, rgb(0,0,0) for black • MAILTO : - SUBJECT and BODY keys : the subject and the body of the email, which will be automatically populated - PLACEHOLDERS : optional information that will be inserted before the body text ; the example provides a list of all supported variables ; each item should be considered a separate line, separated by a empty line, and each line can contain any desired text and variables. This feature is only supported when the UI Helper is swiftDialog 2.5.3 and later, and requires a text display in the help pane.					
UIHELPER_PICTURE_HELP **Standard picture**	Interface	N/A	Supported	Dictionary	TYPE — String — file FILENAME — String — help.png
• TYPE : set to "file" • FILENAME : the picture to be displayed in the help pane (.png file expected) This feature is only supported when the UI Helper is swiftDialog 2.5.3 and later, and requires a text display in the help pane.					
UIHELPER_MAIN_TEXT_HELP	Interface	N/A	Supported	String	**ACME IT Support**\n\nUse your mobile device to scan the QR code.\nThis will take you directly to our support page.
The text to be displayed in the help pane. The string accepts markdown for message formatting. Use exactly two spaces followed by \n for a line break and \n\n for a line break followed by an empty line. Set to "undefined" to ignore the key.					

UIHELPER_BUTTON_LABEL_HELP	Interface	N/A	Supported	String	Close
The label to be displayed in the button of the help pane. This feature is only supported when the UI Helper is swiftDialog 2.5.5 and later, and requires a text display in the help pane.					
UIHELPER_PICTURE_EULA	Interface	Supported	Supported	String	eula.png
The picture to be displayed in the EULA pane (.png file expected).					
UIHELPER_MAIN_TITLE_EULA	Interface	Supported	Supported	String	Welcome to ACME !
The title to be displayed in the EULA pane.					
UIHELPER_MAIN_TEXT_EULA	Interface	Supported	Supported	String	Your organization requires that you accept certain terms of agreement to use this device.
The text to be displayed in the EULA pane. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).					
UIHELPER_BUTTON_LABEL_EULA	Interface	Supported	Supported	String	Agreement
The label to be displayed in the button of the EULA pane when the UI Helper is DEPNotify.					
UIHELPER_TITLE_EULA_FORM	Interface	Supported	Supported	String	Computer user agreement
The title to be displayed in the EULA dropdown.					
UIHELPER_SUBTITLE_EULA_FORM	Interface	Supported	Supported	String	Agree to the following terms and conditions to start using this device.
The subtitle to be displayed in the EULA dropdown.					
UIHELPER_TEXT_EULA_FORM	Interface	Supported	Supported	String	computer_user_agreement.md
The text to be displayed in the EULA dropdown (*.md or *.txt file expected). Markdown is only supported when the UI Helper is swiftDialog. Set the key to "undefined" to disable the EULA pane.					
UIHELPER_TEXT_EULA_MONOSPACE	Interface	Supported	Supported	Boolean	true
Set to "true" to display the EULA text in monospace font on a background. This feature is only supported when the UI Helper is swiftDialog 2.3.3 and later.					
UIHELPER_PICTURE_SETTINGS	Interface	Supported	Supported	String	settings.png
The picture to be displayed in the Settings pane (.png file expected).					
UIHELPER_MAIN_TITLE_SETTINGS	Interface	Supported	Supported	String	Welcome to ACME !
The title to be displayed in the Settings pane.					
UIHELPER_MAIN_TEXT_SETTINGS_FUTURE	Interface	Supported	Supported	String	This device will be managed by :MDMSolution: and assigned to :MDMLocation: location.\r\rSome customized settings must be defined manually.
The text to be displayed in the Settings pane when the device will be enrolled in the MDM Solution (Device Enrollment or Automated Device Enrollment executed outside of the Setup Assistant). :MDMSolution: and :MDMLocation: are expected variables for the specified message. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).					
UIHELPER_MAIN_TEXT_SETTINGS_PRESENT	Interface	Supported	Supported	String	This device is managed by :MDMSolution: and assigned to :MDMLocation: location.\r\rSome customized settings must be defined manually.
The text to be displayed in the Settings pane when the device is already enrolled in the MDM Solution (Automated Device Enrollment executed during the Setup Assistant). :MDMSolution: and :MDMLocation: are expected variables for the specified message. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).					
UIHELPER_PICTURE_MUNKICHECKIN	Interface	Supported	Supported	String	munki.png
The picture to be displayed in the Munki check-in pane (.png file expected).					
UIHELPER_MAIN_TITLE_MUNKICHECKIN	Interface	Supported	Supported	String	Welcome to ACME !
The title to be displayed in the Munki check-in pane.					
UIHELPER_MAIN_TEXT_MUNKICHECKIN	Interface	Supported	Supported	String	Some critical apps must be installed immediately.\r\rThis process normally takes a couple of minutes to complete.
The text to be displayed in the Munki check-in pane. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).					
UIHELPER_PICTURE_LANDING	Interface	Supported	Supported	String	landing.png
The picture to be displayed in the Landing pane (.png file expected).					
UIHELPER_FINALSCREEN_LANDING	Interface	Supported	Supported	Dictionary	PICTURE — String — checkmark.png HIDE_MAIN_TEXT — Boolean — false

PICTURE : The final screen to be displayed in the Landing pane (.png file expected).
HIDE_MAIN_TEXT : Set to "true" to hide any message that would normally appear above the final screen picture ; this key is ignored if an error occurred and needs to be reported.
This feature is only supported when the UI Helper is swiftDialog.

UIHELPER_MAIN_TITLE_LANDING	Interface	Supported	Supported	String	Welcome to ACME !
The title to be displayed in the Landing pane.					
UIHELPER_MAIN_TEXT_LANDING	Interface	Supported	Supported	String	Your device is now fully onboarded in the organization's management solution.\r\rPlease visit the Self Service of :MDMSolution: to discover and install optional resources.
The text to be displayed in the Landing pane. :MDMSolution: is an expected variable for the specified message. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).					
EASYLAPS_INTEGRATION (inside INTEGRATIONS Dictionary)	Configuration	Supported	Supported	Boolean	true
Set to "true" to enable the EasyLAPS integration defined by the EASYLAPS_CONFIGURATION Dictionary.					
EASYLAPS_CONFIGURATION (inside INTEGRATIONS Dictionary)	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary
EasyLAPS Gateway makes available to EasyLAPS the current management account password managed by EasyLAPS or another LAPS solution, so that a true rotation is possible. The password collection is managed by MacOnboardingMate (MOM) during an MDM migration workflow. The collected password is temporarily escrowed in the EasyLAPS Keychain and EasyLAPS Safe mode is enabled. EasyLAPS Gateway. Two scenarios are currently supported : 1. Current management account password managed by EasyLAPS ; set the EASYLAPS_GATEWAY > PASSWORD_SOURCE key to "easylaps" and ensure that EasyLAPS is properly installed and configured for the previous MDM before the MDM unenrollment 2. MDM migration from Jamf Pro and current management account password managed by the native Jamf Pro LAPS solution ; set the EASYLAPS_GATEWAY > PASSWORD_SOURCE key to "jamf_pro_laps" and ensure that the MIGRATION_MDMSOLUTION, MIGRATION_APIURL and MIGRATION_APIAUTHENTICATIONSTRING keys are configured for an MDM migration from Jamf Pro that allows API calls (details in the Integration Guide). ROTATION_REQUEST : Set to "true" to request a management account password rotation at the end of the workflow ; ensure that EasyLAPS is properly installed and configured for the MDM in which the device is enrolled ; to make the workflow wait for EasyLAPS to install, declare an awaited item with the type value set to "path" and the item value set to /Library/Application Support/EasyLAPS/easylaps.sh					
HOMEBREW_INTEGRATION (inside INTEGRATIONS Dictionary)	Installation	Supported	Supported	Boolean	true
Set to "true" to enable the Homebrew integration defined by the HOMEBREW_CONFIGURATION Dictionary.					
HOMEBREW_CONFIGURATION (inside INTEGRATIONS Dictionary)	Installation	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary
HOMEBREW_INSTALL : Set to "enabled" to install Homebrew HOMEBREW_URL : The URL used to download the Homebrew package (Homebrew*.pkg file expected) Set this URL to "undefined" to delegate the installation process to AutoBrew (https://github.com/kennyb-222/AutoBrew). FORMULAE : Add one array item per formula Item > UIHELPER_MAIN_TEXT : Text displayed when the formula is installed Item > UIHELPER_STATUS : Status displayed when the formula is installed Item > FORMULA_NAME : Name of the formula to install Item > FORMULA_ICON : Icon displayed when the formula is installed (.png file expected) ; if the icon is not available, an Homebrew icon is displayed instead Item > FORMULA_CASK : Set to " true" to install the GUI application associated with the formula					
INSTALLOMATOR_INTEGRATION (inside INTEGRATIONS Dictionary)	Installation	Supported	Supported	Boolean	true
Set to "true" to enable the Installomator integration defined by the INSTALLOMATOR_CONFIGURATION Dictionary.					
INSTALLOMATOR_CONFIGURATION (inside INTEGRATIONS Dictionary)	Installation	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

INSTALLOMATOR_INSTALL : Set to "enabled" to install Installomator
INSTALLOMATOR_URL : The URL used to download Installomator (Installomator*.pkg file expected)
INSTALLOMATOR_BLOCKING_PROCESS_ACTION : Set to "ignore" or "silent_fail" or "kill" ; more infos at https://github.com/Installomator/Installomator/wiki/Configuration-and-Variables
LABELS : Add one array item per label
Item > UIHELPER_MAIN_TEXT : Text displayed when the label is installed
Item > UIHELPER_STATUS : Status displayed when the label is installed
Item > LABEL_NAME : Name of the label to install listed at https://github.com/Installomator/Installomator/blob/release/Labels.txt
Item > LABEL_ICON : Icon displayed when the label is installed (.png file expected) ; if the icon is not available, an Installomator icon is displayed instead
Item > FORCE_INSTALLATION : Set to " true" (software installed even if it's the same version) or "false" (software installed only if it is newer/different in version)
Item > IGNORE_APP_STORE_APP : Set to "true" (software installed over App Store app even if latest version) or "false" (installed App Store app never touched no matter its version)

JAMF_CONNECT_INTEGRATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Boolean	true

Set to "true" to enable the Jamf Connect integration defined by the JAMF_CONNECT_CONFIGURATION Dictionary.

JAMF_CONNECT_CONFIGURATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

JAMF_CONNECT_INSTALL : Set to "enabled" to install Jamf Connect.
JAMF_CONNECT_URL : The URL used to download Jamf Connect (*.dmg file expected).
JAMF_CONNECT_CONFIG : Set to "enabled" to activate Jamf Connect (no other sign-in software must be activated). Set to "disabled" to revert to macOS Login Window.
Configurations are supposed to be performed by Configuration profiles.

JAMF_PRO_INTEGRATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Boolean	true

Set to "true" to enable the Jamf Pro integration defined by the JAMF_PRO_CONFIGURATION Dictionary.

JAMF_PRO_CONFIGURATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

Set the JAMF_PRO_API key to "true" for using the Jamf Pro API when possible instead of the Classic API ; the requirements are macOS 10.15 and later, Jamf Pro 10.50 and later.
JAMF_PRO_POLICIES > EXECUTION : Set to "true" to execute the listed policies
JAMF_PRO_POLICIES > DISPLAY : Set to "compact" to display the execution of all policies as a single stage in the stages list, or set to "expanded" to display each policy as a separate stage in the stages list
JAMF_PRO_POLICIES > LIST : Add one array item per policy
Item > UIHELPER_NAME : Name displayed for the policy
Item > UIHELPER_MAIN_TEXT : Text displayed when the policy is executed
Item > UIHELPER_STATUS : Status displayed when the policy is executed
Item > POLICY_TRIGGER : Custom event in the format event:custom_event or Identifier in the format id:identifier
Item > POLICY_ICON : Icon displayed for the policy (.png file expected) ; if the icon is not available, a Jamf icon is displayed
The Custom event associated to a policy is set in Computers > Policies > Policy > Options > General > Custom > Custom Event.
The Identifier associated to a policy is displayed in Computers > Policies > Policy > https://hostname.jamfcloud.com/policies.html?id=X

KERBEROS_SSO_EXTENSION_INTEGRATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Boolean	true

Set to "true" to enable the Kerberos SSO Extension Integration defined by the KERBEROS_SSO_EXTENSION_CONFIGURATION Dictionary.

KERBEROS_SSO_EXTENSION_CONFIGURATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

WAIT_KERBEROS_TICKET : Set to "true" to wait for a Kerberos ticket to be acquired.
WAIT_PASSWORD_SYNC : Set to "true" to wait until password synchronization between the local and network accounts is complete.
TEXT : The instructions displayed while the logged-in user is prompted to acquire a Kerberos ticket and/or synchronize the password between the local and network accounts.
KERBEROS_REALM : The Kerberos realm used by the Kerberos SSO Extension.
The integration is skipped if connectivity to Kerberos services cannot be established.

MSCP_INTEGRATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Boolean	true

Set to "true" to enable the mSCP integration defined by the MSCP_CONFIGURATION Dictionary.

MSCP_CONFIGURATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the 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)

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)

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

MUNKI_INTEGRATION (inside INTEGRATIONS Dictionary)	Configuration	Supported	Supported	Boolean	true
Set to "true" to enable the Munki integration defined by the MUNKI_CONFIGURATION Dictionary.					
MUNKI_CONFIGURATION (inside INTEGRATIONS Dictionary)	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary
MUNKI_INSTALL : Set to "enabled" to install the Munki Tools. MUNKI_URL : The URL used to download the Munki Tools (munkitools*.pkg file expected). MUNKI_CHECKINAFTERSETUP : Set to "enabled" to trigger a Munki check-in during the workflow.					
NOMAD_INTEGRATION (inside INTEGRATIONS Dictionary)	Configuration	Supported	Supported	Boolean	true
Set to "true" to enable the NoMAD integration defined by the NOMAD_CONFIGURATION Dictionary.					
NOMAD_CONFIGURATION (inside INTEGRATIONS Dictionary)	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary
NOMAD_INSTALL : Set to "enabled" to install NoMAD. The configuration is supposed to be performed by a Configuration profile. NOMAD_URL : The URL used to download NoMAD (NoMAD*.pkg file expected). NOMAD_LAUNCHAGENT_URL : The URL used to download NoMAD LaunchAgent (NoMAD*.pkg file expected). NOMAD_LOGINAD_URL : The URL used to download NoMAD Login AD (NoMAD*.pkg file expected). NOMAD_LOGINAD_CONFIG : Set to "enabled" to activate NoMAD Login AD (no other sign-in software must be activated). Set to "disabled" to revert to macOS Login Window. Configurations are supposed to be performed by Configuration profiles.					
SLACK_INTEGRATION (inside INTEGRATIONS Dictionary)	Notification	Supported	Supported	Boolean	true
Set to "true" to enable the Slack integration defined by the SLACK_CONFIGURATION Dictionary.					
SLACK_CONFIGURATION (inside INTEGRATIONS Dictionary)	Notification	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

INCOMING_WEBHOOK_URL : RSA-encrypted_incoming_webhook_URL (refer to https://api.slack.com/messaging/webhooks)

RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.

In the following examples, ":gear:" is an emoji (refer to https://www.webfx.com/tools/emoji-cheat-sheet/) and ":ModelName:" is an available variable for the specified message.

MESSAGE_WORKFLOW_STARTED : message sent when the workflow is started

:gear: :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Workflow of type :WorkflowType: started

MESSAGE_WORKFLOW_EULA_AGREED : message sent when EULA is agreed

:arrow_forward: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - EULA agreed by :LoggedInAccountRealName: (:LoggedInAccount:)

MESSAGE_WORKFLOW_EXITED : message sent when the workflow is exited (the heading emoji is set automatically to indicate success, info or error)

:Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Workflow exited : :ExitMessage:

MESSAGE_DEVICE_ENROLLED : message sent when the device is enrolled

:arrow_forward: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device enrolled in :MDMSolution: > :MDMLocation: - MDM detected : :MDMSolutionDetected:

MESSAGE_DEVICE_PENDING_PROVISIONING : message sent when the enrollment of the device requires an action by the IT Support in the console of the MDM solution to be joined and/or AxM

:warning: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device pending provisioning to enroll in :MDMSolution: - Number of ADE attempts in the last :ADEComputationTimeframe: hours : :ADEEnrollmentAttempts:

MESSAGE_DEVICE_PENDING_ENROLLMENT : message sent when the enrollment of the device requires assistance from IT Support

:warning: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device pending enrollment in :MDMSolution: - Number of ADE attempts in the last :ADEComputationTimeframe: hours : :ADEEnrollmentAttempts:

MESSAGE_DEVICE_PENDING_UNENROLLMENT : message sent when the unenrollment of the device requires an action by the IT Support in the console of the MDM solution to be left

:warning: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device pending unenrollment from :MDMSolutionUnenroll:

MESSAGE_DEVICE_UNENROLLED : message sent when the device is unenrolled

:warning: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device unenrolled from :MDMSolutionUnenroll:

MESSAGE_PROMOTION_START : message sent when administrative privileges are granted

:warning: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Admin privileges granted for logged in account :LoggedInAccountRealName: (:LoggedInAccount:)

MESSAGE_PROMOTION_STOP : message sent when administrative privileges are withdrawn

:information_source: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Admin privileges withdrawn for logged in account :LoggedInAccountRealName: (:LoggedInAccount:) after :PromotionDuration: seconds

MESSAGE_FLIGHT_RECORDER : message sent when the Flight recorder has recorded at least one error during the workflow

:warning: Date : :Date: :Time:\rModel Name : :ModelName:\rSerial Number : :SerialNumber:\rComputer Name : :ComputerName:\rLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)\rmacOS Version : :macOSVersion:\rFlight Recorder Report :\r:FlightRecorderReport:

MESSAGE_MSCP_COMPLIANCE : message sent for the compliance report generated by the mSCP integration

Date : :Date: :Time:\rModel Name : :ModelName:\rSerial Number : :SerialNumber:\rComputer Name : :ComputerName:\rLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)\rmacOS Version : :macOSVersion:\rmSCP Compliance Report :\r:mSCPComplianceReport:

TEAMS_INTEGRATION (inside INTEGRATIONS Dictionary)	Notification	Supported	Supported	Boolean	true
Set to "true" to enable the Teams integration defined by the TEAMS_CONFIGURATION Dictionary.					
TEAMS_CONFIGURATION (inside INTEGRATIONS Dictionary)	Notification	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary

INCOMING_WEBHOOK_PROCESSING : set to "workflows"

INCOMING_WEBHOOK_URL : RSA-encrypted_incoming_webhook_URL (refer to the Integration Guide for the details)

RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.

In the following examples, "⚙" is an emoji (refer to https://unicode.org/emoji/charts/full-emoji-list.html) followed by a wide space and ":ModelName:" is an available variable for the specified message.

MESSAGE_WORKFLOW_STARTED : message sent when the workflow is started

⚙ :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Workflow of type :WorkflowType: started

MESSAGE_WORKFLOW_EULA_AGREED : message sent when EULA is agreed

▶ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - EULA agreed by :LoggedInAccountRealName: (:LoggedInAccount:)

MESSAGE_WORKFLOW_EXITED : message sent when the workflow is exited (the heading emoji is set automatically to indicate success, info or error)

:ModelName: :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Workflow exited : :ExitMessage:

MESSAGE_DEVICE_ENROLLED : message sent when the device is enrolled

▶ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device enrolled in :MDMSolution: > :MDMLocation: - MDM detected : :MDMSolutionDetected:

MESSAGE_DEVICE_PENDING_PROVISIONING : message sent when the enrollment of the device requires an action by the IT Support in the console of the MDM solution to be joined and/or AxM

⚠ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device pending provisioning to enroll in :MDMSolution: - Number of ADE attempts in the last :ADEComputationTimeframe:

hours : :ADEEnrollmentAttempts:

MESSAGE_DEVICE_PENDING_ENROLLMENT : message sent when the enrollment of the device requires assistance from IT Support

⚠ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device pending enrollment in :MDMSolution: - Number of ADE attempts in the last :ADEComputationTimeframe: hours : :ADEEnrollmentAttempts:

MESSAGE_DEVICE_PENDING_UNENROLLMENT : message sent when the unenrollment of the device requires an action by the IT Support in the console of the MDM solution to be left

⚠ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device pending unenrollment from :MDMSolutionUnenroll:

MESSAGE_DEVICE_UNENROLLED : message sent when the device is unenrolled

⚠ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Device unenrolled from :MDMSolutionUnenroll:

MESSAGE_PROMOTION_START : message sent when administrative privileges are granted

⚠ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Admin privileges granted for logged in account :LoggedInAccountRealName: (:LoggedInAccount:)

MESSAGE_PROMOTION_STOP : message sent when administrative privileges are withdrawn

ℹ :Date: :Time: :ModelName: :SerialNumber: :ComputerName: - Admin privileges withdrawn for logged in account :LoggedInAccountRealName: (:LoggedInAccount:) after :PromotionDuration: seconds

MESSAGE_FLIGHT_RECORDER : message sent when the Flight recorder has recorded at least one error during the workflow

⚠ Date : :Date: :Time:\n\nModel Name : :ModelName:\n\nSerial Number : :SerialNumber:\n\nComputer Name : :ComputerName:\n\nLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)

\n\nmacOS Version : :macOSVersion:\n\nFlight Recorder Report :\n\n:FlightRecorderReport:

MESSAGE_MSCP_COMPLIANCE : message sent for the compliance report generated by the mSCP integration

Date : :Date: :Time:\n\nModel Name : :ModelName:\n\nSerial Number : :SerialNumber:\n\nComputer Name : :ComputerName:\n\nLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)\n\nmacOS

Version : :macOSVersion:\n\nmSCP Compliance Report :\n\n:mSCPComplianceReport:

Key	Context	Launcher	AutoLauncher	Type	Example
XCREDS_INTEGRATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Boolean	true
Set to "true" to enable the XCreds integration defined by the XCREDS_CONFIGURATION Dictionary.					
XCREDS_CONFIGURATION **(inside INTEGRATIONS Dictionary)**	Configuration	Supported	Supported	Dictionary	Refer to the template for the structure of the Dictionary
XCRED_INSTALL : Set to "enabled" to install XCreds.					
XCREDS_URL : The URL used to download XCreds (*.pkg file expected).					

MOM Switch

The following keys apply to MOM Switch only and will be ignored if the license key does not match this version.

Key	Context	Launcher	AutoLauncher	Type	Example
MIGRATION_DISALLOWED_ACCOUNTS	Migration	N/A	Supported	String	ladmin,helpdesk
List of account names separated with commas that are not offered to execute a migration workflow when they are logged in.					
The purpose of this key is to ensure that a management account does not inadvertently become the MDM enabled user.					
MIGRATION_DISALLOWED_AFTER_WORKFLOW_DONE	Migration	N/A	Supported	Boolean	true
Set to "false" to allow the execution of a migration workflow if a MOM workflow was already executed.					
MIGRATION_DISALLOWED_PROCESSES	Migration	N/A	Supported	String	Cisco Webex Meetings,FaceTime,Microsoft Teams,zoom.us
List of processes as they appear in Activity Monitor and separated with commas that prevent a migration workflow from running when detected.					
The purpose of this key is to ensure that a migration workflow won't be executed or offered unexpectedly during a meeting.					
The migration workflow is forcibly postponed by 15 minutes to avoid piling up notifications about detected disallowed processes.					
MIGRATION_WARNING_MIGRATION_DONE	Migration	N/A	Supported	Boolean	true

Set to "true" to be warned that the device was already migrated from a management solution with MOM.					
MIGRATION_CHOOSE_INVENTORY_SOURCE	Migration	Supported	Supported	Boolean	false
By default, the inventory source is the management solution the devices leaves.					
Set to "true" to display a dialog that offers to choose the inventory source between the previous and the new management solution.					
This key is mainly used in the context of testing.					
MIGRATION_POSTPONE	Migration	N/A	Supported	String	deadline:2022-11-12 12:00|defer:1 day-86400|defer:1 hour-3600
Set this key to offer the user to postpone the migration workflow so that it can be triggered at an opportune time.					
Values are separated with pipes.					
To set one or two defer choices displayed as buttons, add "defer:" followed by "button_label-delay_in_seconds".					
To set an optional deadline, add "deadline:" followed by "YYYY-MM-DD" and if desired "<space>HH:MM" (no seconds) before the first defer.					
MIGRATION_TIME_SLOTS	Migration	N/A	Supported	Array	Refer to the template for the structure of the Array
Scheduling of the time slots allowed for migration, aimed to reflect the availability of the IT Support.					
In the following example, the migration is allowed for CEST time zone each week day from 9:30 to 12:30 and from 13:30 to 17:30, and each saturday and sunday from 9:30 to 12:30.					
CEST|Mon=09:30-12:30|Mon=13:30-17:30|Tue=9:30-12:30|Tue=13:30-17:30|Wed=9:30-12:30|Wed=13:30-17:30|Thu=9:30-12:30|Thu=13:30-17:30|Fri=9:30-12:30|Fri=13:30-17:30|Sat=9:30-12:30|Sun=9:30-12:30					
An entry that does not begin with an official time zone abbreviation followed by a "|" applies as a fallback to all devices which time zone is not specifically referenced in the array.					
Time zone abbreviations are available on this page : https://en.wikipedia.org/wiki/List_of_tz_database_time_zones. Type the command "date +%Z" to display the current device time zone abbreviation.					
MIGRATION_MDMSOLUTION	Migration	Supported	Supported	String	Meraki Systems Manager
The management solution the devices leaves : "FileWave", "Hexnode UEM", "Jamf Now", "Jamf Pro", "Jamf School", "JumpCloud", "Kandji", "ManageEngine MDM", "Meraki Systems Manager", "Microsoft Intune", "Miradore", "Mosyle Business", "Mosyle Manager", "Omnissa Workspace ONE", "SimpleMDM" (exact name from this list with case-sensitivity respected).					
MIGRATION_MDMLOCATION	Migration	Supported	Supported	String	Paris
This setting only applies to Meraki Systems Manager.					
The exact name of the Network defined inside the Organization the device leaves.					
MIGRATION_APIURL	Migration	Supported	Supported	String	https://api.meraki.com/api/v1
The URL to make API calls with the management solution the device leaves.					
FileWave : https://hostname.filewave.net (API v1 and v2 usage)					
Hexnode UEM : https://hostname.hexnodemdm.com/api					
Jamf Pro : https://hostname.jamfcloud.com (Classic API and Jamf Pro API usage)					
Jamf School : https://hostname.jamfcloud.com/api					
JumpCloud : https://console.jumpcloud.com/api					
Kandji : https://hostname.api.kandji.io (US) or https://hostname.api.eu.kandji.io (EU) ; refer to https://support.kandji.io/api					
Meraki Systems Manager : https://api.meraki.com/api/v1					
Microsoft Intune : https://graph.microsoft.com/Beta (API 1.0 is not supported)					
Miradore : https://sitename.online.miradore.com (API v1 and v2 usage)					
Mosyle Business : https://businessapi.mosyle.com/v1					
Mosyle Manager : https://managerapi.mosyle.com/v2					
Omnissa Workspace ONE : Groups & Settings > All Settings > System > Advanced > API > Rest API — General > REST API URL : https://asX.awmdm.com/api					
SimpleMDM : https://a.simplemdm.com/api/v1					
MIGRATION_APIAUTHENTICATIONSTRING	Migration	Supported	Supported	String	RSA-encrypted_authentication_string

The string to be used to authenticate API calls with the management solution the device leaves.

FileWave : FileWave Admin > Assistants > Manage Administrators > + Local Account > User details : Login Name - Set password / Permissions / Application tokens : Token (base64)

Hexnode UEM : Admin > API > Configure API > Enable > padlock

Jamf Pro (API Roles and Clients) : concatenation of those 2 values separated with a colon : Client ID:Client Secret (refer to the Integration Guide for the details)

Jamf Pro (User account) : concatenation of those 2 values separated with a colon : apisvcaccount:apisvcaccountpassword

Jamf School : Network ID:API Key (School > Devices > Enroll Device(s) > On-device enrollment > Network ID / School > Settings > API > Add API Key > Name + Key > Apply)

JumpCloud : API Key (Account > API Settings)

Kandji : API Token ; refer to https://support.kandji.io/api

Meraki Systems Manager : Organization > Configure > Settings > Dashboard API access > Enable access to the Cisco Meraki Dashboard API + Account > My Profile > API access > Generate new API key

Microsoft Intune : concatenation of those 3 values separated with commas : tenant_domain,application_(client)_id,client_secret_value

Miradore : API key (Infrastructure diagram > API > Create key > Name > API key > Create key)

Mosyle Business : concatenation of those 3 values separated with commas : apisvcaccountemail,apisvcaccountpassword,accesstoken

- API Service Account : Organization > Administrators > Add Administrator > Name / User ID / Email / Send welcome e-mail : unchecked / Password / Account type : Administrator > Save

- Access Token : Organization > Integrations > Mosyle API Integration > Add new token > Profile name / Access Method : Public / Allowed Endpoint : Devices > Save > Access Token

Mosyle Manager : concatenation of those 3 values separated with commas : apisvcaccountemail,apisvcaccountpassword,accesstoken

- API Service Account : MySchool > Administrators > Add new administrator > Name / User ID / Email / Send welcome e-mail : unchecked > Save > Edit > Password / Account type : Leader > Save

- Access Token : MySchool > Integrations > Mosyle API Integration > Enable API Integration > Access Token

Omnissa Workspace ONE (OAuth2 authentication) : concatenation of those 3 values separated with commas : Token URL,Client ID,Client Secret

- Token URL : refer to https://docs.omnissa.com/bundle/WorkspaceONE-UEM-Console-BasicsVSaaS/page/UsingUEMFunctionalityWithRESTAPI.html

- Groups & Settings > Configurations > OAuth Client Management > Name, Description, Organization Group, Role : Console Administrator / Custom Role, Status : Enabled > Client ID, Client Secret

Omnissa Workspace ONE (Basic authentication) : concatenation of those 3 values separated with commas : username,password,API Key

- Accounts > Administrators > List View > Username — Roles > Organization Group : Console Administrator / Custom Role — API > Authentication : User Credentials

- Groups & Settings > All Settings > System > Advanced > API > Rest API — General > Enable API Access : Enabled / Service : AirWatchAPI | Account Type : Admin | API Key — Authentication > Basic : Enabled

SimpleMDM : API Key (Account > API > Add API Key > name > Save > Secret Access Key > reveal)

RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.

MIGRATION_ATTRIBUTE_REDIRECTS	Migration	Supported	Supported	String	Tags>Asset Tag,Notes>Notes

The mappings that associate the name of a source attribute in the previous MDM with the name of a destination attribute in the new MDM.

In the example, the attribute "Tags" in the previous MDM is redirected to the attribute "Asset Tag" in the new MDM and the attribute "Notes" in the previous MDM is redirected to the attribute "Notes" in the new MDM.

All migrated values are eventually treated as strings.

If the EXTRA_INPUT_ATTRIBUTE string contains the source attribute(s), its/their value(s) is/are displayed in the Settings form as the value(s) of the destination attribute(s) that may be optionally edited.

MIGRATION_FILEVAULT_PRK_REISSUANCE	Migration	Supported	Supported	String	required

This key only applies to devices with FileVault enabled and configured with a Personal Recovery Key.

Set to "required" to reissue a FileVault Personal Recovery Key after the device is enrolled.

Set to "optional" for the same action but with the possibility to skip it when a password must be entered interactively.

The reissuance requires the MDM in which the device enrolls to provide an FDERecoveryKeyEscrow configuration at enrollment. The methods used are in this order :

- Automated reissuance with FileVault Personal Recovery Key escrowed in the MDM the devices leaves (supported with Jamf Pro, JumpCloud, Omnissa Workspace ONE, SimpleMDM ; macOS 10.14 and later required)

- Automated reissuance with management account credentials read from MDM configuration file

- Automated reissuance with credentials escrowed during SecureToken granting (see MGTACCOUNTSECURETOKEN) or FileVault enablement (see MGTACCOUNTFILEVAULT)

- Interactive reissuance with credentials entered by a user who holds a SecureToken (APFS Boot Volume only).

This key is ignored with JumpCloud (FileVault PRK escrow not based on a FDERecoveryKeyEscrow configuration).

Set to "undefined" to ignore the key.

MIGRATION_FILEVAULT_PRK_REISSUANCE_DEFER_ROUND1	Migration	Supported	Supported	Integer	20

Number of seconds, starting to the reissuance execution at the beginning of the workflow, to wait the FDERecoveryKeyEscrow configuration.

When the time limit has passed, the reissuance is rescheduled at the end of the workflow.

The number should be adjusted according to the time measured to receive the FDERecoveryKeyEscrow configuration, knowing that a reissuance at the end of the workflow could eventually be preferable.

MIGRATION_FILEVAULT_PRK_REISSUANCE_DEFER_ROUND2	Migration	Supported	Supported	Integer	300

Number of seconds, starting from initial device enrollment, to wait the FDERecoveryKeyEscrow configuration when the reissuance was rescheduled at the end of the workflow.

When the time limit has passed, the reissuance is skipped.

FALLBACK_WIFI_NETWORKS	Migration	Supported	Supported	Array	FALLBACK_WIFI_NETWORKS — Array -- Item 0 — Dictionary -- -- SSID — String — Rescue -- -- PASSWORD — String — RSA-encrypted_password
List of Wi-Fi Networks attempted to be joined in loop when the DNS check executed after unenrollment fails (see DNSCHECKHOSTNAME). Each Wi-Fi Network is defined by a dictionary containing SSID and PASSWORD keys. RSA encryption : use the script "mom_rsa_engine" to generate the full value including the "RSA-" prefix.					
UNENROLLMENT_ALLOWED_TO_DELETE_DEVICE	Migration	Supported	Supported	Boolean	false
An Automated Device Enrollment Remote Management profile protected by the "prevent unenrollment" option can be removed by making an API call. Set to "true" to allow the device deletion in the MDM the devices leaves when an unenrollment-only API call is not offered. Explicit allowance is required because device details in the MDM the device leaves may be lost once the unenrollment is done, specifically if attributes are not redirected (see MIGRATION_ATTRIBUTE_REDIRECTS). This setting only applies to FileWave, Hexnode UEM, JumpCloud, Kandji and SimpleMDM.					
UNENROLLMENT_SCRIPT	Migration	Supported	Supported	String	uninstall.sh
The name of the script that is executed to uninstall the resources of the management solution left by the device. FileWave : the required script titled "FileWaveUninstallermacOS[...].sh" must be downloaded from this page : https://kb.filewave.com/books/filewave-client/page/uninstall-the-filewave-client-on-macos ("Standalone" section) Set to "undefined" to execute the built-in scripts.					