EasyLAPS

Integration Guide

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

Introduction 7
Synopsis 8
Resources overview 8
Implementation workflow 9
EasyLAPS logics 10
Software requirements 15
macOS 15
EasyLAPS packages 15
Packaging editor 15
Property List editor 15
Text Editor 15
VMware Workspace ONE Admin Assistant 15
EasyLAPS Toolkit installation 16
Encryption keys creation 17
Key pair to encrypt the sensitive informations in an EasyLAPS Property List 17
Key pair to encrypt the rotated passwords stored in the MDM 18
EasyLAPS configuration file edition 21
Access to the configuration file template 21
Reference for configuration file keys 21
Public key to encrypt the rotated passwords stored in the MDM 22
License key 22
Management account keys 23
Password policy 24
Initial password of the local administrator account 24
FileWave : APIAUTHENTICATIONSTRING key 26
Jamf Pro - API Roles and Clients : APIAUTHENTICATIONSTRING key 28
Jamf Pro - User account : APIAUTHENTICATIONSTRING key 31
Jamf School : APIAUTHENTICATIONSTRING key 32
JumpCloud : APIAUTHENTICATIONSTRING key 33
Meraki Systems Manager : APIAUTHENTICATIONSTRING key 34
Microsoft Intune : APIAUTHENTICATIONSTRING key 35
Miradore : APIAUTHENTICATIONSTRING key 40
Mosyle Business : APIAUTHENTICATIONSTRING key 41
Mosyle Manager : APIAUTHENTICATIONSTRING key 42

SimpleMDM : APIAUTHENTICATIONSTRING key....43
VMware Workspace ONE - OAuth authentication : APIAUTHENTICATIONSTRING key....44
VMware Workspace ONE - Basic authentication : APIAUTHENTICATIONSTRING key....47
Microsoft Teams integration....53
EasyLAPS configuration files to Custom configuration profiles conversion....58
EasyLAPS Content building....60
Package signature requirement....60
Package signature options....61
Project opening....62
Signing configuration....63
Project building....64
Configuration profiles requirements....67
Provisioning FileWave....68
General configuration....68
EasyLAPS Custom Field....68
Custom configuration profile....70
EasyLAPS-Content package....70
EasyLAPS-Core package....70
Deployment on the EasyLAPS group....71
Result of a successful rotation....72
Provisioning Jamf Pro....74
General configuration....74
Custom configuration profile : importing a .plist file....74
Custom configuration profile : importing a .mobileconfig file....74
EasyLAPS-Content package....75
EasyLAPS-Core package....75
Result of a successful rotation....76
Re-enrollment settings....77
Provisioning Jamf School....78
General configuration....78
Custom configuration profile....78
EasyLAPS-Content package....78
EasyLAPS-Core package....78
Result of a successful rotation....79

Provisioning JumpCloud 80
General configuration 80
Custom configuration profile 80
EasyLAPS-Content package 81
EasyLAPS-Core package 81
Result of a successful rotation 81
Provisioning Meraki Systems Manager 82
General configuration 82
Custom configuration profile 82
EasyLAPS-Content package 82
EasyLAPS-Core package 83
Result of a successful rotation 83
Provisioning Microsoft Intune 84
General configuration 84
Custom configuration profile 84
EasyLAPS-Content package 85
EasyLAPS-Core package 86
Result of a successful rotation 89
Provisioning Miradore 90
General configuration 90
Custom configuration profile 90
EasyLAPS-Content package 90
EasyLAPS-Core package 90
Provisioning policy configuration 91
Result of a successful rotation 91
Provisioning Mosyle Business 93
General configuration 93
Custom configuration profile 93
EasyLAPS-Content package 93
EasyLAPS-Core package 94
Result of a successful rotation 95
Provisioning Mosyle Manager 96
General configuration 96
Custom configuration profile 96

EasyLAPS-Content package 96
EasyLAPS-Core package 97
Result of a successful rotation....98
Provisioning SimpleMDM 99
General configuration....99
Custom configuration profile 99
EasyLAPS-Content package 99
EasyLAPS-Core package 99
Result of a successful rotation....100
Provisioning VMware Workspace ONE 101
General configuration....101
Custom configuration profile 101
EasyLAPS-Content package 102
EasyLAPS-Core package 105
Result of a successful rotation....105
Revealing an encrypted password....107
Renewing EasyLAPS license 109
Editing the LICENSE key of the deployed Custom configuration profile....109
Editing the EasyLAPS configuration file(s)....110
Updating EasyLAPS....112
EasyLAPS Toolkit....112
EasyLAPS configuration file(s)....114
Custom configuration profile(s)....114
EasyLAPS Content package....114
EasyLAPS Core package....114
Edge cases....115
Troubleshooting....116
Display the follow-up file....116
Enable the debug logging manually....117
Enable the debug logging with Custom configuration profile....117
Display the debug logs from the Console utility 118
Display the debug logs from the Terminal utility 118
Run the rotation manually 118

Enable the trace log with Custom configuration profile....119
Display the trace log of type "log file" from the Console utility....119
Display the trace log of type "Unified Logging" from the Terminal utility....119
Resolve a Custom configuration profile deployment failure....120
Info code matrix....121
Error code matrix....123
Microsoft Intune - Solve a non-reinstallation issue....128
VMware Workspace ONE - Distribute an updated Custom configuration profile....128
Collect the password for developments....130
Support....132
Paid support included in EasyLAPS offers....132
Free community support....132
Release notes....132

Introduction

EasyLAPS is a tool designed to regularly rotate the local administrator account password of a Mac and store it in a Mobile Device Management (MDM) solution. The main purpose of EasyLAPS is to have unique passwords on a Mac fleet which are centralized in the MDM console.

EasyLAPS operates a true rotation of the local administrator password, so the account keeps its cryptographic status. That means that once the password is changed, the account is still a Crypto user and Volume owner, able to unlock the device, install macOS updates, make changes to the startup security policy, initiate an Erase All Content and Settings, and more.

Before reading this documentation, please consult the following pages.

• Introduction

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

• Management solutions support

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

• Capabilities

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

• Offers and pricing

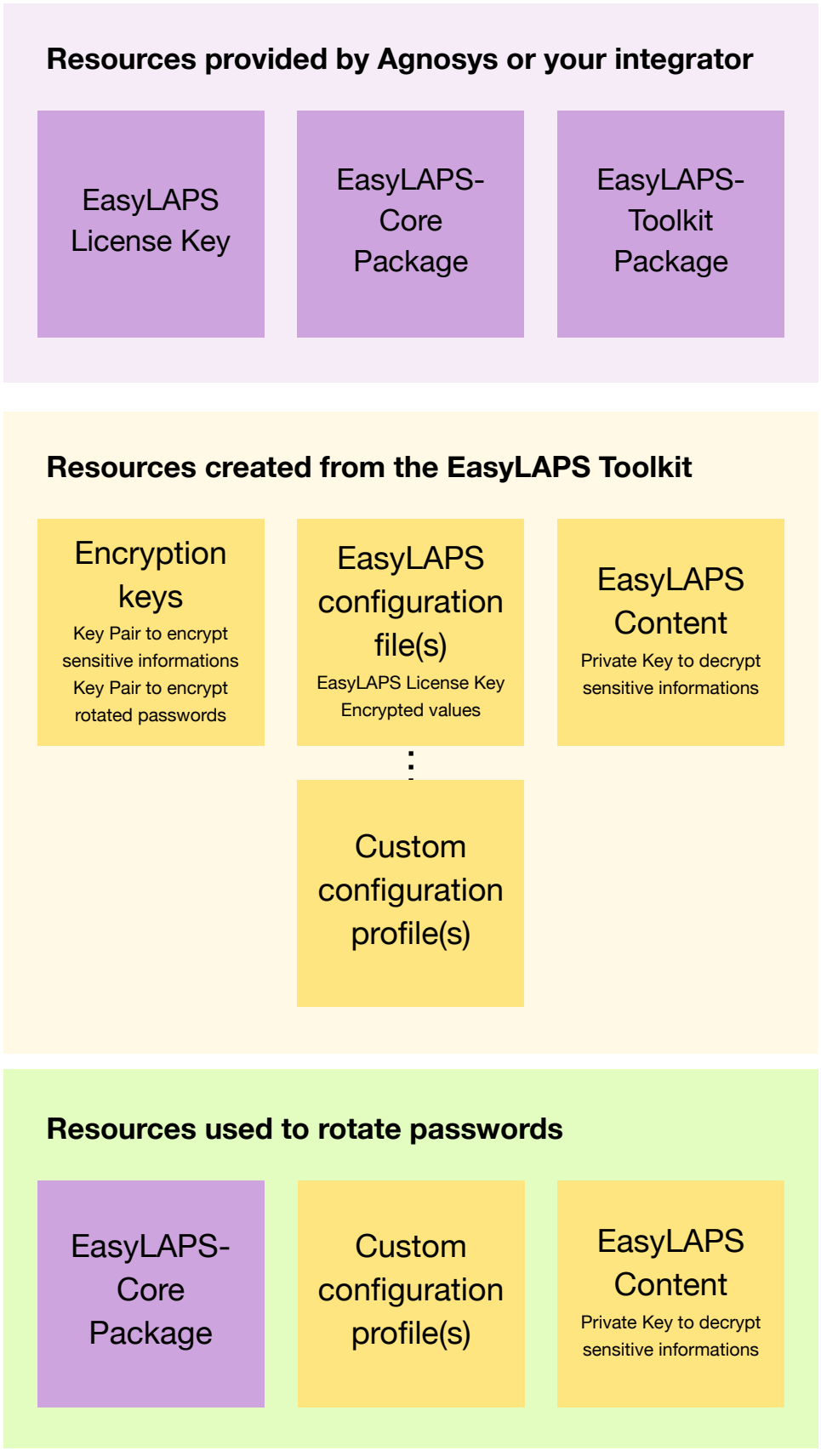
`https://www.agnosys.com/logiciels/easylaps-offers-en/`

Important notice

EasyLAPS is designed with a mechanism that will cancel the rotation if the password written to the MDM (either in encrypted form or in clear text) cannot be validated by a reread and match process. However, it remains recommended to enable FileVault on computers running EasyLAPS. In the event of an highly unexpected incident, it will then be possible to revert manually the local administrator account password to a default one that will then be rotated.

Synopsis

Resources overview



Implementation workflow

Step	Chapter in this document
Get an EasyLAPS License Key	Software requirements
Download the EasyLAPS-Core Package	
Download the EasyLAPS-Toolkit Package	
Install the Packages app	
Install a Property List editor	
Install the EasyLAPS-Toolkit	EasyLAPS Toolkit installation
Create the encryption keys	Encryption keys creation
Customize the EasyLAPS configuration file	EasyLAPS configuration file edition
Create other EasyLAPS configuration files if necessary	
Convert configuration files to Custom configuration profiles	
Build (and sign) the EasyLAPS-Content package	EasyLAPS Content building
Provision the MDM for Background Item Management	Configuration profiles requirements
Provision the MDM with EasyLAPS components	Provisioning *MDM*
Observe the result of a successful rotation	
Display a password stored in encrypted form in MDM	Revealing an encrypted password
Renewing the license code (once every year)	Renewing EasyLAPS license
Updating EasyLAPS to a newer version (year-round)	Updating EasyLAPS
Enable logging and display logs	Troubleshooting
Run a rotation manually	
Learn more about error codes	

EasyLAPS logics

EasyLAPS offers two functioning logics and is designed to manage transparently a change between the two.

You may find that neither of these two logics fits perfectly your security requirements, specifically in highly regulated environments. The main purpose of EasyLAPS remains to have unique passwords on a Mac fleet which are centralized in the MDM console. If you know what should be improved in EasyLAPS after seeing the product in action so this last fits your requirement, please feel free to share your ideas with Franck Sartori (francks) on the EasyLAPS Slack community, publicly or privately.

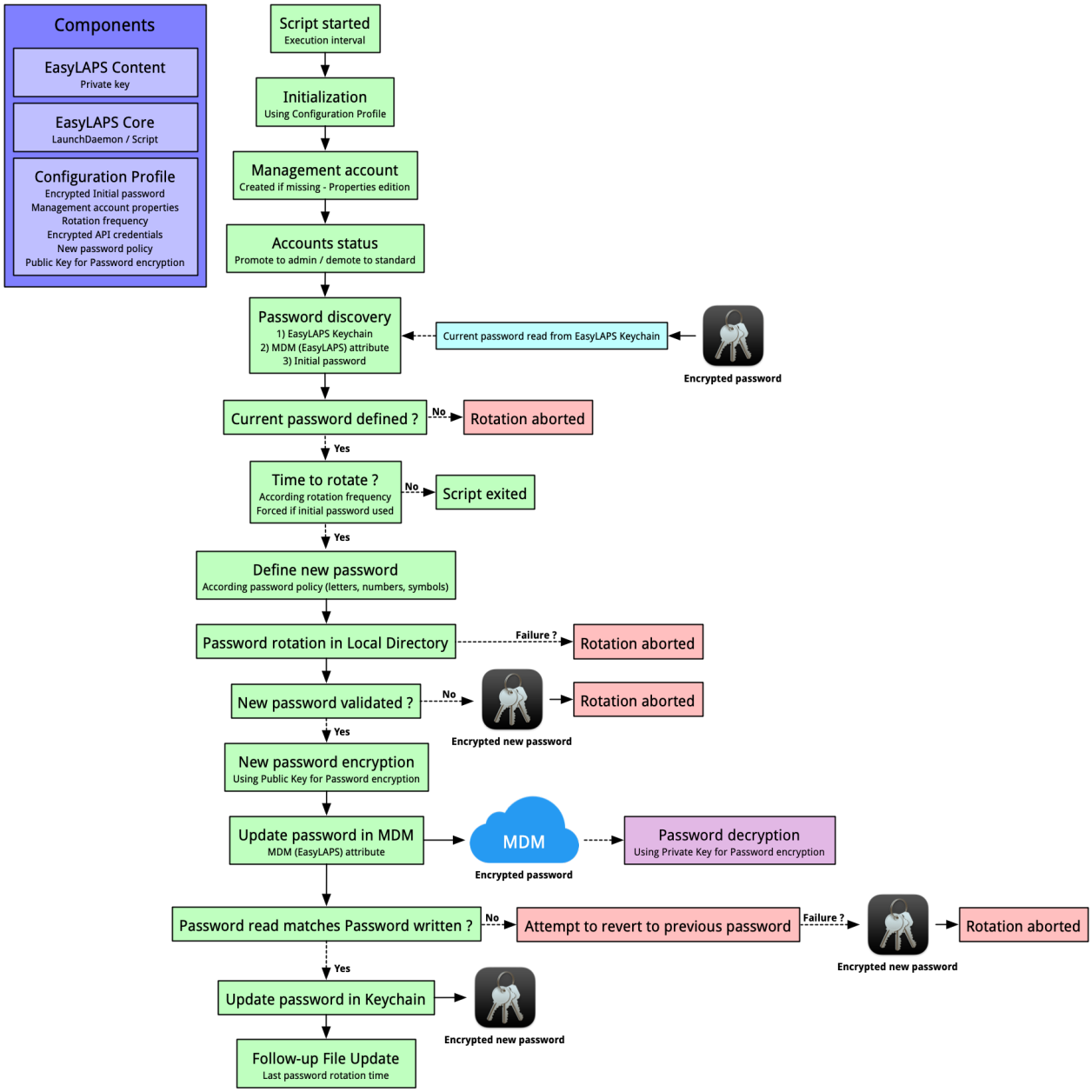
Logic #1 or Logic #2 can be enabled anytime due to the failover to the other logic planned at the "Define current password" step in the following diagrams.

The Key pair used to encrypt and decrypt values in the Configuration Profiles and new password for Logic #1 are generated by the customer and therefore unknown by the vendor.

Logic #1

Logic 1 - Password Discovery mode 1 (recommended)

Password stored in encrypted form in MDM
Password always stored in EasyLAPS Keychain



The password is stored in encrypted form in the MDM and in the EasyLAPS Keychain. EasyLAPS uses the locally stored password as the current password to manage the rotation to the new generated one which is then written in the MDM. The public key used for the encryption is part of the EasyLAPS configuration file. The private key is not present on the device and must be kept in restricted access.

This logic fits best when a large number of technicians have access to the MDM console and only those who own a copy of the EasyLAPS-Toolkit with the private key can reveal a rotated password.

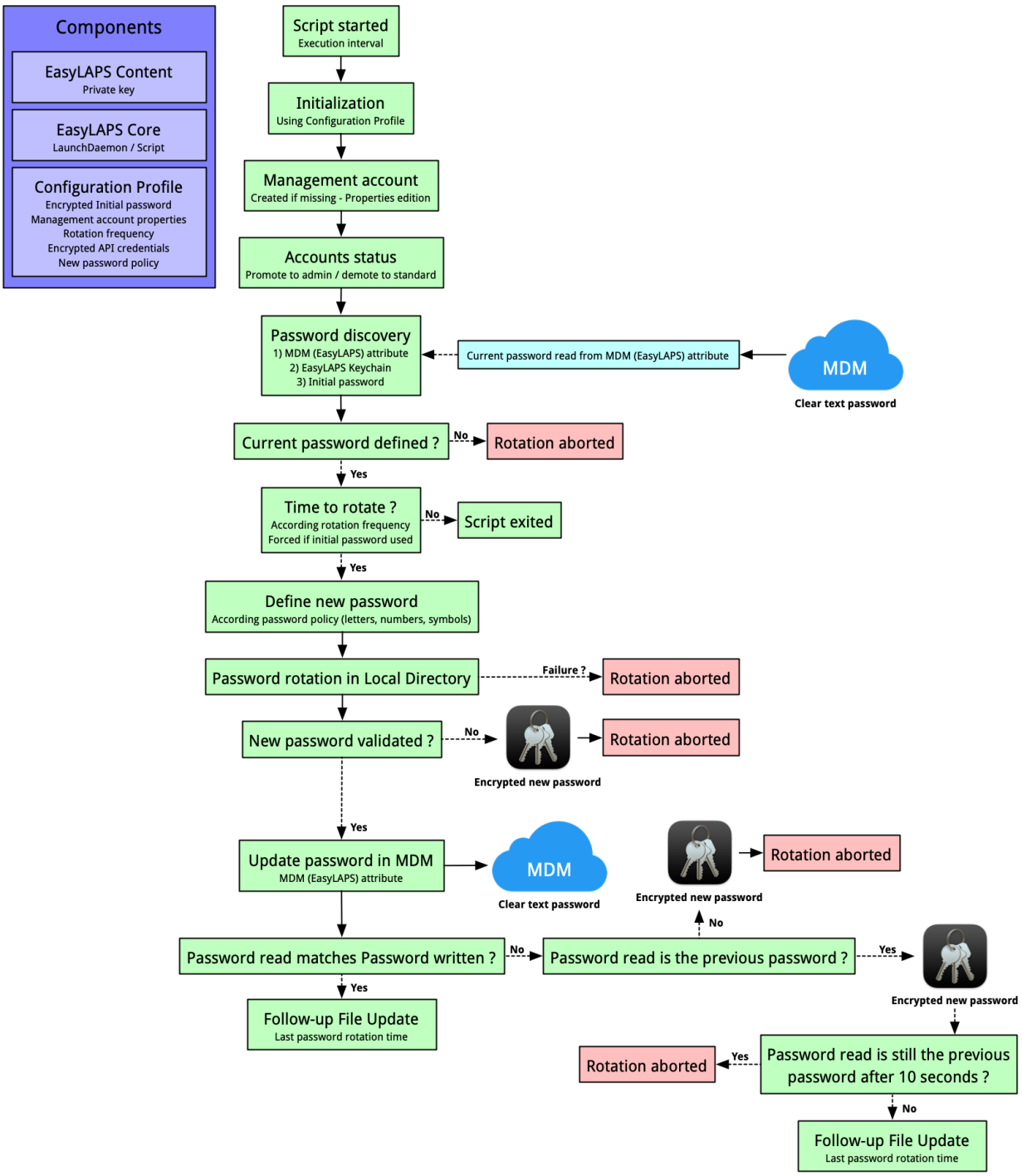
When the new password fails to be updated in the MDM, a password reversion to the previous one is triggered so the management account password continues to match the password stored in MDM. If this reversion fails, most of the time because it is prevented by a password policy, there will be a mismatch between the management account password and the password stored in the MDM. This mismatch will be solved at the next rotation as the management account password is always stored in encrypted form in the EasyLAPS Keychain. Expecting the next rotation is successful, the password stored in MDM will be the correct one at the next EasyLAPS execution.

To activate this logic, the MDMPASSWORDENCRYPTIONKEY key **must be configured** in the EasyLAPS configuration file. The "public key" placeholder must therefore be replaced by a public key generated with the "easylaps_rsa_keygen_passwd" script as explained in this document.

Logic #2

Logic 2 - Password Discovery mode 1 (recommended)

Password stored in clear text form in MDM
Password not stored in EasyLAPS Keychain unless a rotation issue occurs



The password is stored in clear text in the MDM and is not stored in the EasyLAPS Keychain unless a rotation issue occurs. EasyLAPS reads the password stored in the MDM and uses it as the current password to manage the rotation to the new generated one which is then written in the MDM.

The logic fits best when a restricted number of technicians have access to the MDM console and then are able to reveal a rotated password.

When the new password fails to be updated in the MDM, the management account password is temporarily stored in encrypted form in the EasyLAPS Keychain. Expecting the next rotation is successful, the password stored in MDM will be the correct one at the next EasyLAPS execution.

To activate this logic, the MDMPASSWORDENCRYPTIONKEY key **must be deleted** in the EasyLAPS configuration file. Please note that the only presence of this key, even with an empty value, will trigger the activation of Logic #1.

Software requirements

macOS

EasyLAPS requires macOS 10.13.4 and later.

EasyLAPS packages

Download (only) the following packages from this URL :

https://www.dropbox.com/sh/x5tn8u3gpokotgc/AAAaygDDf-ZWzT-ni7csZ4KOa?dl=0

- EasyLAPS-Core-*version*.pkg

- EasyLAPS-Toolkit-*version*.pkg

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

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

Packaging editor

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

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

Property List editor

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

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

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

Text Editor

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

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

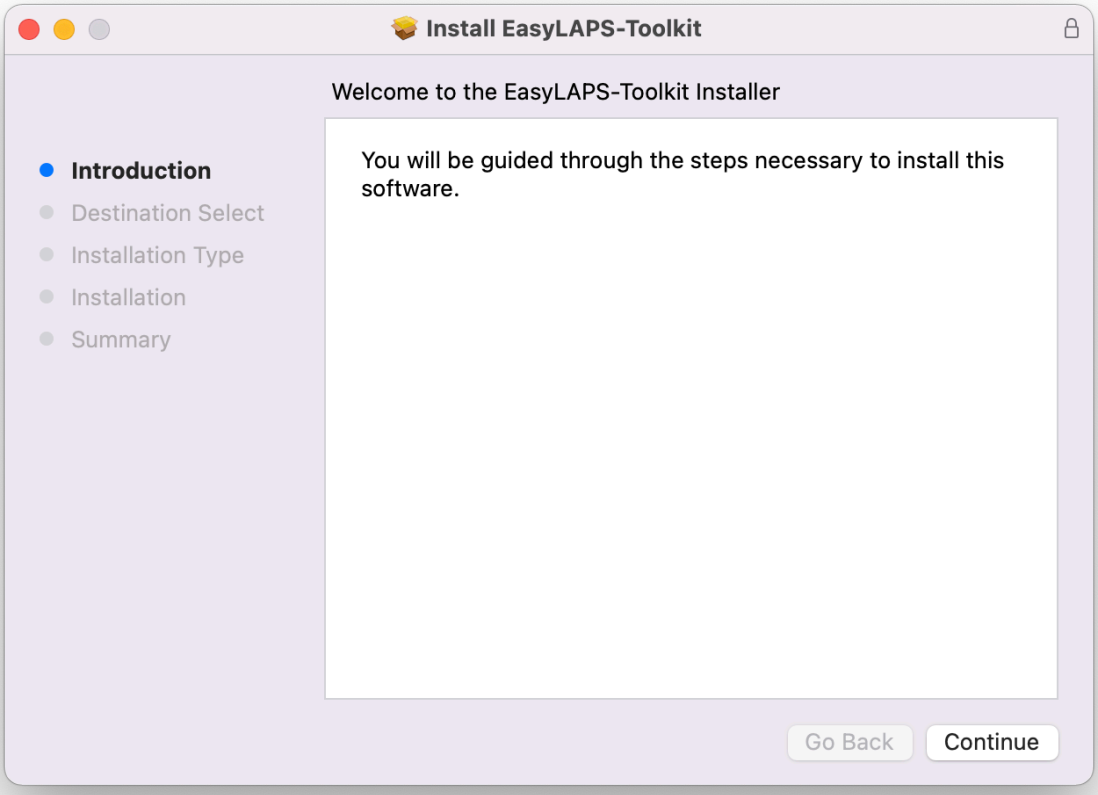
VMware Workspace ONE Admin Assistant

If the MDM solution is VMware Workspace ONE, download and install this tool :

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

EasyLAPS Toolkit installation

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



Enter your administrator password when prompted.

The "EasyLAPS-Toolkit" folder is created in /Users/Shared. It contains the following subfolders :
- easylaps_configs
- easylaps_content
- easylaps_library
- easylaps_secrets

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

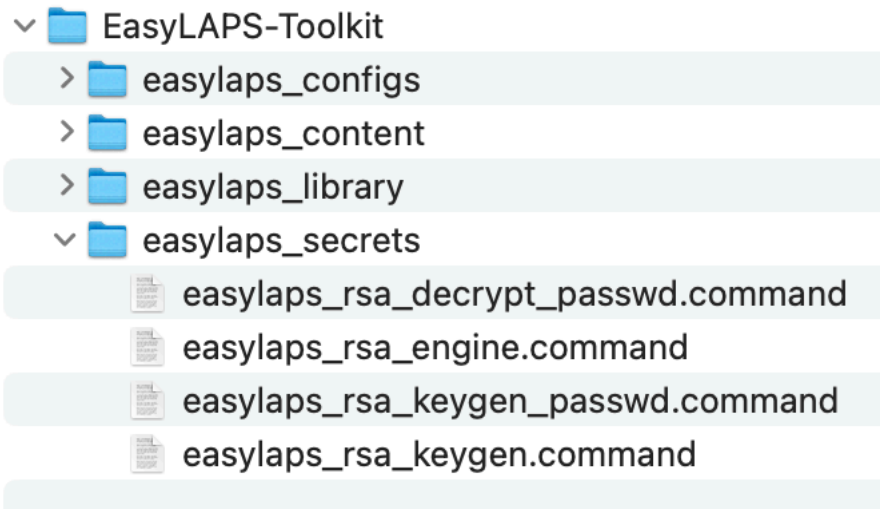
Do not modify the content of the "EasyLAPS-Toolkit" folder unless instructed to do so for specific items.

Encryption keys creation

EasyLAPS uses two private / public key pairs :
- one pair recommanded to encrypt the sensitive informations in an EasyLAPS Property List
- one pair required only if you want to encrypt the rotated passwords stored in the MDM.

Key pair to encrypt the sensitive informations in an EasyLAPS Property List

Sensitive informations in an EasyLAPS Property List are protected from direct observation using a RSA encryption method :
- a private / public key pair is created with the "easylaps_rsa_keygen" script
- the public key is used when encrypting a value with the "easylaps_rsa_engine" script
- the private key is used by EasyLAPS to decrypt locally the encrypted values
- the private key is automatically embedded in the EasyLAPS-Content package.

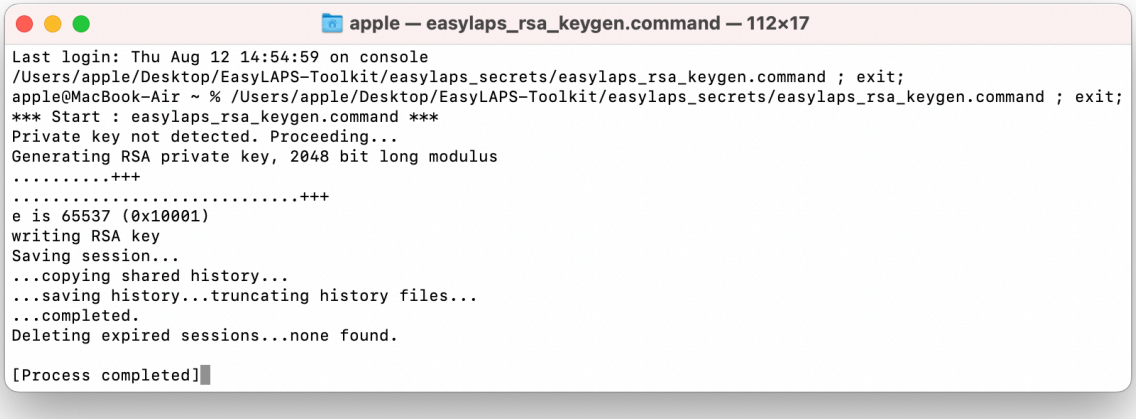


Open the "EasyLAPS-Toolkit" folder.

Open the "easylaps_secrets" subfolder.

Execute the "**easylaps_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 EasyLAPS integration lifetime.



The private / public key pair is created at the following path :
EasyLAPS-Toolkit > easylaps_secrets > easylaps_rsa_key.pri and easylaps_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 EasyLAPS-Content package.

The private key is automatically copied at the following path :
EasyLAPS-Toolkit > easylaps_content > Content > easylaps_rsa_key.pri

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

Key pair to encrypt the rotated passwords stored in the MDM

This section only applies if the activation of Logic #1 is planned.

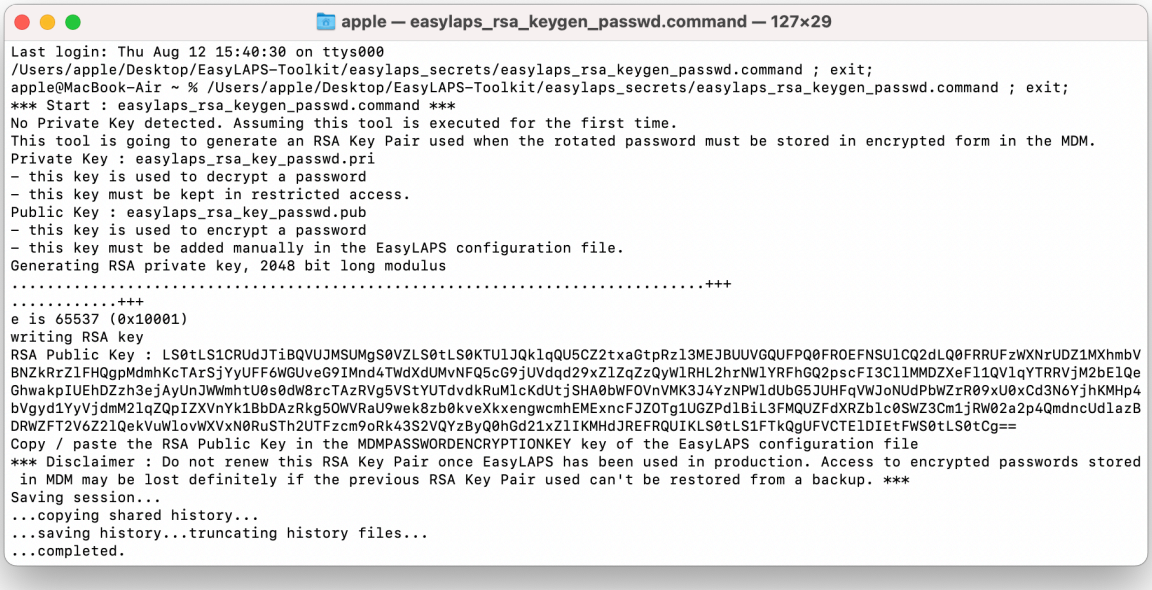
Rotated passwords stored in MDM can be protected from direct observation (aka not displayed as clear text) using a RSA encryption method :
- a private / public key pair is created with the "easylaps_rsa_keygen_passwd" script
- the public key is used by EasyLAPS to encrypt the password before storing it in MDM
- the private key is used when decrypting a password with the "easylaps_rsa_decrypt_passwd" script.

Open the "EasyLAPS-Toolkit" folder.

Open the "easylaps_secrets" subfolder.

Execute the "**easylaps_rsa_keygen_passwd**" 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 EasyLAPS integration lifetime.



Do not close this window that displays the encoded RSA Public Key which will be used in the next chapter to populate the MDMPASSWORDENCRYPTION key.

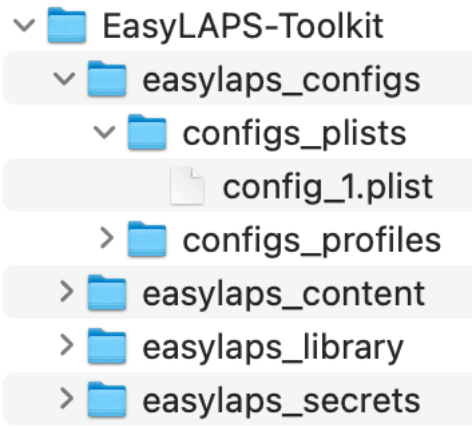
The private / public key pair is created at the following path :
EasyLAPS-Toolkit > easylaps_secrets > easylaps_rsa_key_passwd.pri and easylaps_rsa_key_passwd.pub

If you inadvertently closed the window, execute the "**easylaps_rsa_keygen_passwd**" script to display the encoded RSA Public Key again.

EasyLAPS configuration file edition

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

Access to the configuration file template



Open the "EasyLAPS-Toolkit" folder.

Open the "easylaps_configs" subfolder.

Open the "configs_plists" subfolder.

Open the "config_1.plist" property list with you favorite editor.

Reference for configuration file keys

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

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

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

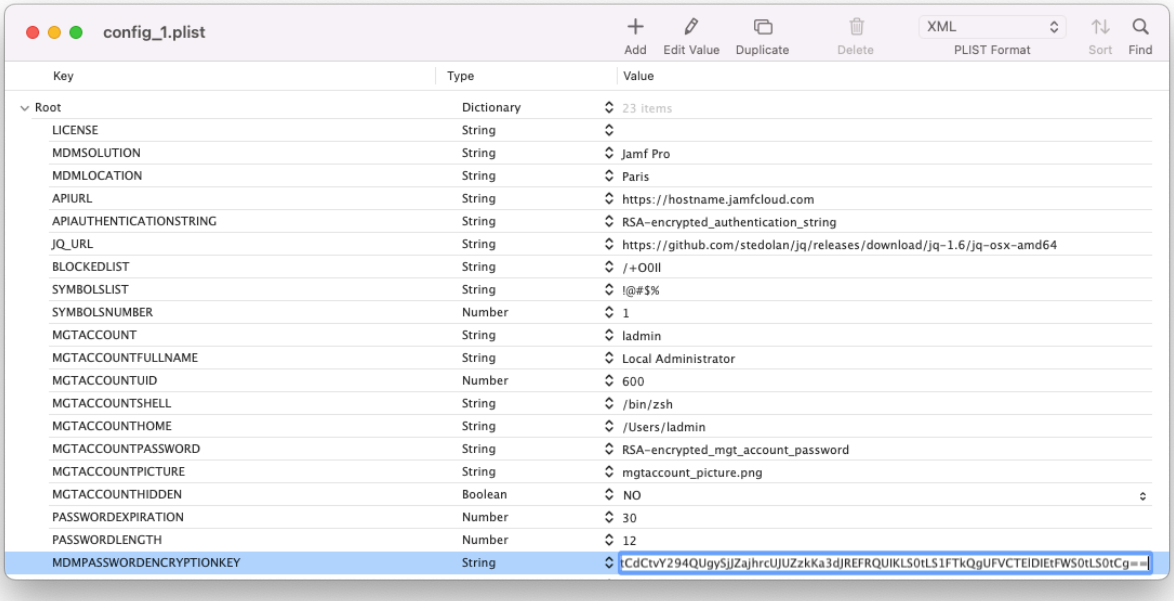
Please do not forget to delete the MDMPASSWORDENCRYPTION key if the activation of Logic #2 is planned.

Public key to encrypt the rotated passwords stored in the MDM

This section only applies if the activation of Logic #1 is planned.

You should start with this key considering it is currently displayed in the still opened Terminal window.

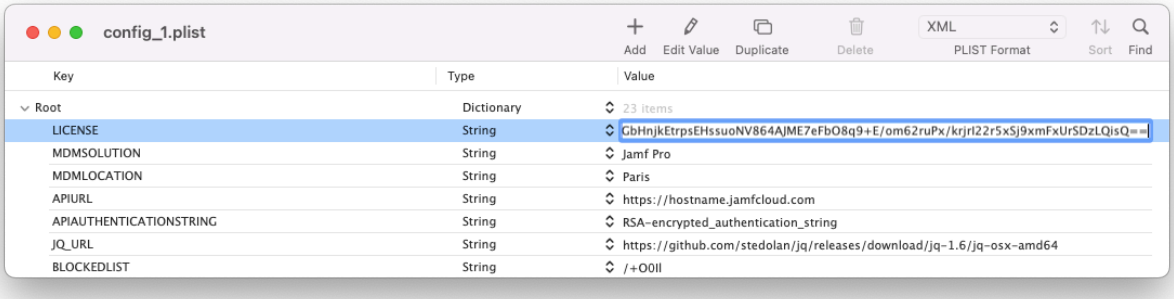
Copy the encoded RSA Public Key (one-line string ending exactly with two "=" characters) from the Terminal window.



Paste the encoded RSA Public Key in the MDMPASSWORDENCRYPTION key.

Select File > Save and then you can safely close the Terminal window.

License key



Paste the EasyLAPS license key in the LICENSE key.

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

Management account keys

The expected starting situation is that the devices already have the management account defined by the management account keys of the EasyLAPS configuration file.

When EasyLAPS is executed, it detects the existence of the targeted management account.

If the management account does exist, it is eventually updated for the MGTACCOUNTFULLNAME, MGTACCOUNTSHELL, MGTACCOUNTPICTURE and MGTACCOUNTHIDDEN keys.

If the management account does not exist, it is created according the complete set of the management account keys which are MGTACCOUNT, MGTACCOUNTFULLNAME, MGTACCOUNTUID, MGTACCOUNTSHELL, MGTACCOUNTHOME, MGTACCOUNTPASSWORD, MGTACCOUNTPICTURE and MGTACCOUNTHIDDEN keys.

The MGTACCOUNT key must contain the local administrator account name (short name) whom password will be rotated. For example, if the password of the account "sysadmin" must be rotated, use exactly "sysadmin" for this key.

The MGTACCOUNTFULLNAME key must contain the local administrator account full name. When the rotation occurs, if the current full name of the local administrator account is not the value of this key, the value of this key will replace the current full name of the local administrator account, so all local administrator accounts share the same full name.

The MGTACCOUNTUID key can be left to the example value of 600. This key is only used when EasyLAPS creates the targeted local administrator account.

The MGTACCOUNTSHELL key can be left to the recommended value of "/bin/zsh" which is the default Shell for new local accounts since macOS 10.15. When the rotation occurs, if the current Shell of the local administrator account is not the value of this key, the value of this key will replace the current Shell of the local administrator account, so all local administrator accounts share the same Shell.

The MGTACCOUNTHOME key contains the path to the local administrator account home folder. This key is only used when EasyLAPS creates the targeted local administrator account.

The MGTACCOUNTPASSWORD key must contain the local administrator account password as it is currently. The password must be the existing password, therefore it cannot be an empty string or an arbitrary string as EasyLAPS requires to know the current password to rotate it. By design, EasyLAPS changes known passwords and never resets unknown passwords. Please do not miss to read the "Password complexity" and "Initial password of the local administrator account" sections below that give more details about this password and its encryption.

The MGTACCOUNTPICTURE key must contain the name of the file included in the EasyLAPS Content that defines the local administrator account picture. When the rotation occurs, if no custom picture has been already set, the defined picture will be used, so all local administrator accounts share the same picture.

The MGTACCOUNTHIDDEN key defines the visibility of the local administrator account. When the rotation occurs, the account will be made invisible if the key is set to "true", and visible if the key is set to "false", whatever the previous visibility status was.

Password policy

If a local account password policy has been defined to meet your organization's requirements, often enforced via a Passcode Configuration profile, please pay attention to the following points.

• When defining a new password, EasyLAPS generates a long string containing random letters and digits. Then the characters defined in the BLOCKEDLIST key are stripped from this string and this last is cut according to the PASSWORDLENGTH key. Eventually, the number of symbols defined by the SYMBOLSNUMBERMAX and SYMBOLSNUMBERMIN keys, chosen at random in the SYMBOLSLIST key, substitute characters chosen at random in the cut string.

• The BLOCKEDLIST key, the SYMBOLSLIST key and both SYMBOLSNUMBERMAX and SYMBOLSNUMBERMIN keys are optional.

• The substitution is triggered when the SYMBOLSLIST value is not set to "undefined" and the SYMBOLSNUMBERMAX value is greater than 0.

• The SYMBOLSNUMBERMIN value can be equal as the SYMBOLSNUMBERMAX value to set a fixed number of symbols. The SYMBOLSNUMBERMAX value is automatically set to the PASSWORDLENGHT value if the former is greater than the latter. The SYMBOLSNUMBERMIN value is automatically set to the SYMBOLSNUMBERMAX value if the former is greater than the latter, or if it is equal to 0.

• As defined in the EasyLAPS logics section, failures may trigger the reversion of the management account password to the previous one. In case this reversion fails because a password history is set to prevent the reuse of previous passwords, the new password is stored in encrypted form in the EasyLAPS Keychain, which is the expected behaviour for Logic #1 but an exception for Logic #2.

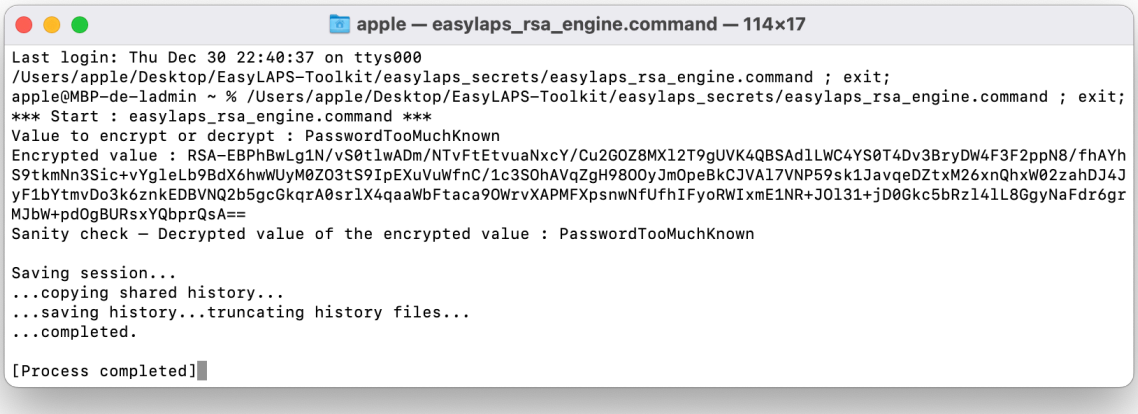
• EasyLAPS creates the management account defined in the configuration file if it is detected as missing at the time of the rotation (normally the first one). In this context, the initial password of the management account before it is rotated is the password defined in the MGTACCOUNTPASSWORD key. **This password must therefore comply with the local account password policy.** In case this compliance is not respected, the management account creation will fail and the rotation will be aborted.

Initial password of the local administrator account

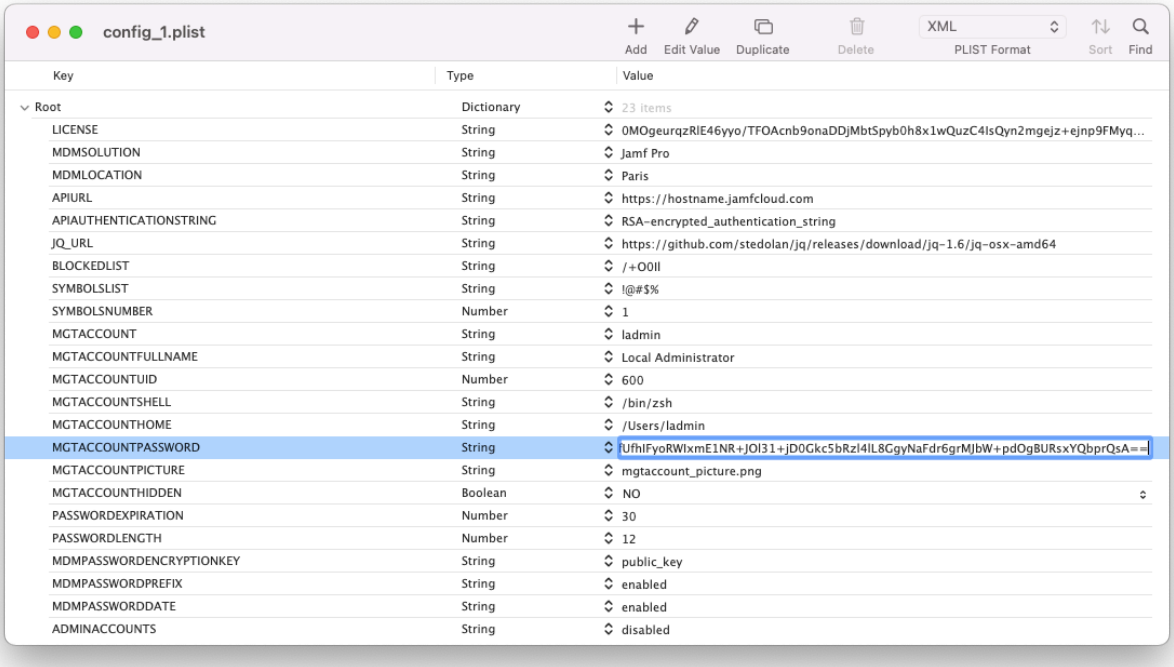
This password will normally be used only for the first rotation. Then the current password will be read from the local password file or from the MDM depending of the logic chosen.

To generate the value, follow these instructions :
- open the "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder

- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- enter the initial password of the local administrator account



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



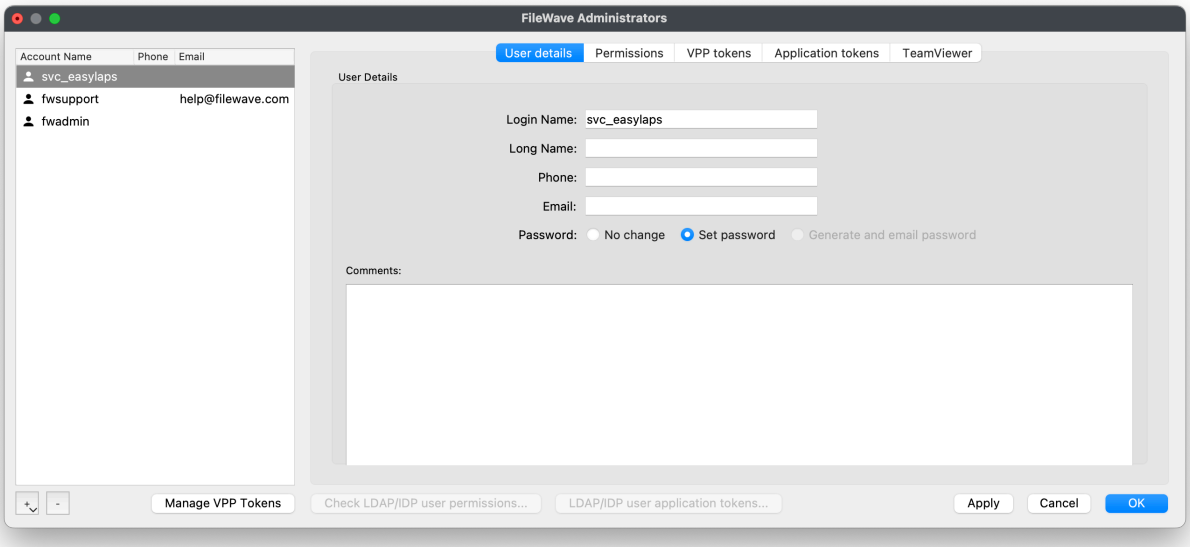
Paste the encrypted password in the MGTACCOUNTPASSWORD key.

FileWave : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is FileWave.

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

FileWave Admin > Assistants > Manage Administrators > + Local Account



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

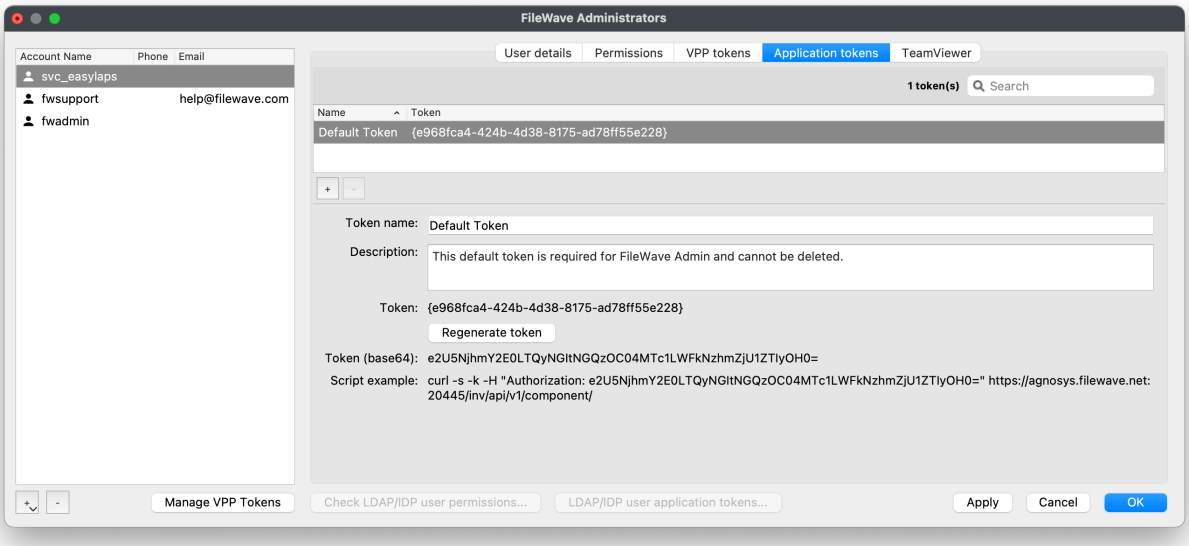
Select "Permissions".

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

The Custom Field "EasyLAPS" (exactly) should be created manually before EasyLAPS is deployed. However, EasyLAPS can create this Custom Field (and other Custom Fields required for Immediate reporting) when detected as missing if the account has this supplemental permission :

- Modify Custom Fields

No other permission should be granted to the account.



Select "Application tokens".

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

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

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).

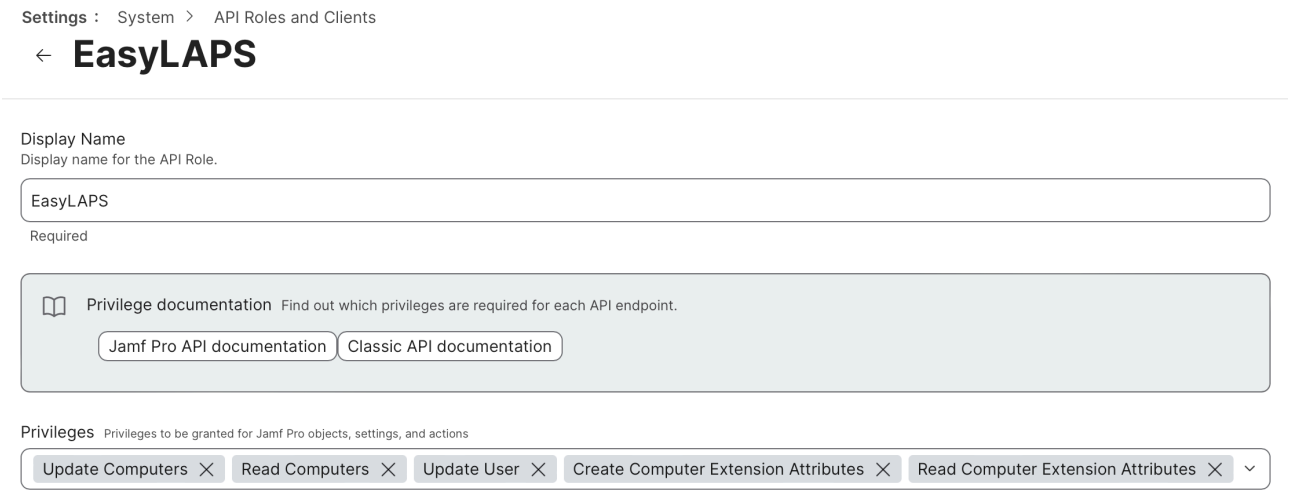
The key will be used by EasyLAPS to make API calls.

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

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

First create a new role with limited API privileges.

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



Enter a name like "EasyLAPS".

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

Warning : Omitting the Update User privilege will result in the error "Password read from MDM does not match password written in MDM." in the debug log and in the trace log.

The Computer Extension Attribute "EasyLAPS" (exactly) should be created manually before EasyLAPS is deployed. However, EasyLAPS can create this attribute (and other Extension Attributes required for Immediate reporting) when detected as missing if the Role has this supplemental privilege :

- Create Computer Extension Attributes

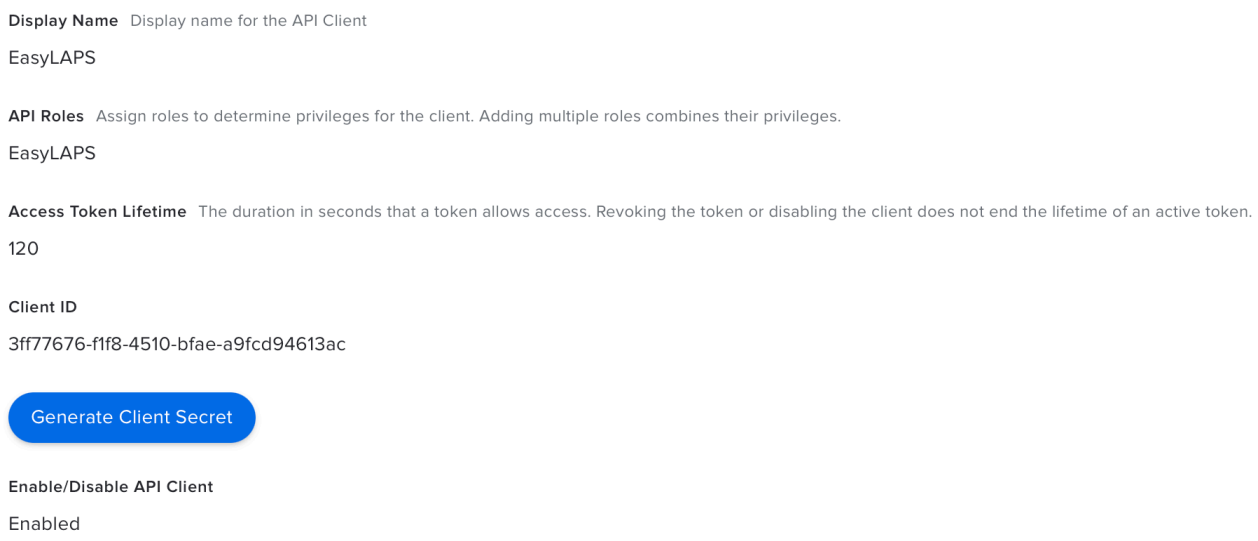
Click on "Save".

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

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

Enter a name like "EasyLAPS", select the EasyLAPS 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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Jamf Pro - User account : APIAUTHENTICATIONSTRING key

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

First create a new Jamf Pro User Account that will be used by EasyLAPS 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

Warning : Omitting the Users - Update privilege will result in the error "Password read from MDM does not match password written in MDM." in the debug log and in the trace log.

All other privileges should be disabled.

The Computer Extension Attribute "EasyLAPS" (exactly) should be created manually before EasyLAPS is deployed. However, EasyLAPS can create this attribute (and other Extension Attributes required for Immediate reporting) when detected as missing if the account has this supplemental privilege :

- Jamf Pro Server Objects

    - Computer Extension Attributes : Create

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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Jamf School : APIAUTHENTICATIONSTRING key

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

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

Go to School > Settings > API. Click on "Add API Key" and enter "EasyLAPS" 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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

JumpCloud : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is JumpCloud.

First create a new JumpCloud Administrator account whose API Key will be used by EasyLAPS 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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the API Key
- the API Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Meraki Systems Manager : APIAUTHENTICATIONSTRING key

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

First create a new API Key that will be used by EasyLAPS 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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the API Key
- the API Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

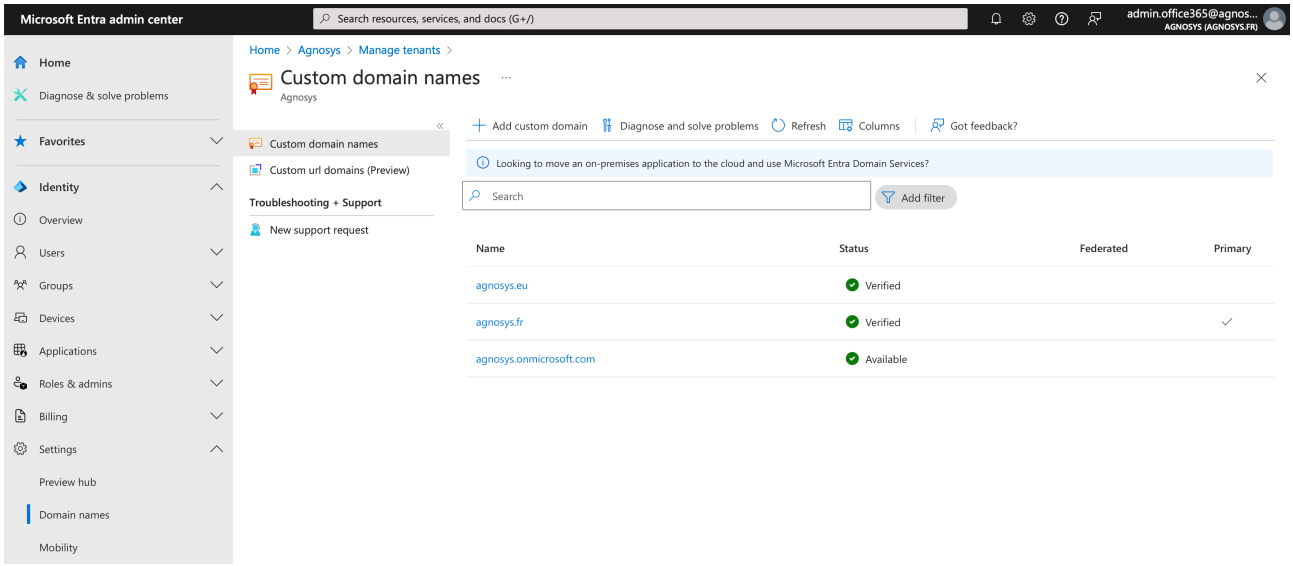
Microsoft Intune : APIAUTHENTICATIONSTRING key

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

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

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

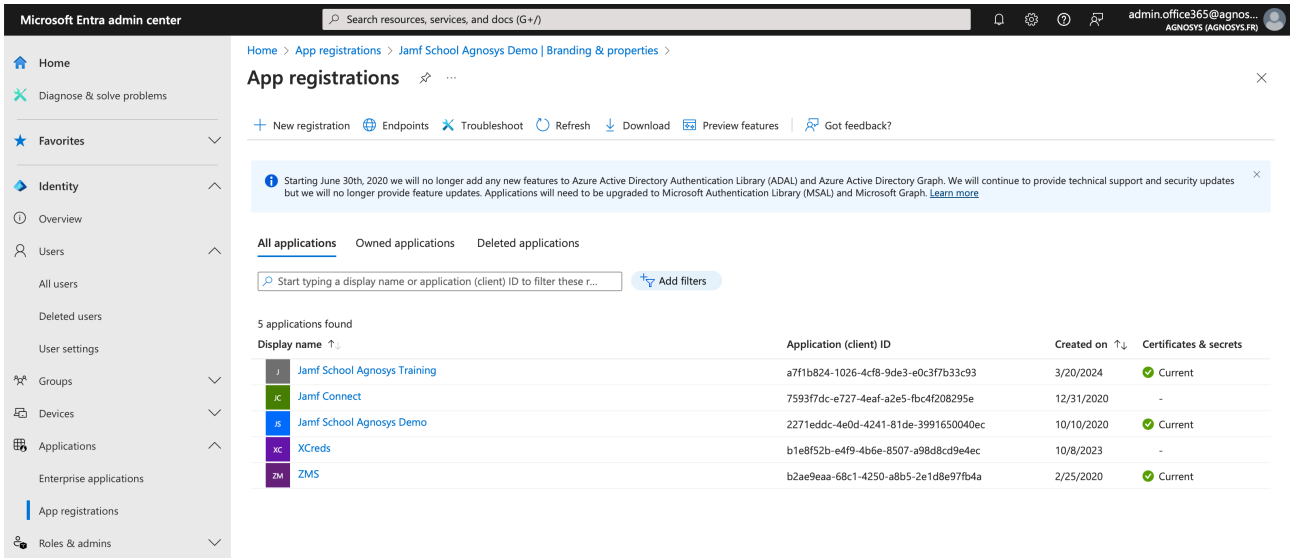
Connect to Microsoft Entra admin center.



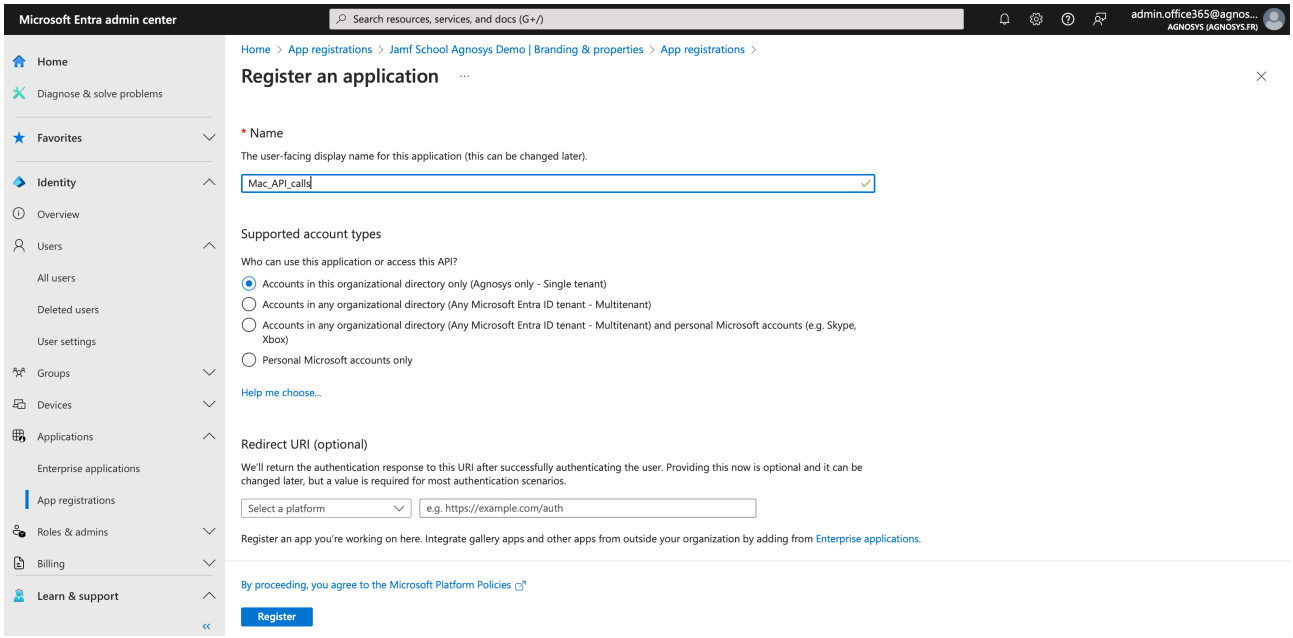
Go to Identity > Settings > Domain names.

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

Go to Identity > Applications > App registrations.



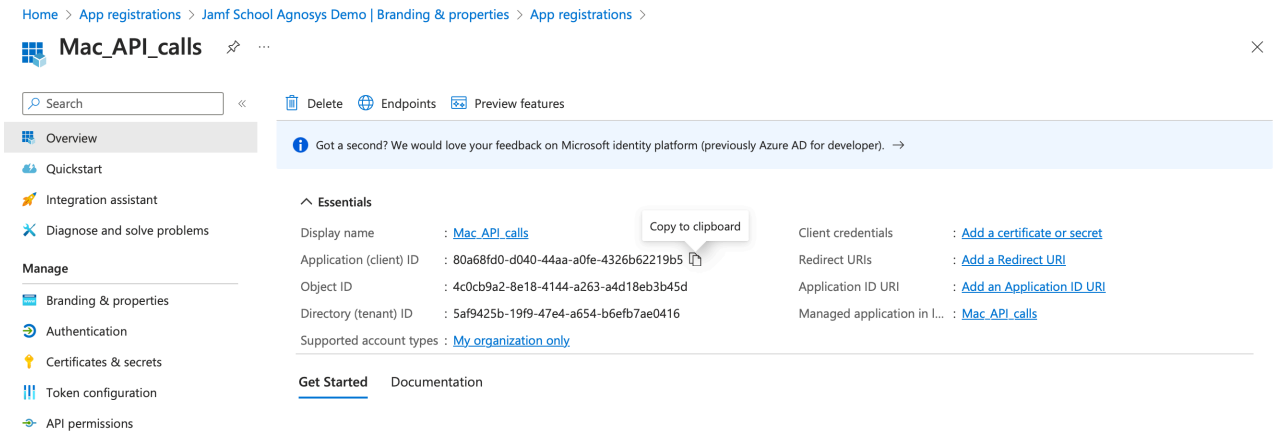
Click on "All applications", then on "New registration".



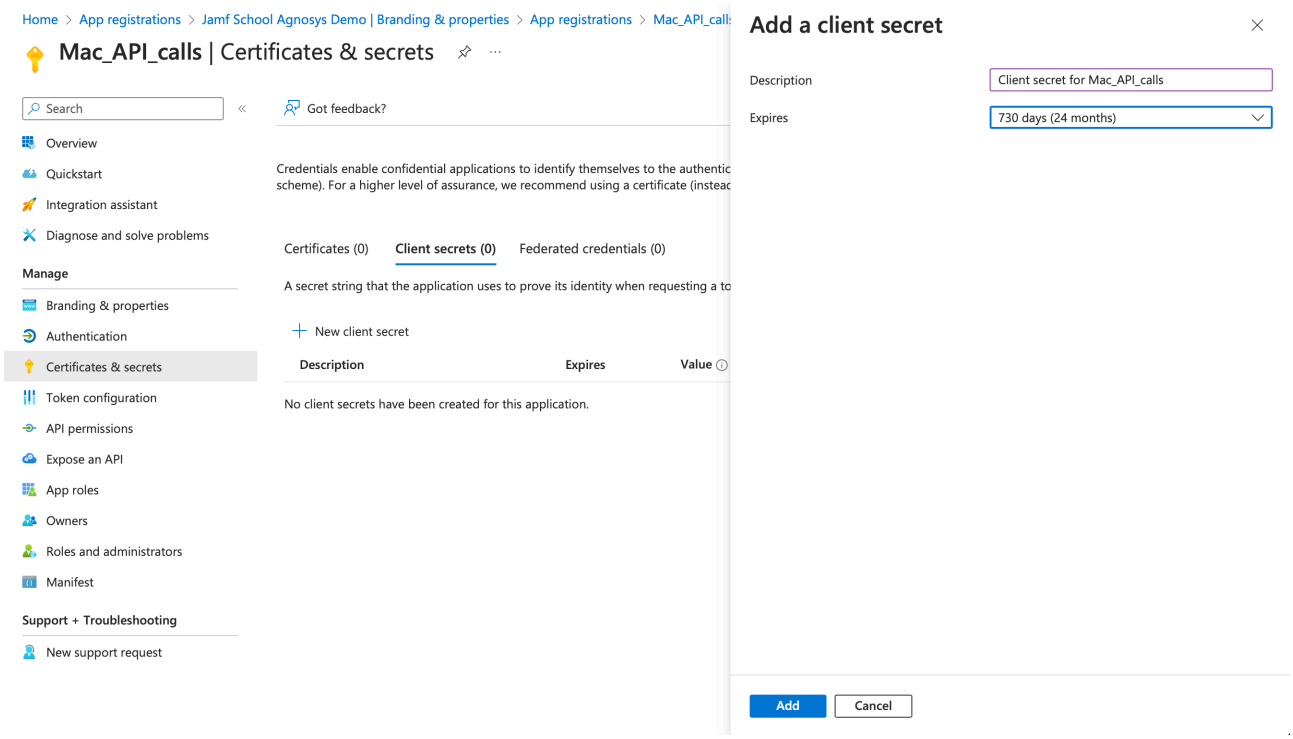
Enter a name for the application.

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

Click on "Register".



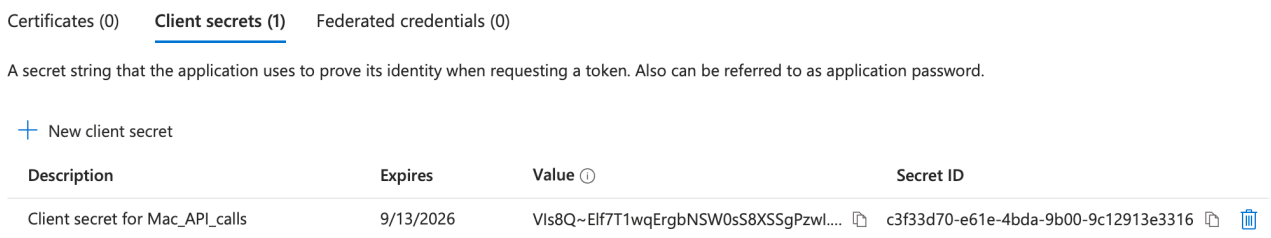
Copy / paste the Application (client) ID in the text document.



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

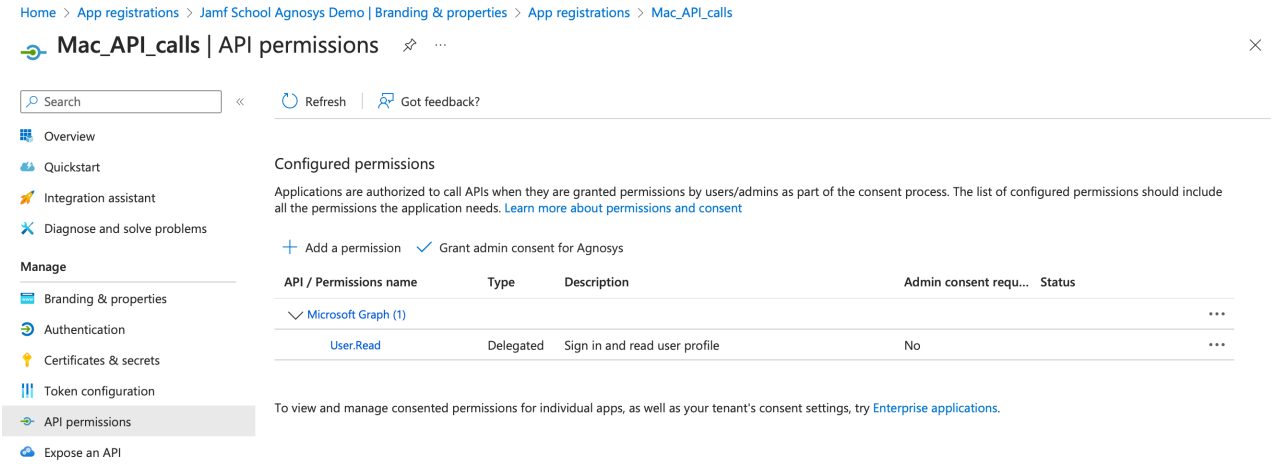
Enter a description and select a life time.

Click on "Add".

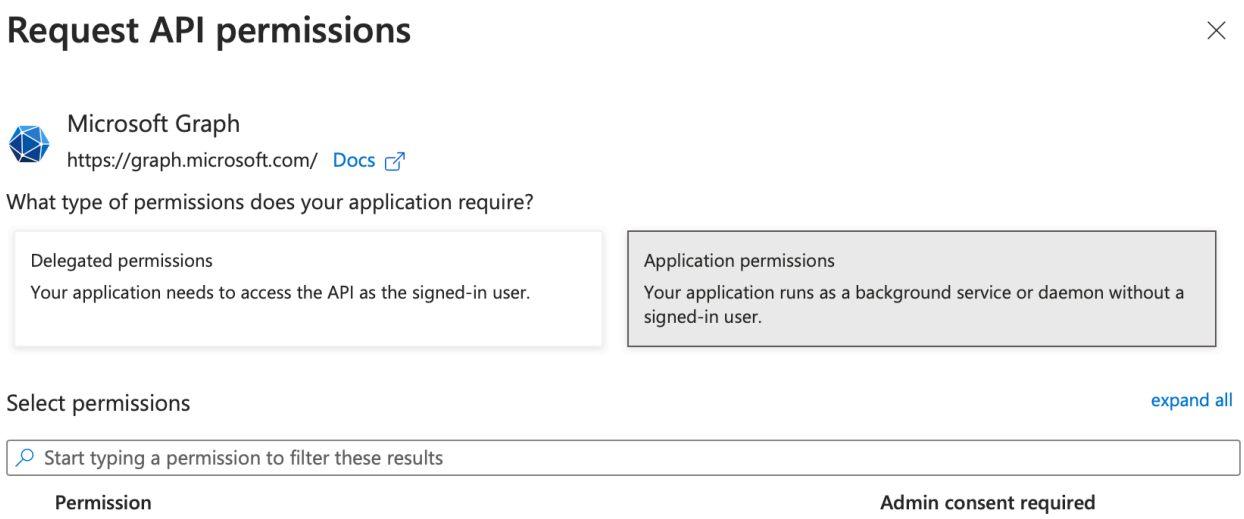


You will see this information **only once**.

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



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

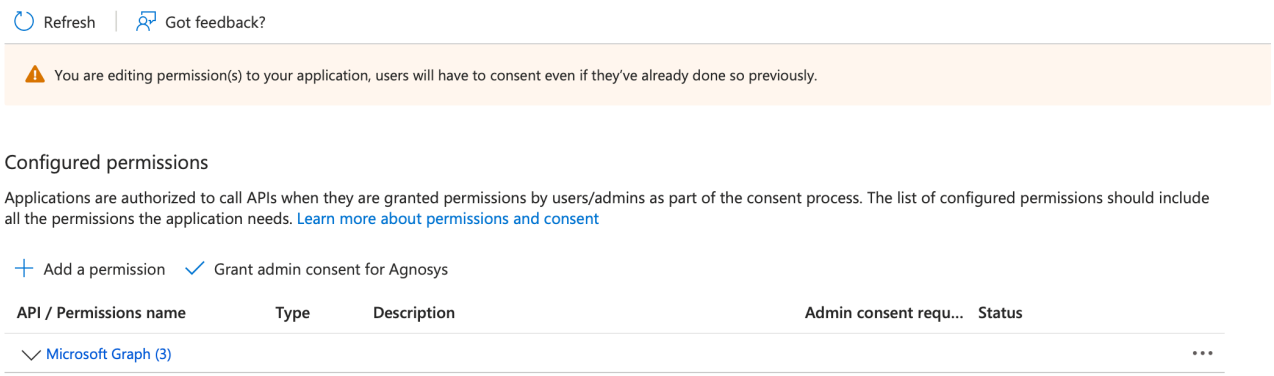


Click on "**Application permissions**".

If the password is to be stored in the device notes, select the following API permissions :
- "DeviceManagementManagedDevices.**ReadWrite**.All"
- "Device.**ReadWrite**.All" **only if** Immediate reporting is configured.

If the password is to be stored in an Extension attribute, select the following API permissions :
- "Device.**ReadWrite**.All"
- "DeviceManagementManagedDevices.**Read**.All".

Click on "Update permissions".



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

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

```
Tenant domain : agnosys.onmicrosoft.com
Application (client) ID : 66974f69-d2be-4b76-9415-2b8863bc3caa
Client secret value : znGafq6e.V4HT.C34kGN0O9-D~ZV_iyetv

agnosys.onmicrosoft.com,66974f69-d2be-4b76-9415-2b8863bc3caa,znGafq6e.V4HT.C34kGN0O9-D~ZV_iyetv
```

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

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Miradore : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is Miradore.

First create a new API key that will be used by EasyLAPS 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 : EasyLAPS
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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the API key
- the API key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted API key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Mosyle Business : APIAUTHENTICATIONSTRING key

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

The key will be used by EasyLAPS 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 : EasyLAPS Role
- Organization > Integrations :
    - API Integration : View - Create

All other privileges should be disabled.

Click on "Save". Back to the "Role Selector", click on "EasyLAPS Role". Check that the new administrator account is limited to the "EasyLAPS 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 "EasyLAPS 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) 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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

Mosyle Manager : APIAUTHENTICATIONSTRING key

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

The key will be used by EasyLAPS 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 : EasyLAPS Role
- My School > Integrations :
    - API Integration : View - Update

All other privileges should be disabled.

Click on "Save". Back to the "Role Selector", click on "EasyLAPS Role". Check that the new administrator account is limited to the "EasyLAPS 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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the concatenated string
- the concatenated string is encrypted, displayed and then decrypted for sanity check
- copy the encrypted concatenated string (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

SimpleMDM : APIAUTHENTICATIONSTRING key

This section only applies if the management solution is SimpleMDM.

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

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

Select the following permissions :

- Custom Attributes : Write

- Devices : Read

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 "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the Secret Access Key
- the Secret Access Key is encrypted, displayed and then decrypted for sanity check
- copy the encrypted Secret Access Key (one-line string ending exactly with two "=" characters).

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

VMware Workspace ONE - OAuth authentication : APIAUTHENTICATIONSTRING key

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

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

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

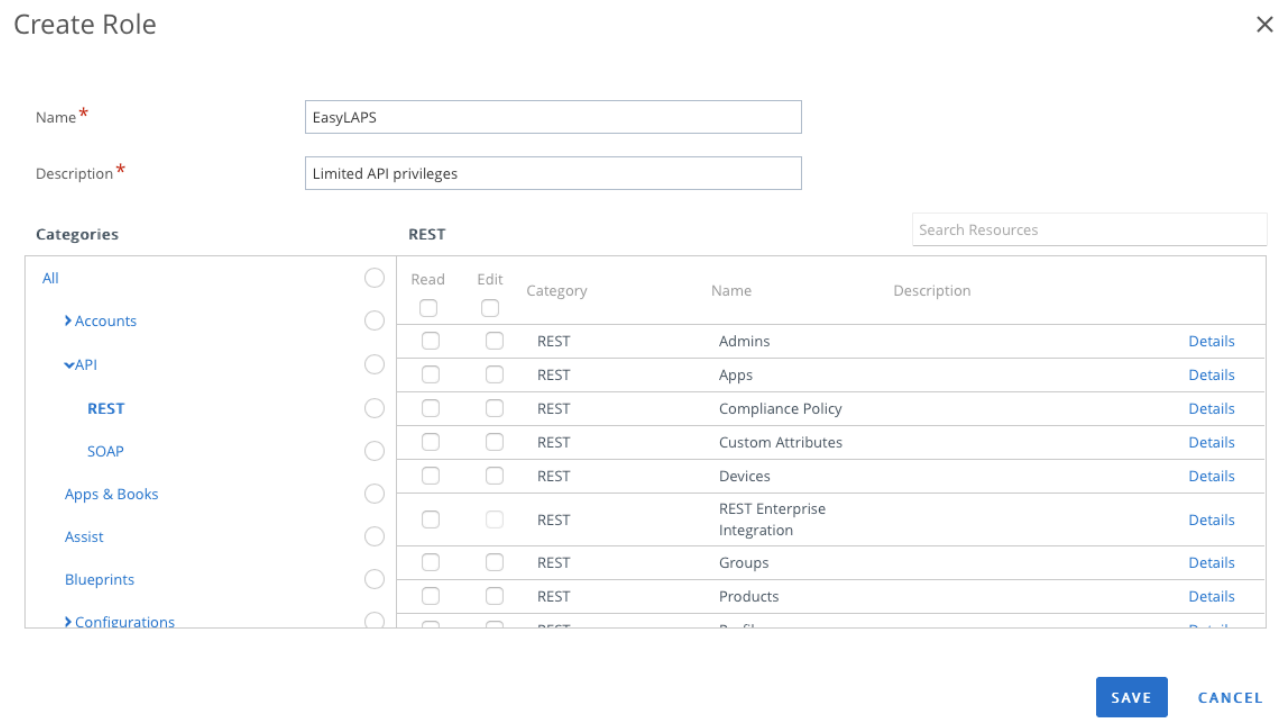
To define the Token URL, please consult this article :

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".



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

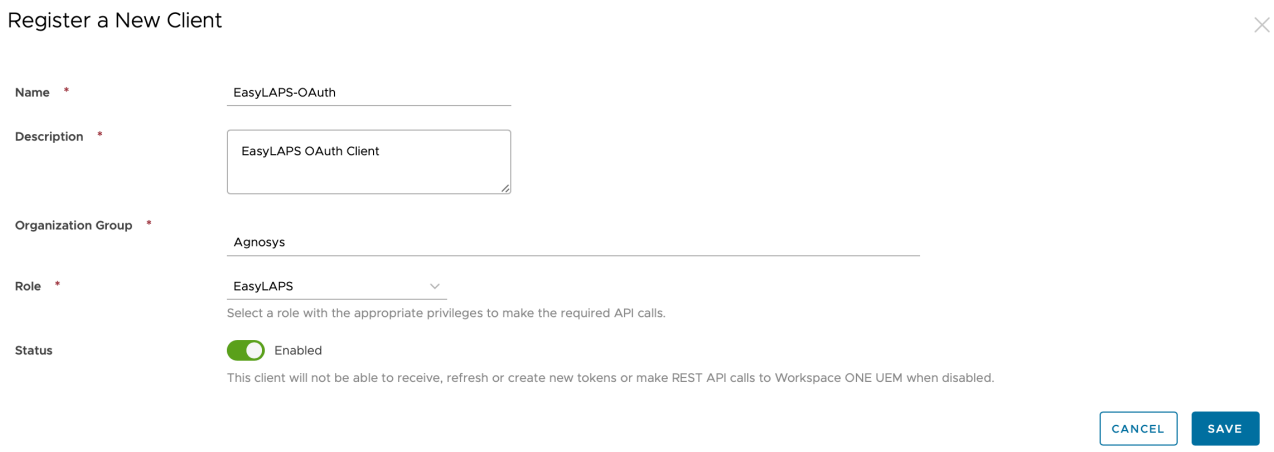
The role requires the following set of privileges :

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

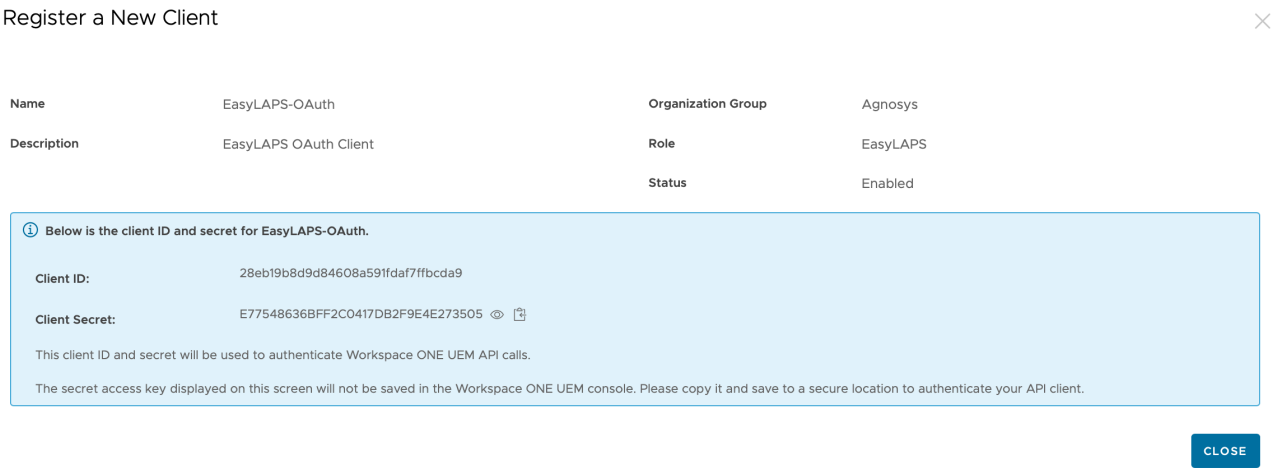
Click on "Save".

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

Click on "Add".



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



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

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

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

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

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

VMware Workspace ONE - Basic authentication : APIAUTHENTICATIONSTRING key

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

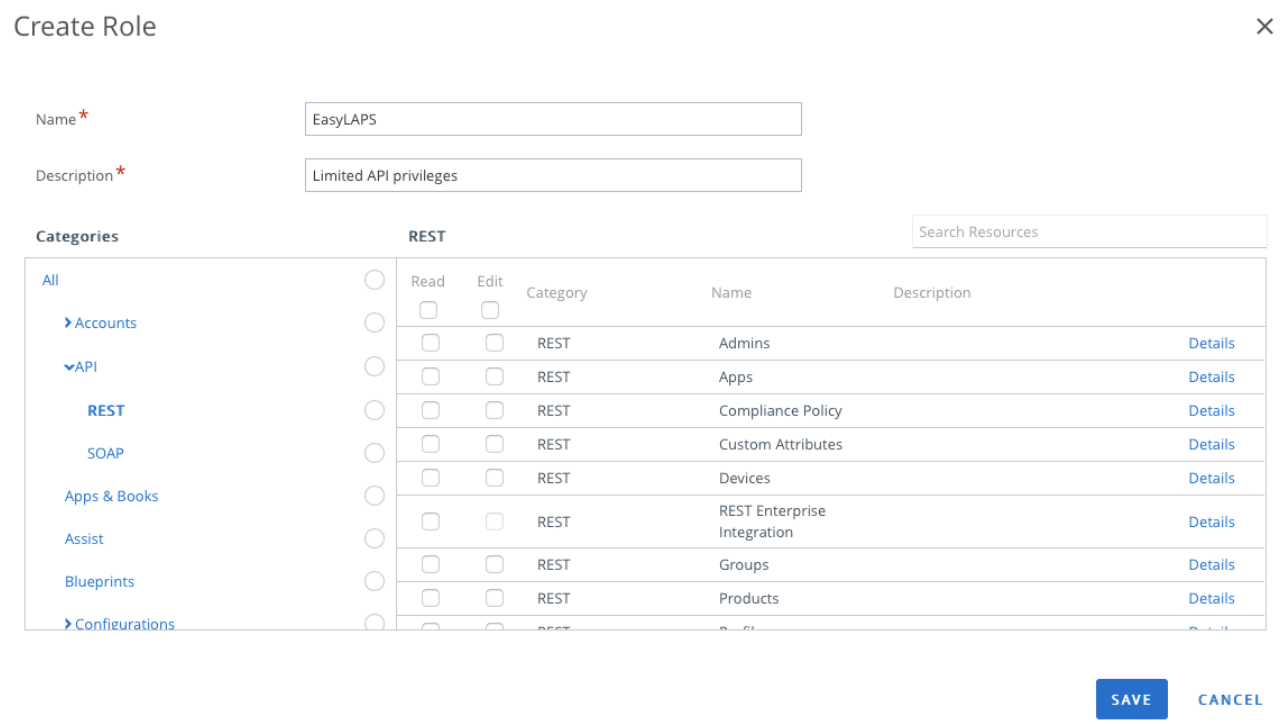
The key will be used by EasyLAPS to make API calls.

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

First create a new role with limited API privileges.

Go to Accounts > Administrators > Roles.

Click on "Add Role".



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

The role requires the following set of privileges :

- Custom Attributes > Details

- Edit — Rest API Custom Attributes Write

        - Read — Rest API Custom Attributes Read

    - Devices > Details

        - Edit — REST API Devices Execute

        - Edit — REST API Devices Delete

        - Read — REST API Devices Read

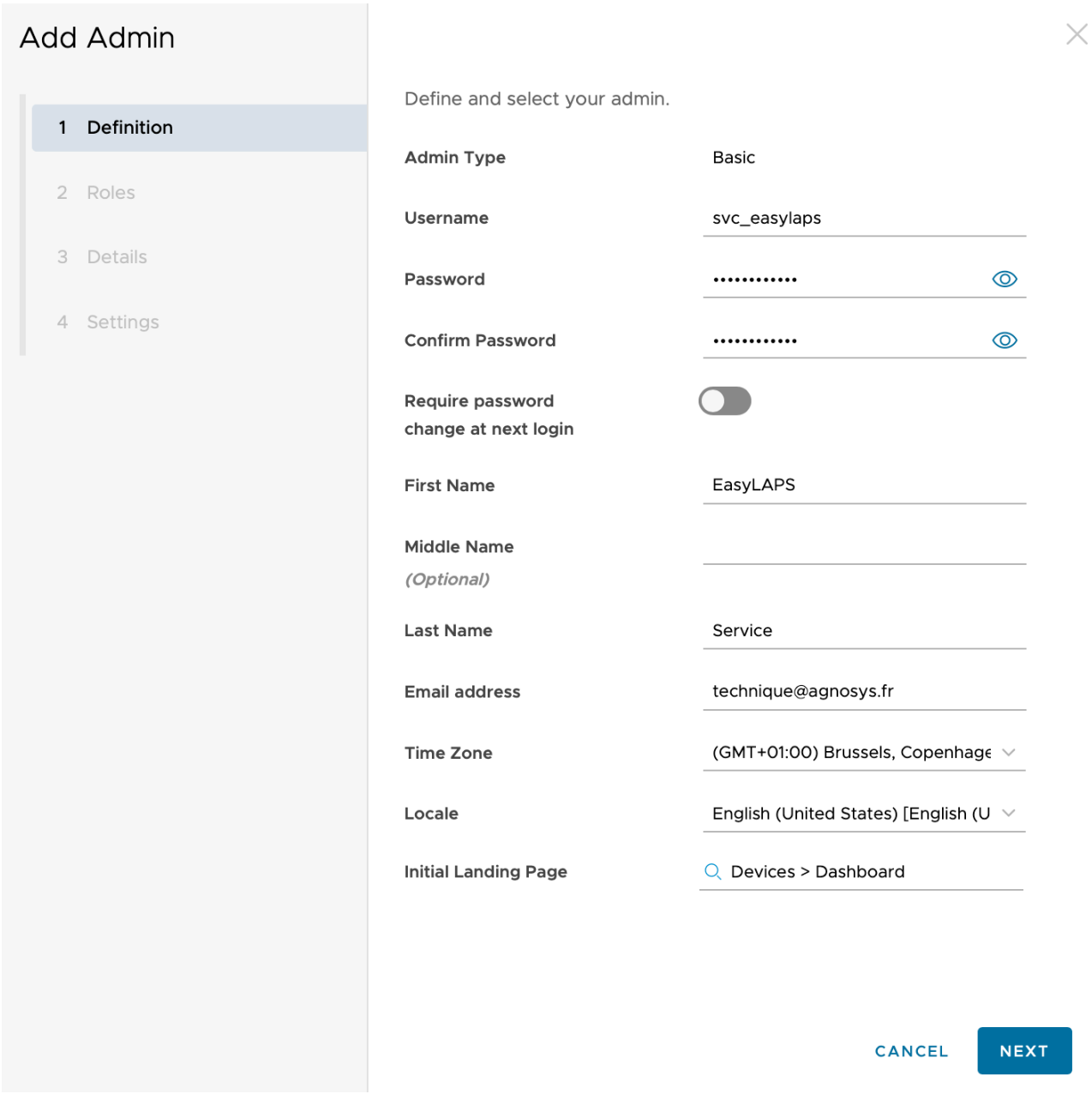
Click on "Save".

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

Go to Accounts > Administrators > List View.

Click on "Add" > "Add Admin".

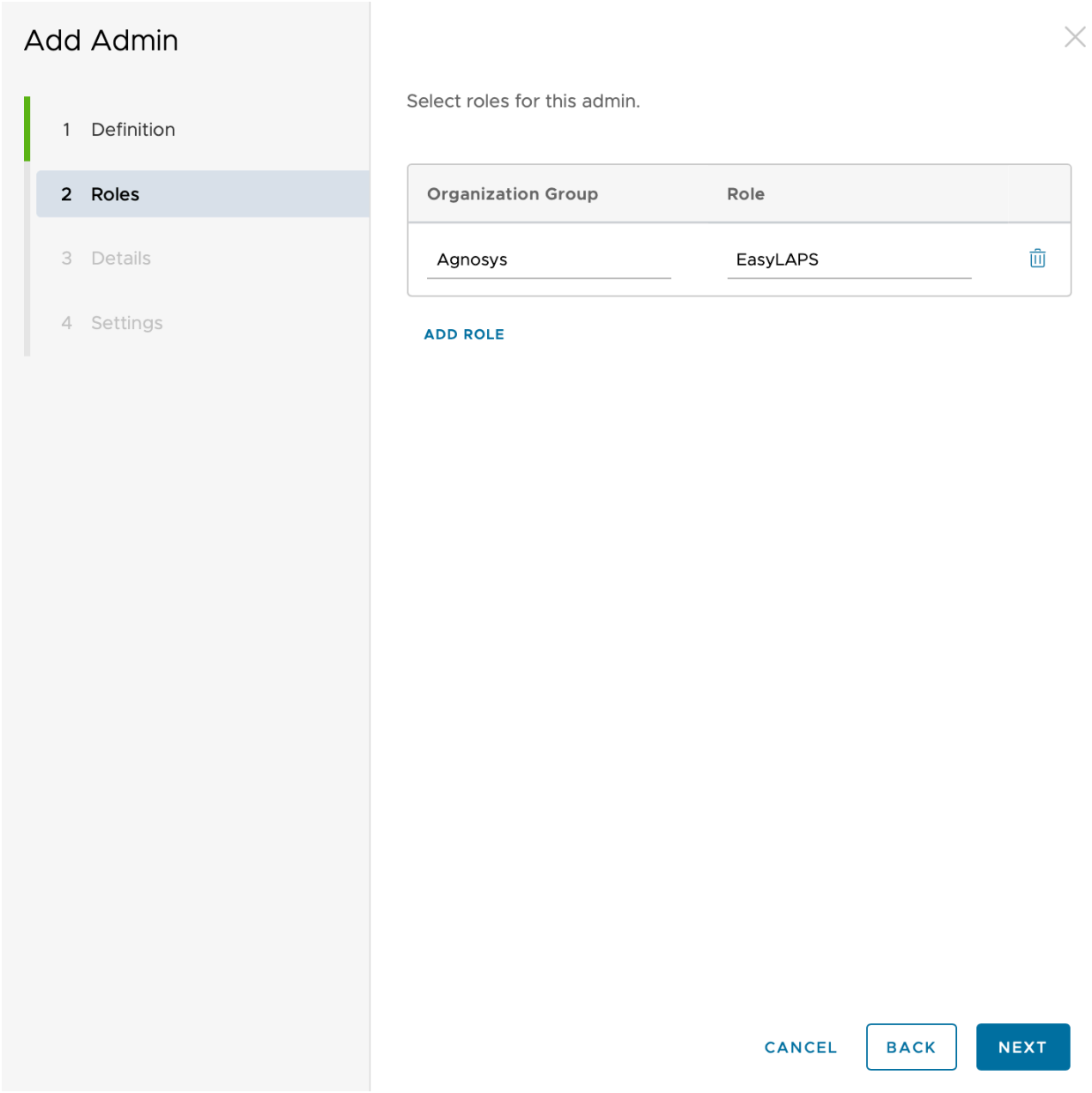
Select "Basic" then click on "Next".



Fill in the required fields.

Complete the text document with the chosen username and password.

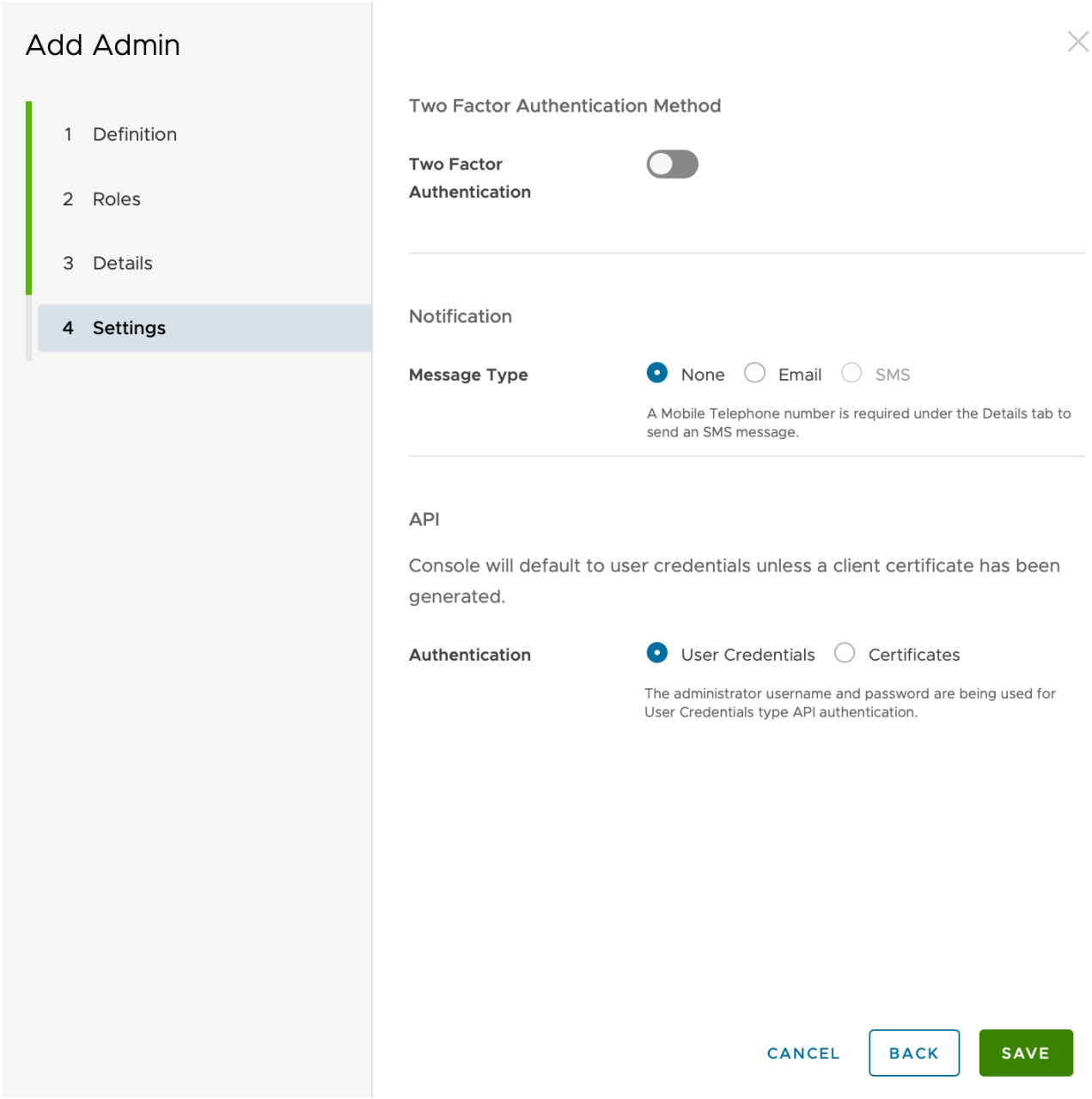
Click on "Next".



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

Click on "Next".

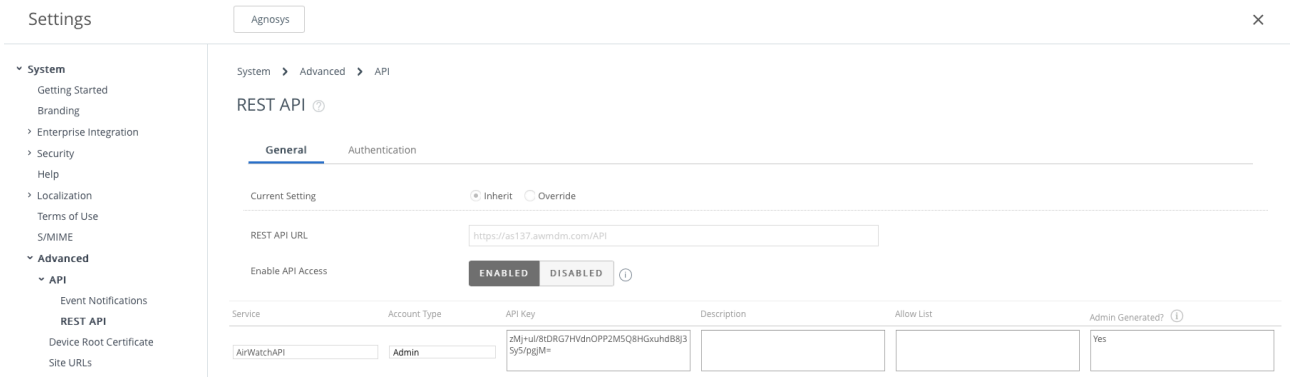
On the pane "3 Details", click on "Next".



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

Click on "Save".

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



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

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

```
Username : svc_easylaps
Password : SuperSecretPassword
API Key  : zMj+ul/8tDSG7HVdnOPQ2M5Q8HGxuhdB8J3Sy5/pgjN=

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

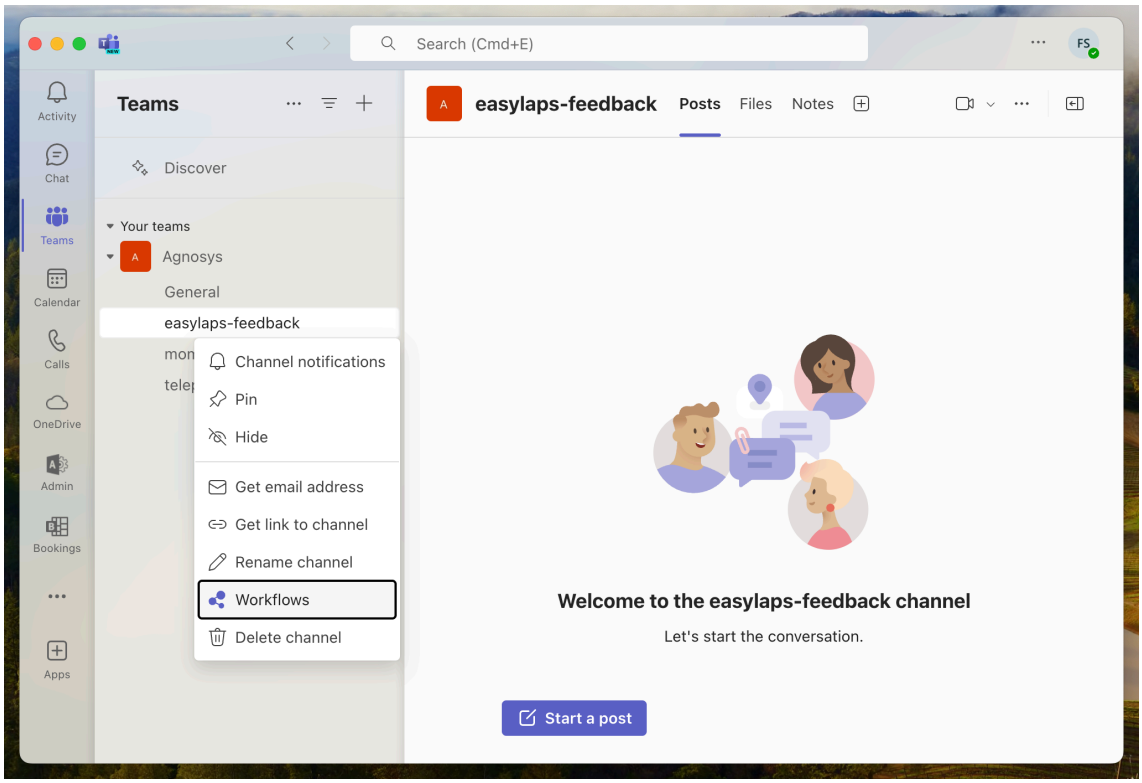
Concatenate the 3 values separated with commas then follow these instructions :
- copy the concatenated string (exactly)
- open the "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the concatenated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

Paste the encrypted value in the APIAUTHENTICATIONSTRING key.

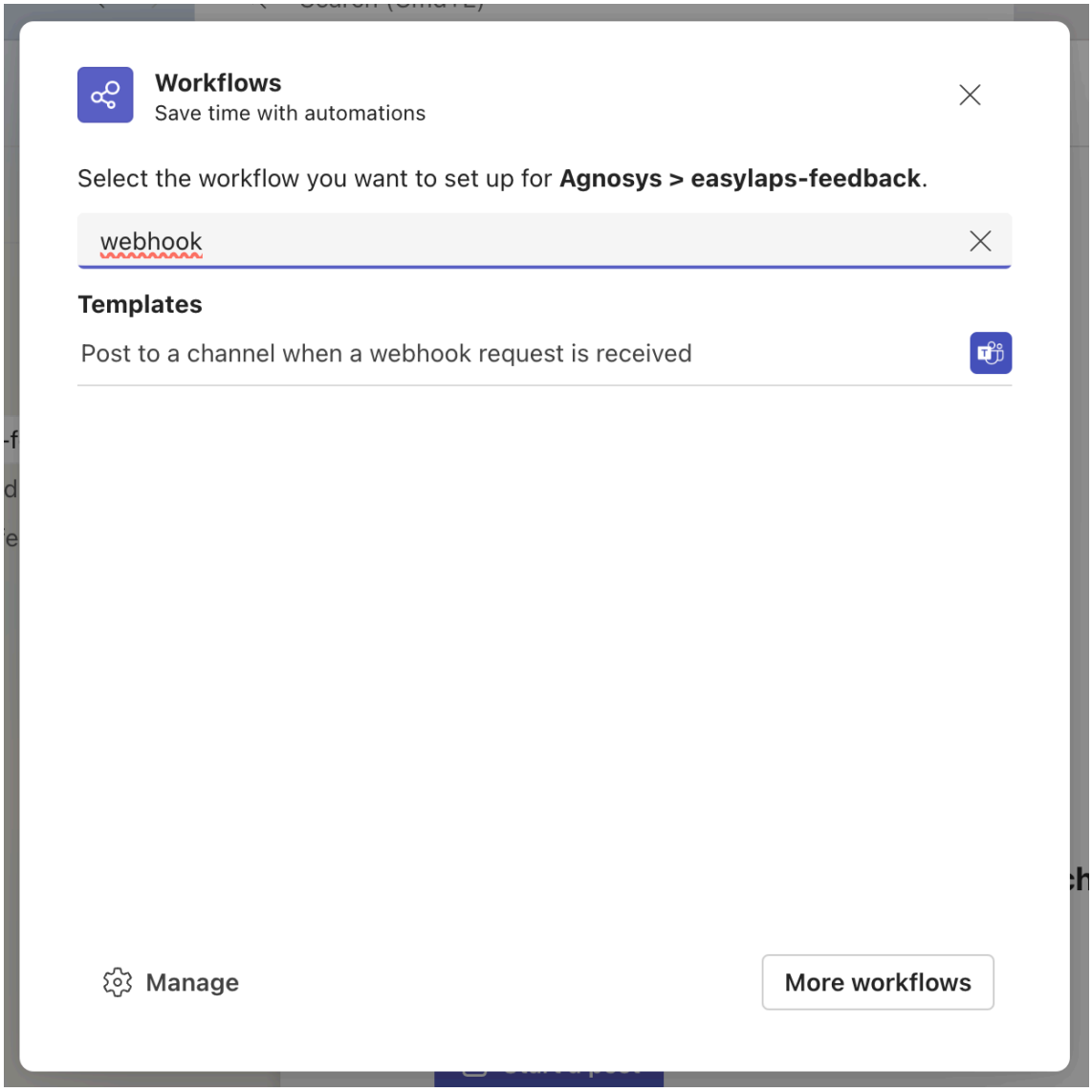
Microsoft Teams integration

EasyLAPS can report to a dedicated Microsoft Teams channel the status message of its execution.

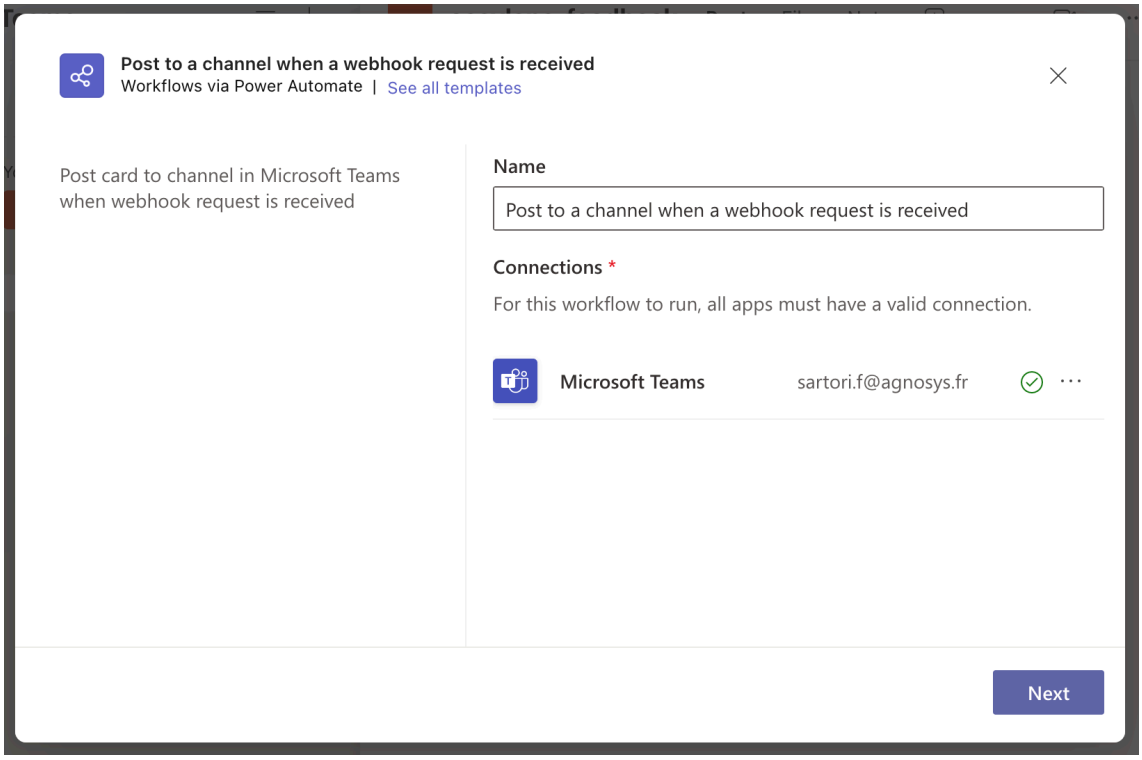
First create a dedicated Microsoft Teams channel of type "Standard" (everyone on the team has access).



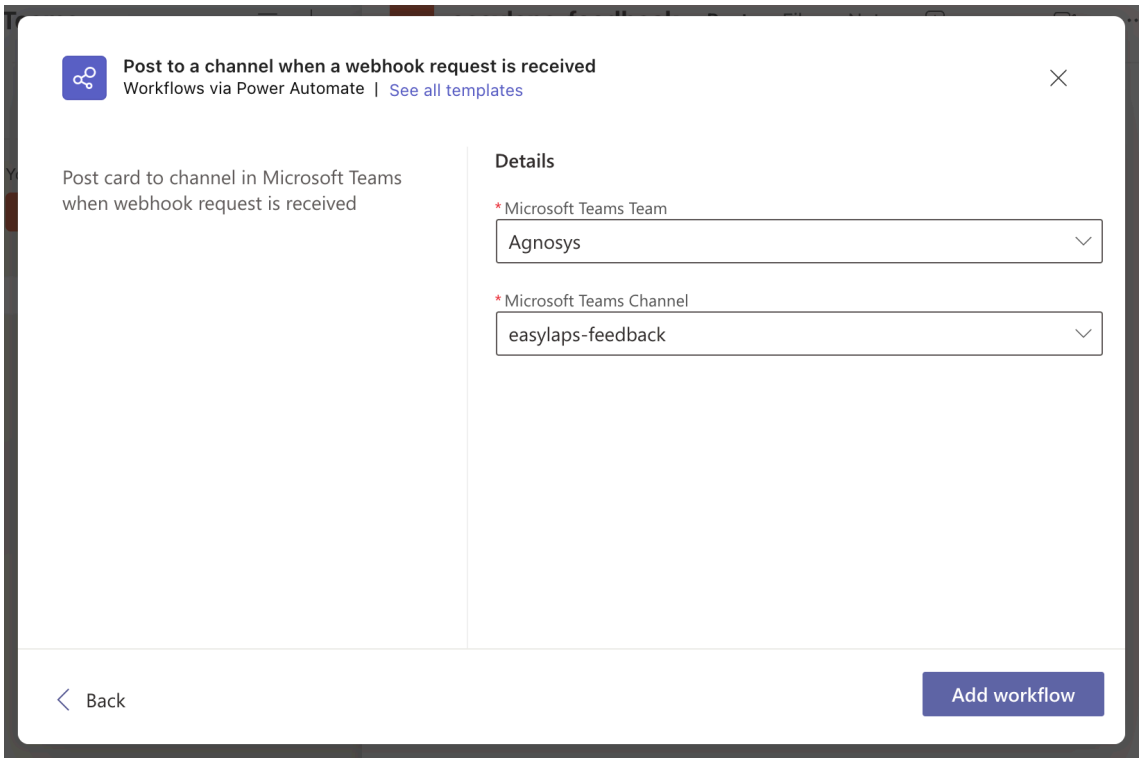
Click on the "..." button to the right of the channel name, then select "Workflows".



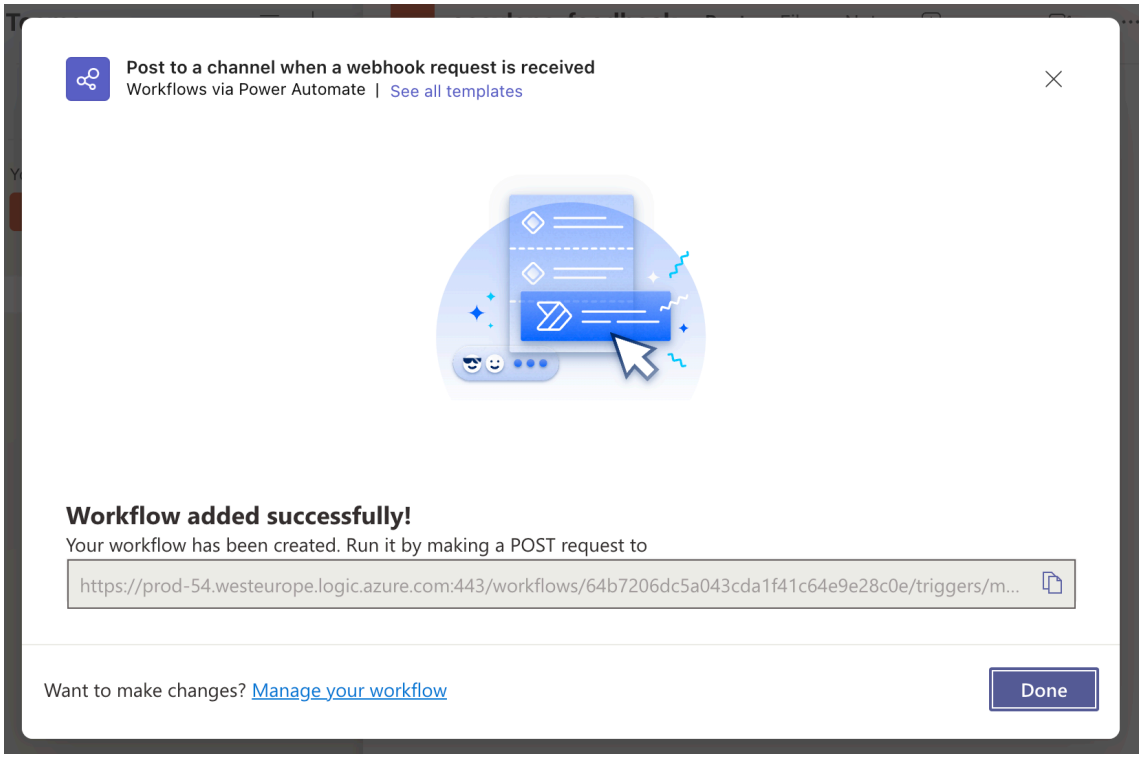
Type "webhook" in the search field, then click on "Post to a channel when a webhook request is received".



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



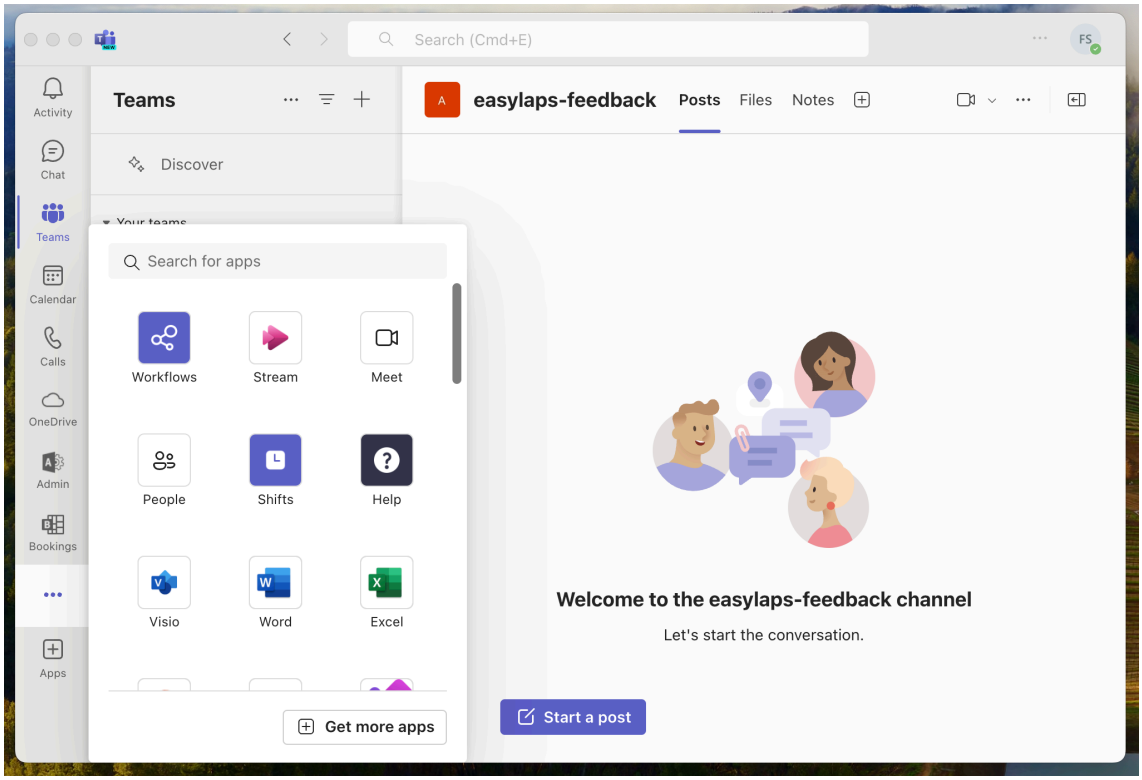
Check the Microsoft Teams team and the Microsoft Teams channel, then click on "Add workflow".



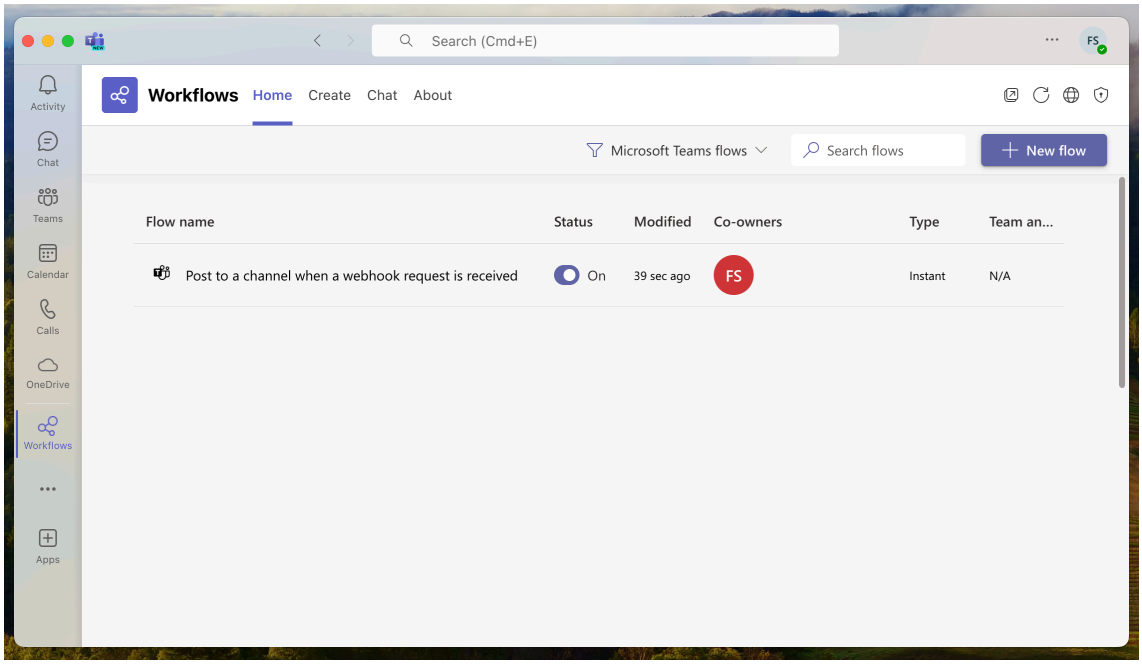
Click on the button to the right of the URL displayed to copy it, then follow these instructions :
- open the "EasyLAPS-Toolkit" folder
- open the "easylaps_secrets" subfolder
- execute the "easylaps_rsa_engine" script (double-click on the .command file)
- paste the copied URL
- the URL is encrypted,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

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

Back in the pane, click on "Done".



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



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

EasyLAPS configuration files to Custom configuration profiles conversion

If the MDM solution is Jamf Pro — This step is **optional** because this MDM offers to upload an EasyLAPS 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.

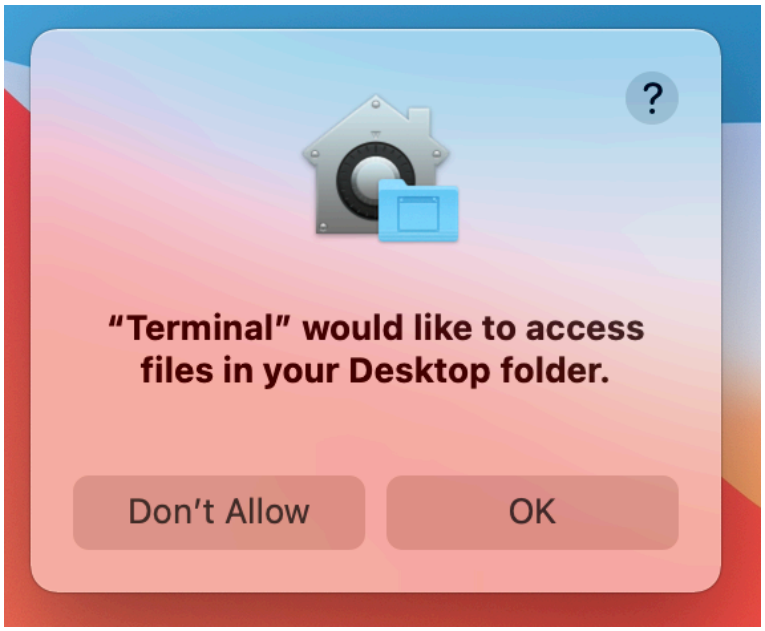
If the MDM solution is not Jamf Pro — This step is **required**. Follow these instructions.

Open the "EasyLAPS-Toolkit" folder.

Open the "easylaps_configs" subfolder.

Open the "configs_profiles" subfolder.

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



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

In this example, the script has converted two EasyLAPS configuration files into two Custom configuration profiles ready to be deployed by the MDM (only one must be scoped to a specific device).

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

EasyLAPS Content building

The EasyLAPS-Content package currently embeds 3 custom resources :
- the private key used to decrypt sensitive informations in an EasyLAPS Custom configuration
- a detection app named "EasyLAPS-Content.app"
- an icon for the management account.

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

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

Package signature requirement

• **FileWave**

No signature required.

• **Jamf Pro**

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

• **Jamf School**

No signature required.

• **JumpCloud**

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

• **Meraki Systems Manager**

No signature required.

• **Microsoft Intune**

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

• **Miradore**

Signature required.

• **Mosyle Business**

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

• **Mosyle Manager**

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

• **SimpleMDM**

Signature required.

• **VMware Workspace ONE**

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

Package signature options

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

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

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

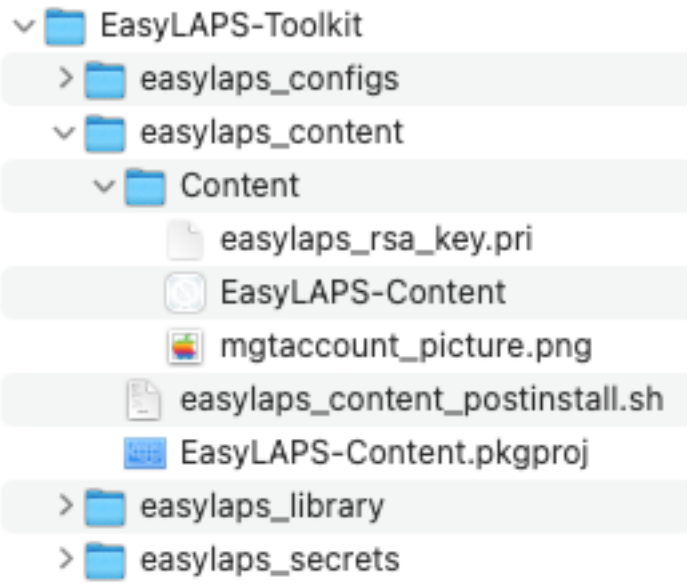
- the certificate forged with the Jamf Pro's Built-in CA can be validated by a device only if it is already enrolled in Jamf Pro
- for more information, please consult this article : https://docs.jamf.com/technical-articles/Creating_a_Signing_Certificate_Using_Jamf_Pros_Built-in_CA_to_Use_for_Signing_Configuration_Profiles_and_Packages.html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

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

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

• Open an EasyLAPS support ticket to get the package signed by Agnosys or your integrator.

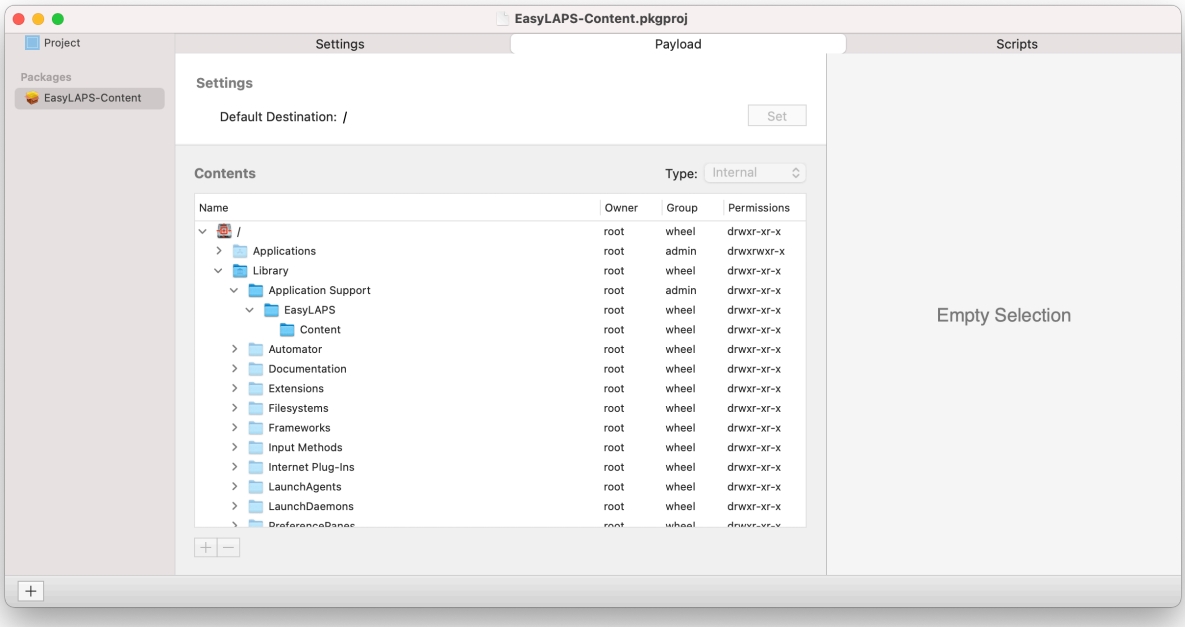
Project opening



Open the "EasyLAPS-Toolkit" folder.

Open the "easylaps_content" subfolder.

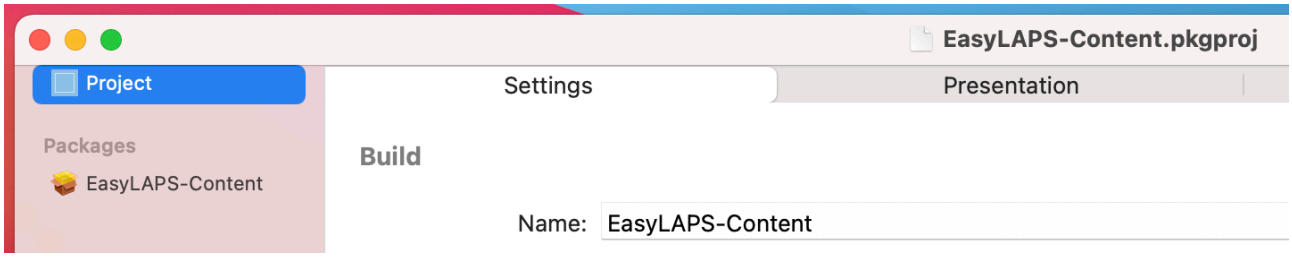
Open the "EasyLAPS-Content.pkgproj" file with the Packages app.



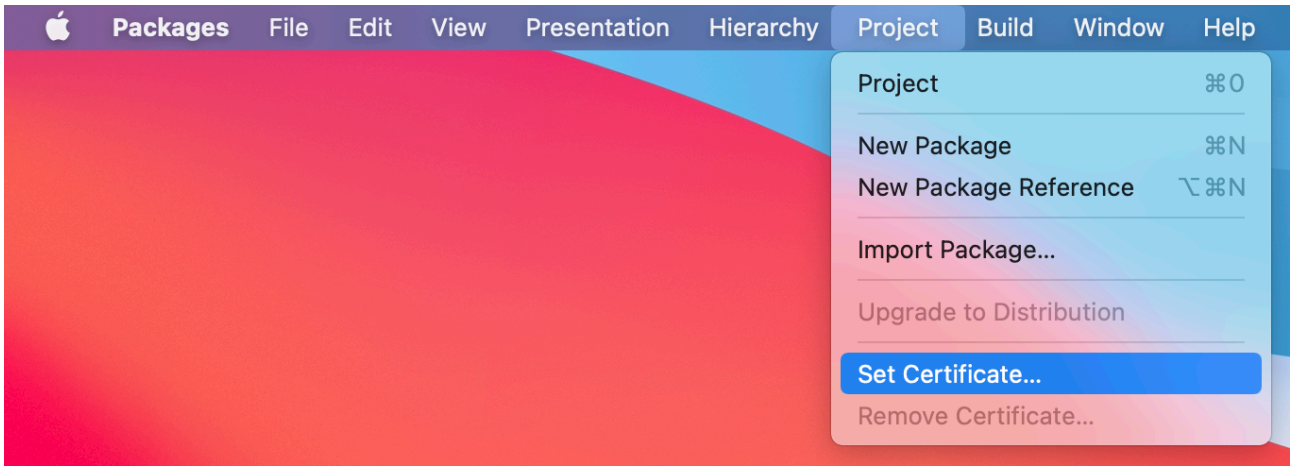
The generated package will embed the "Content" folder for an installation in /Library/Application Support/EasyLAPS/

Signing configuration

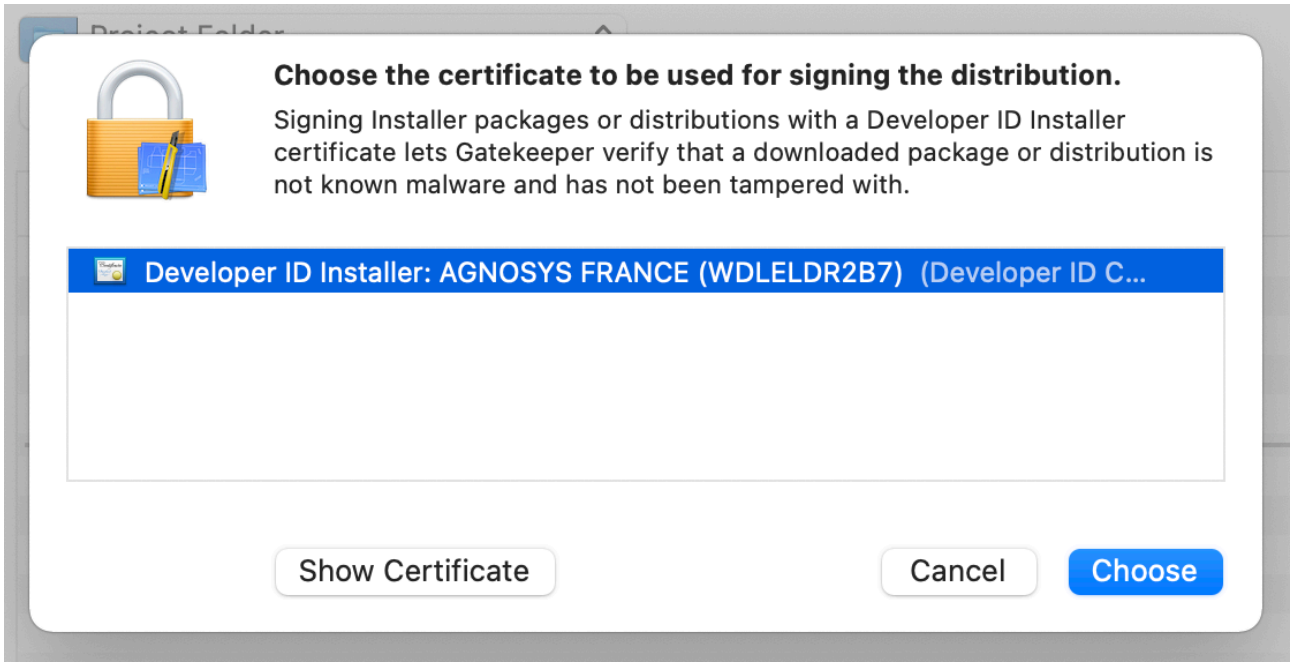
Open the Keychain Access app and check that your "Developer ID Installer" certificate is installed in the "login" keychain.



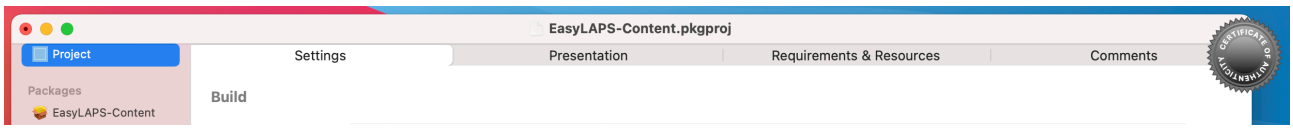
Click on "Project" then select the "Settings" tab.



Select Project > Set Certificate.

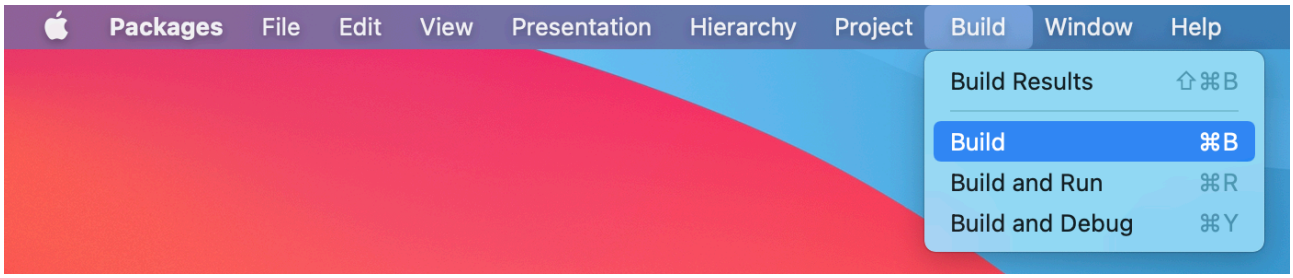


Select your "Developer ID Installer" certificate and click on "Choose".

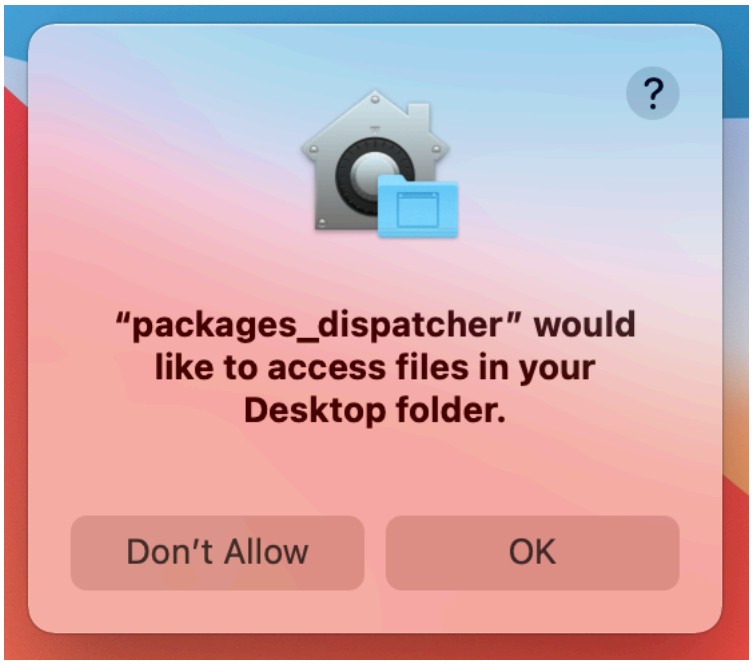


A "Certificate of authenticity" badge is now visible in the upper right corner of the project window.

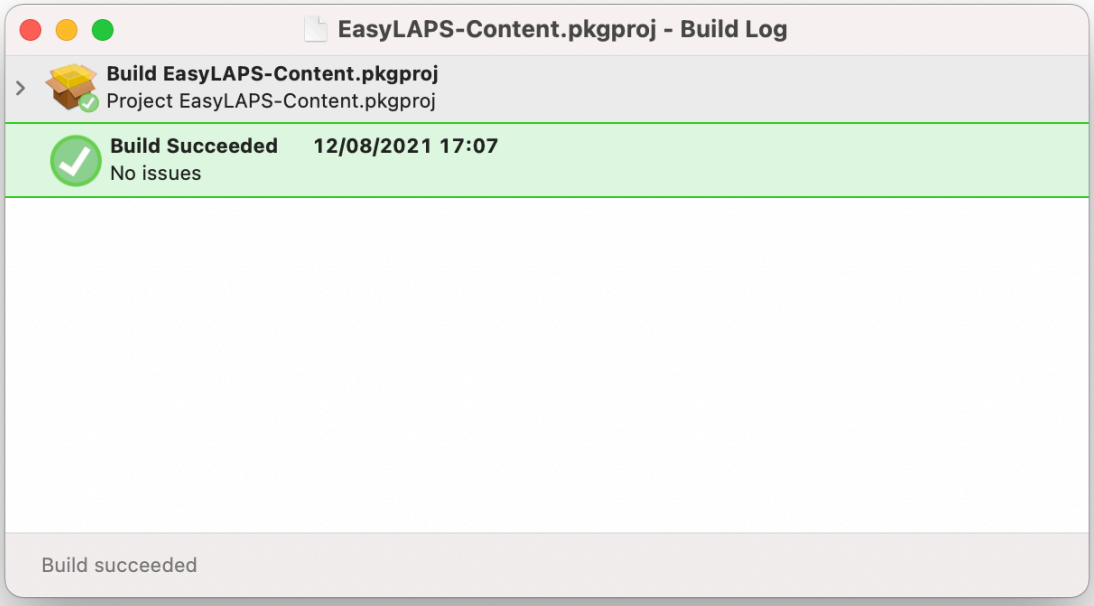
Project building



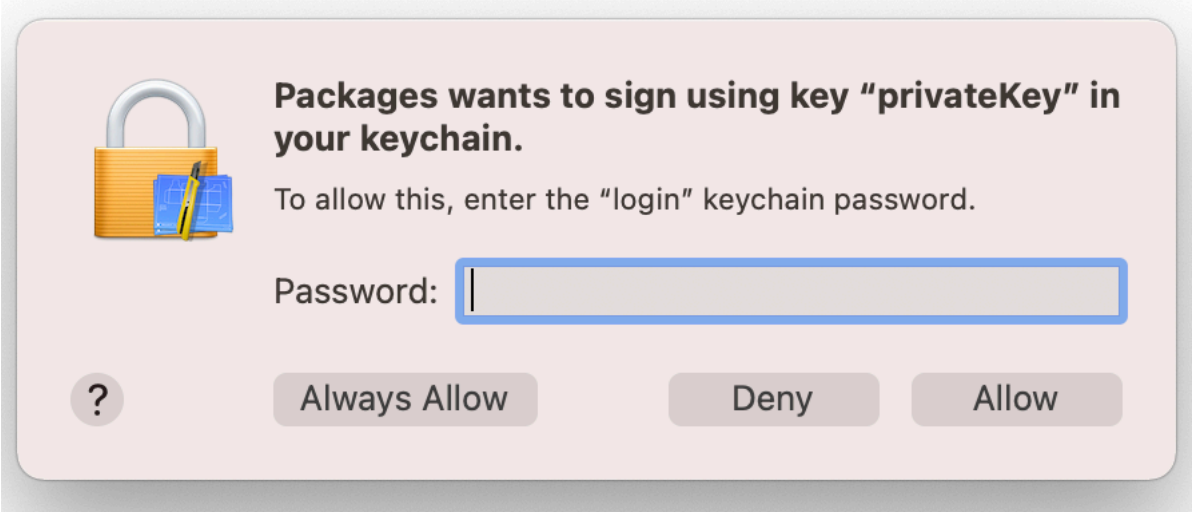
Select Build > Build.



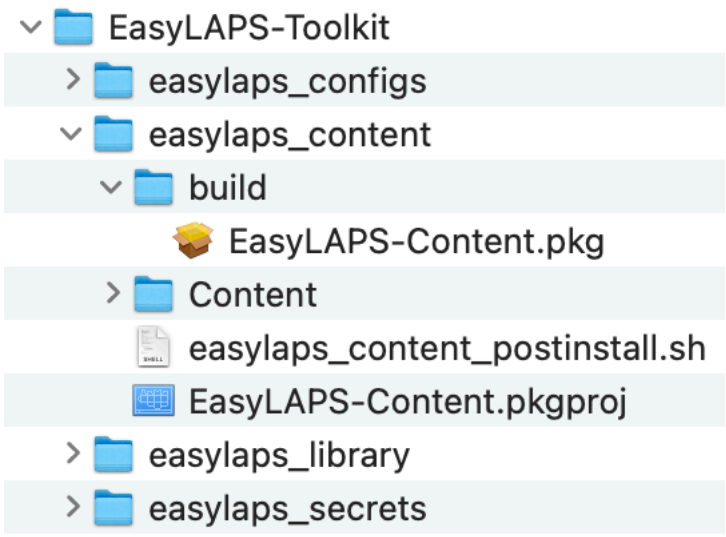
If prompted to authorize the Packages app to access files in a specific folder like your Desktop folder, click on "OK".



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



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



The package is built at the following path :
EasyLAPS-Toolkit > easylaps_content > build

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

Configuration profiles requirements

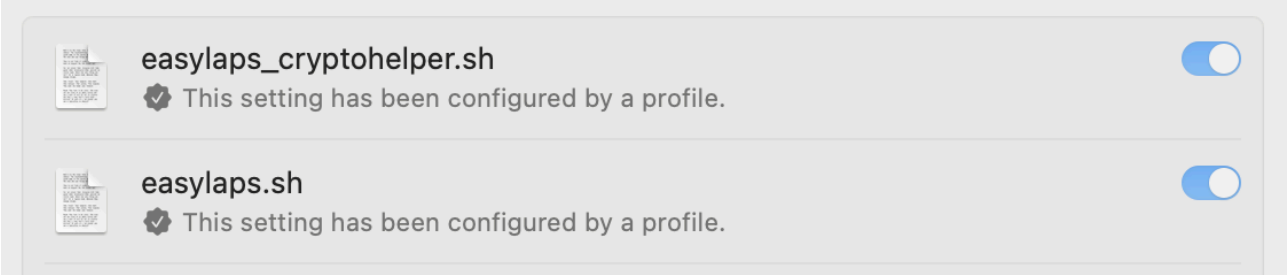
This section details the configuration profiles required by EasyLAPS in addition to the EasyLAPS Custom configuration profile.

• **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 EasyLAPS has installed a Login item that can run in the background and that can be managed in System Settings.

Payload required : Background Item Management

- For the EasyLAPS Launch Daemon :
    - Rule Type : Label
    - Rule Value : com.agnosys.easylaps
- For the EasyLAPS Crypto Helper Launch Daemon :
    - Rule Type : Label
    - Rule Value : com.agnosys.easylaps_cryptohelper



Once the configuration profile is deployed on a device running EasyLAPS, open System Settings > Login Items and check that the Login items "easylaps.sh" and "easylaps_cryptohelper.sh" (visible only when the Crypto Helper is active) 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 "easylaps_btm_signed.mobileconfig" provided in the subfolder "easylaps_library" of the EasyLAPS Toolkit.

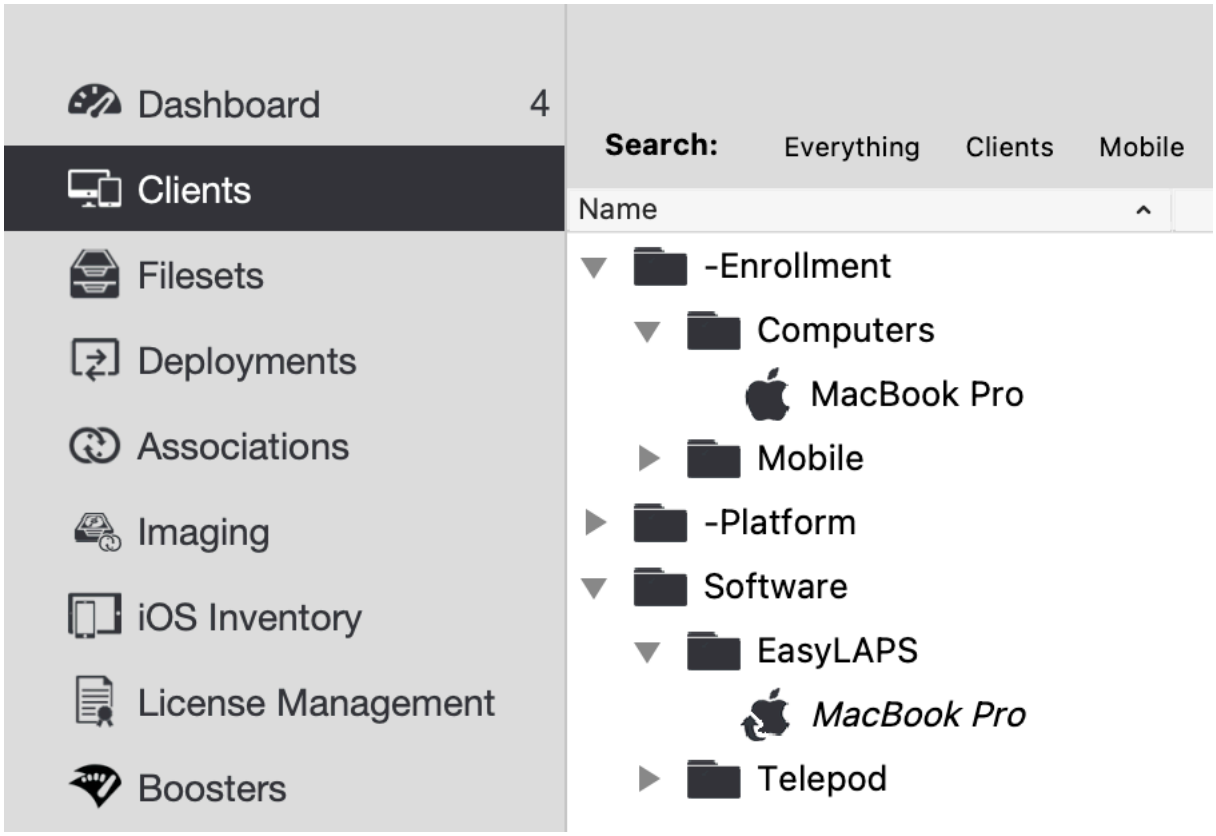
Provisioning FileWave

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

General configuration

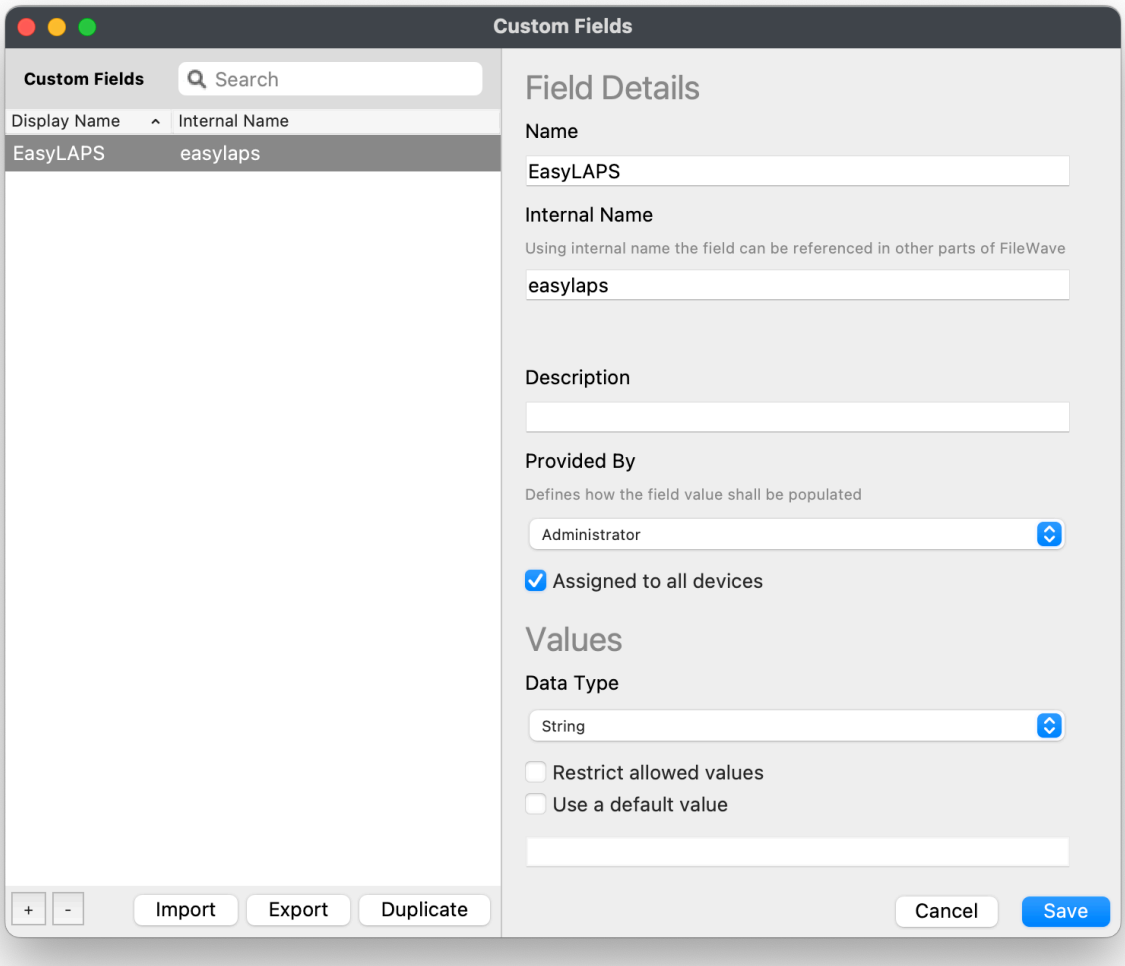
In this example, the devices are part of group named "EasyLAPS" following this structure.



EasyLAPS Custom Field

The EasyLAPS Custom Field should be created manually before the first rotation.

FileWave Admin > Assistants > Custom Fields > Edit Custom Fields



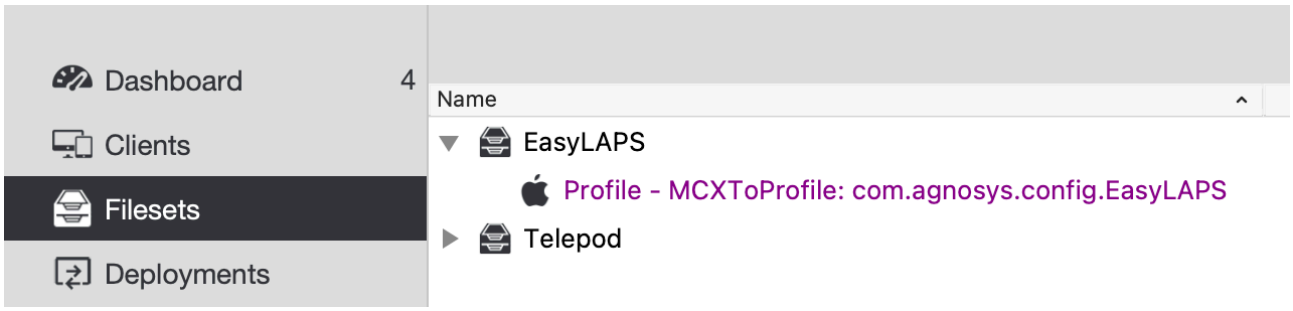
Enter "EasyLAPS" in the Name field and "easylaps" (exactly) in the Internal Name field.

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

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

Custom configuration profile

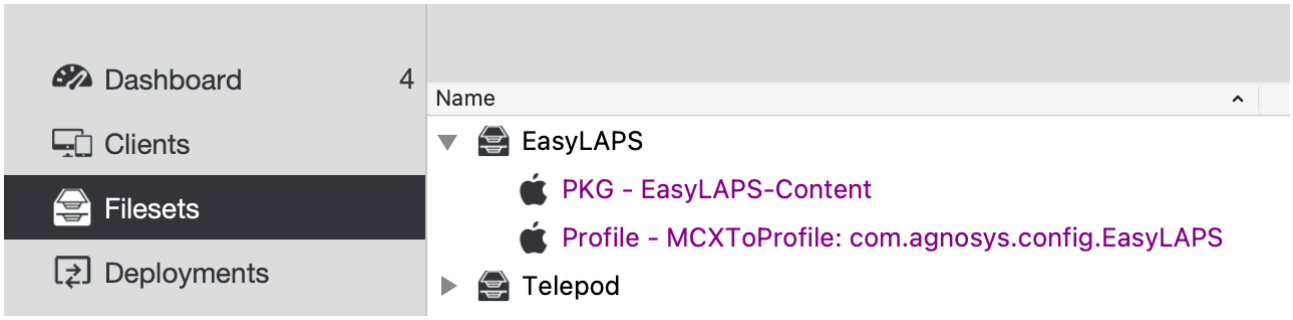
The Custom configuration profile is provisioned with the following steps :
- Filesets > New Fileset Group > Name : EasyLAPS
- Select the Fileset Group "EasyLAPS"
- Click on "New Desktop Fileset" then click on "Profile"
- In the Profile Editor, click on "Load Profile"
- Select the file : com.agnosys.config.FileWave.Paris.EasyLAPS.mobileconfig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



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

EasyLAPS-Content package

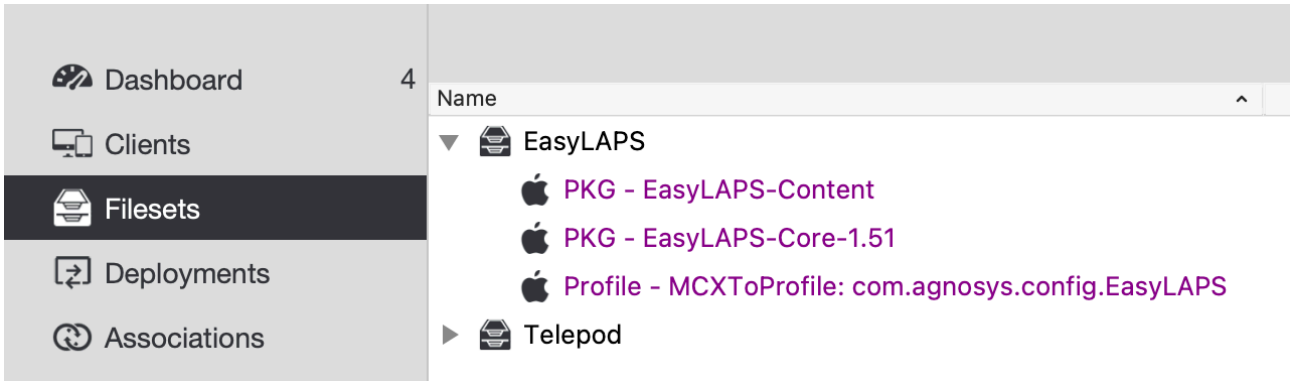
The EasyLAPS-Content package is defined with the following steps :
- Filesets > EasyLAPS
- Click on "New Desktop Fileset" then click on "MSI / PKG"
- Select the file : EasyLAPS-Content.pkg > Open.



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

EasyLAPS-Core package

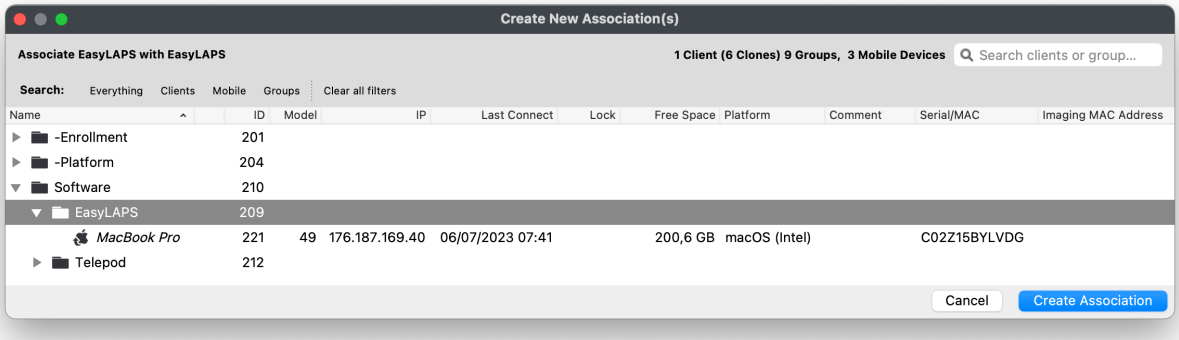
The EasyLAPS-Core package is defined with the following steps :
- Filesets > EasyLAPS
- Click on "New Desktop Fileset" then click on "MSI / PKG"
- Select the file : EasyLAPS-Core.pkg > Open.



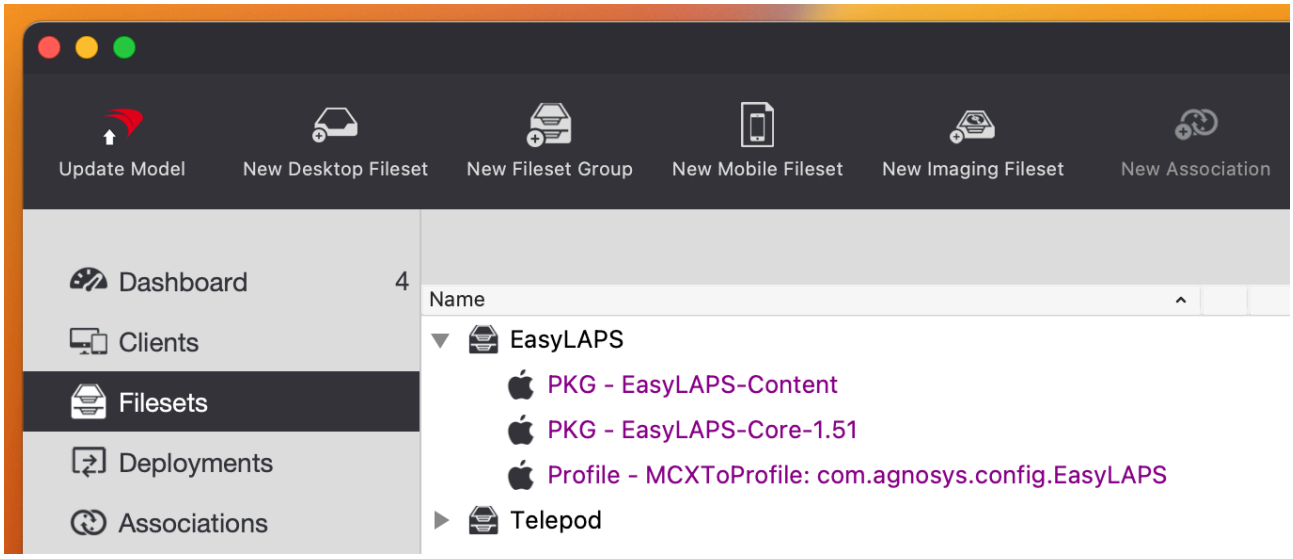
The EasyLAPS-Core package is linked to the "EasyLAPS" Fileset Group.

Deployment on the EasyLAPS group

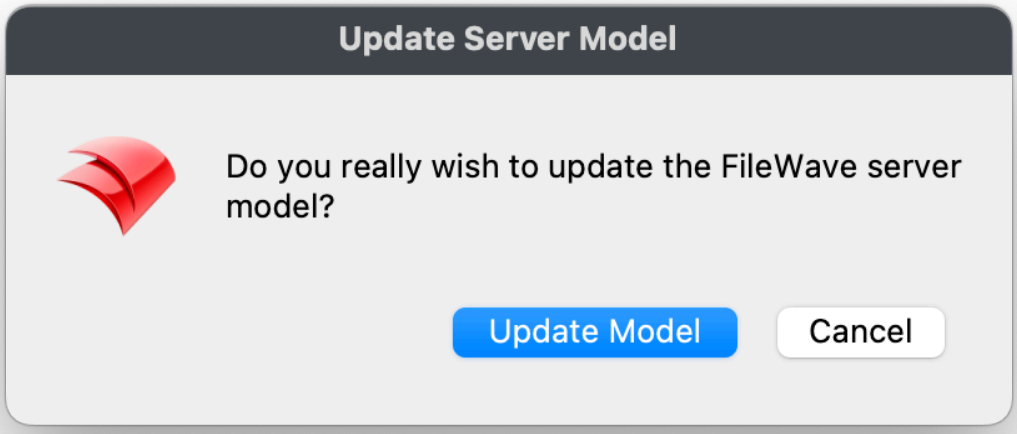
The EasyLAPS Fileset is associated to the EasyLAPS group with the following steps :
- Filesets > EasyLAPS
- In the toolbar, click on "New Association".



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

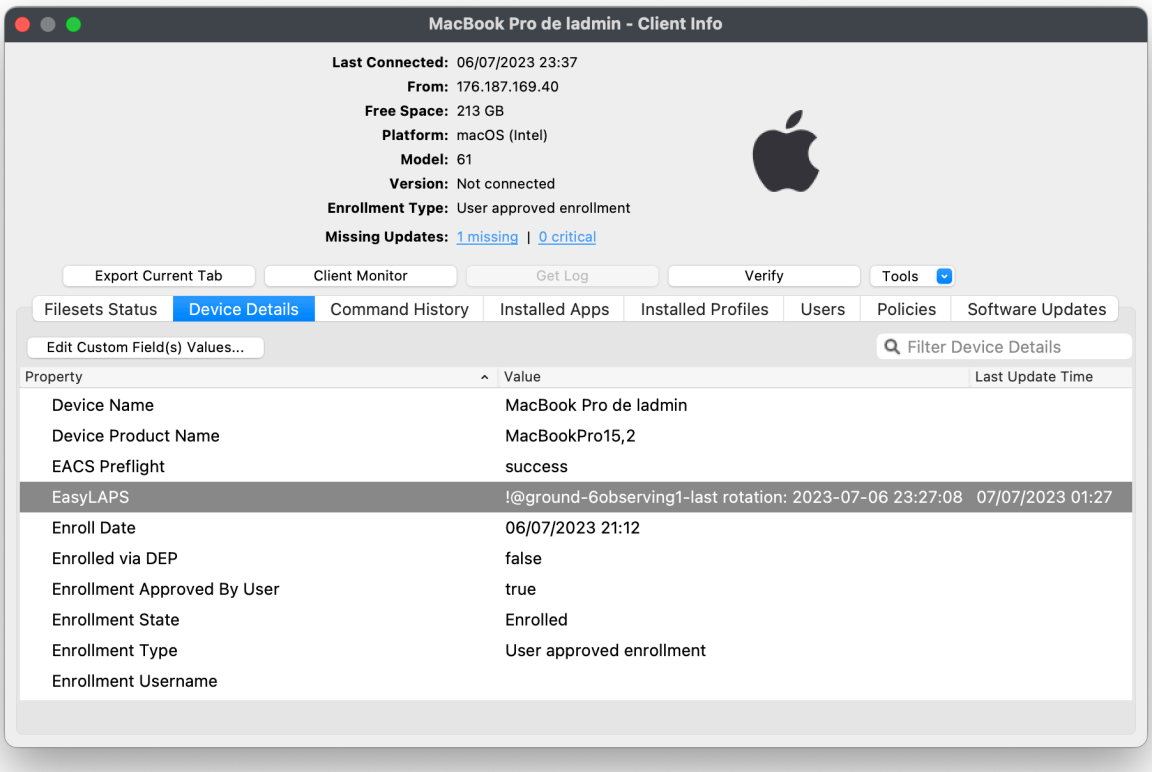


In the toolbar, click on "Update Model".



Click on "Update Model".

Result of a successful rotation



After the first successful rotation, the new password is visible in the Custom Field named "EasyLAPS". In this example, the password is stored in clear text.

Note that the EasyLAPS Custom Field is created automatically if missing when the FileWave administrator account has the appropriate privileges.

Provisioning Jamf Pro

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-Core package.

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

General configuration

In this example, the devices are part of a computer group named "EasyLAPS".

Custom configuration profile : importing a .plist file

Follow these instructions if you want to upload in Jamf Pro an EasyLAPS 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. EasyLAPS-Custom configuration profile)
    - Level : Computer Level
    - Distribution Method : Install Automatically
- Application & Custom Settings > Upload > Add
    - Preference Domain : com.agnosys.config.EasyLAPS
    - Upload > config_1.plist
- Scope
    - Targets > Specific Computers
    - Add > Computer Groups > EasyLAPS > 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 an EasyLAPS configuration file to Custom configuration profile conversion.

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

EasyLAPS-Content package

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

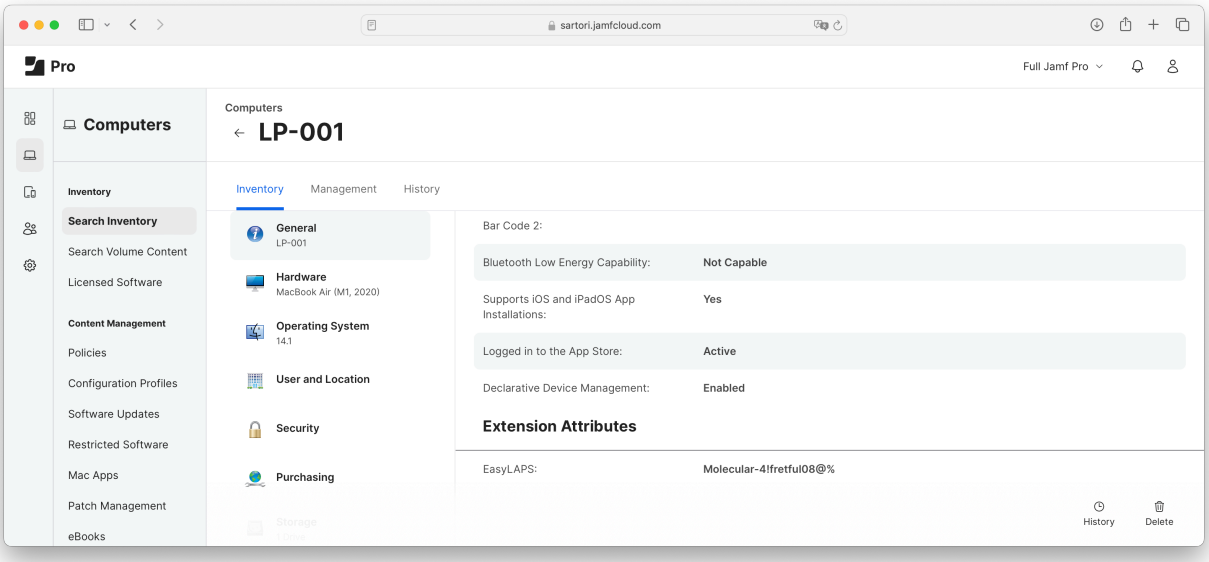
The EasyLAPS-Content package is provisioned with the following steps :
- Computers > Policies > New
- Options
    - General
        - Display Name : EasyLAPS-Content Install
        - Trigger : Recurring Check-in — Execution Frequency : Once per computer
    - Packages
        - Configure > EasyLAPS-Content.pkg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

EasyLAPS-Core package

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

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

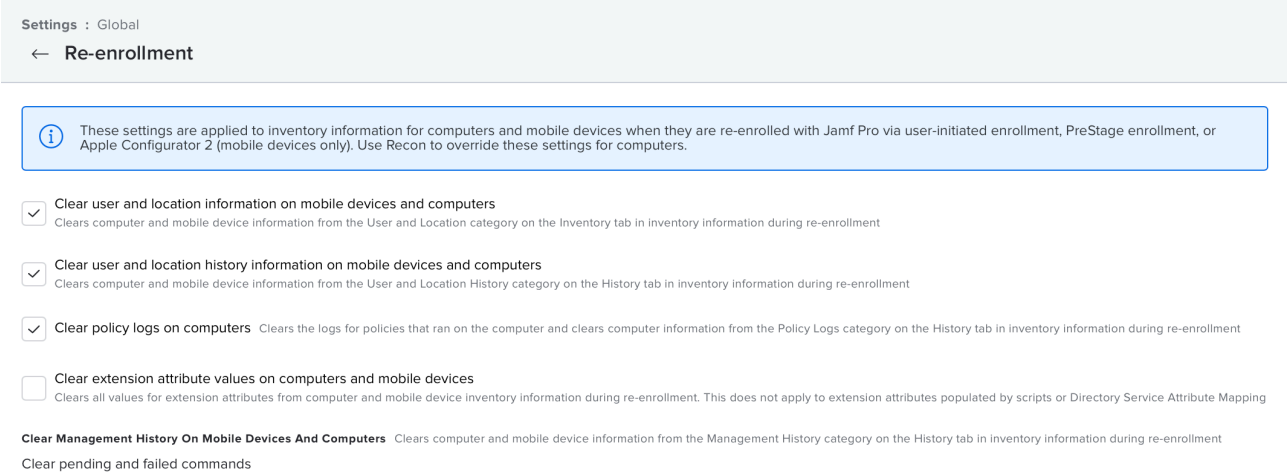
Result of a successful rotation



After the first successful rotation, the new password is visible in the Extension attribute named "EasyLAPS". In this example, the password is stored in clear text.

Note that the EasyLAPS Extension attribute is created automatically if missing when the API Client or the Jamf Pro User Account has the appropriate privileges.

Re-enrollment settings



Make sure the option "Clear extension attribute values on computers and mobiles devices" is disabled so that the password stored in MDM is not lost after the device is re-enrolled.

If you need that this option is enabled, do not forget to copy the content of the EasyLAPS attribute before the device is re-enrolled.

Provisioning Jamf School

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-Core package.

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 EasyLAPS.

General configuration

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

Custom configuration profile

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

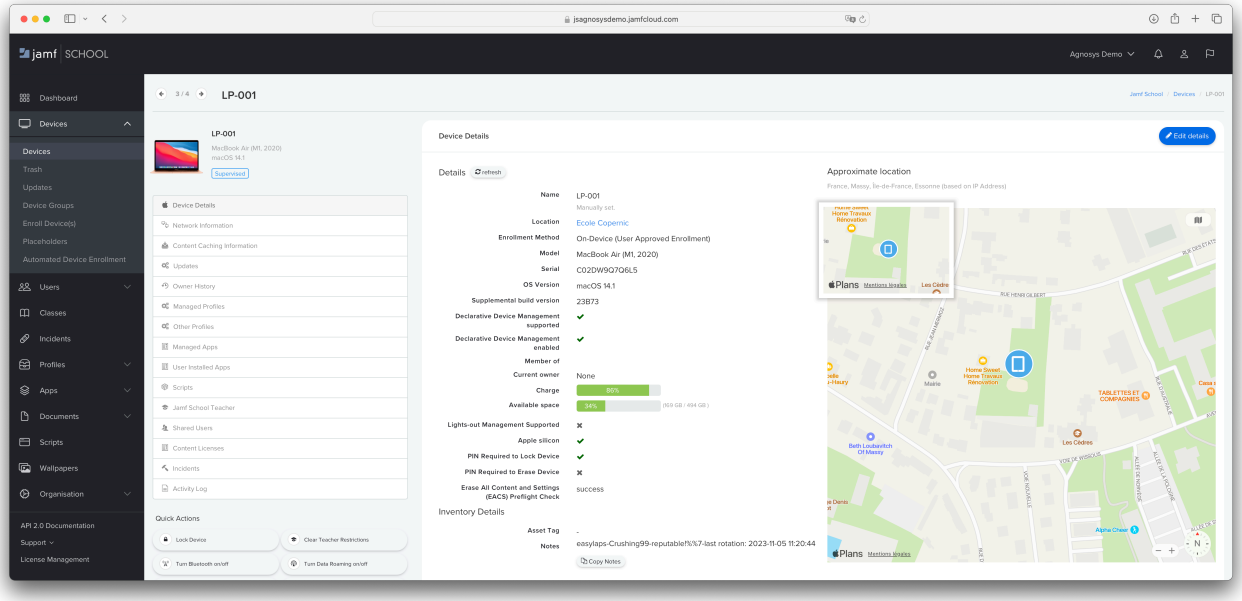
EasyLAPS-Content package

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

EasyLAPS-Core package

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

Result of a successful rotation



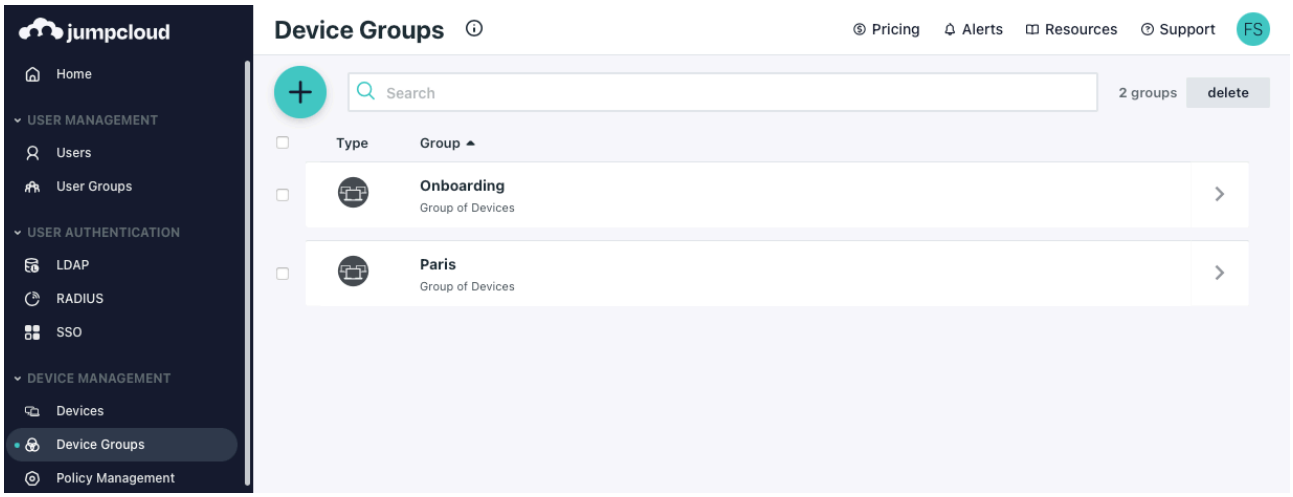
After the first successful rotation, the new password is visible in the field named "Notes". In this example, the password is stored in clear text.

Provisioning JumpCloud

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

General configuration



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

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

EasyLAPS-Content package

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

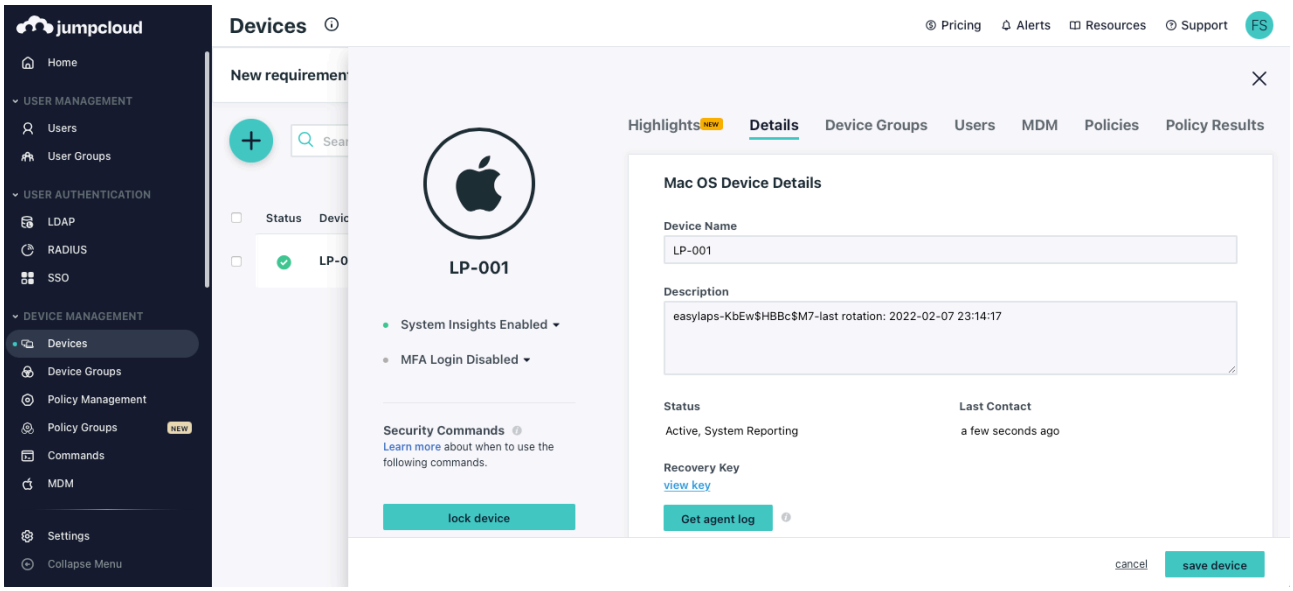
If you need to update the package, delete the configuration and start it over.

EasyLAPS-Core package

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

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

Result of a successful rotation



After the first successful rotation, the new password is visible in the field named "Description". In this example, the password is stored in clear text.

Provisioning Meraki Systems Manager

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

General configuration

In this example, the devices are part of the "Paris" network and associated to the "easylaps" 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.EasyLAPS.mobileconfig
- Deploy channel : Device
- Scope > Manual > with ANY of the followings tags
- Device tags : easylaps
- Save

EasyLAPS-Content package

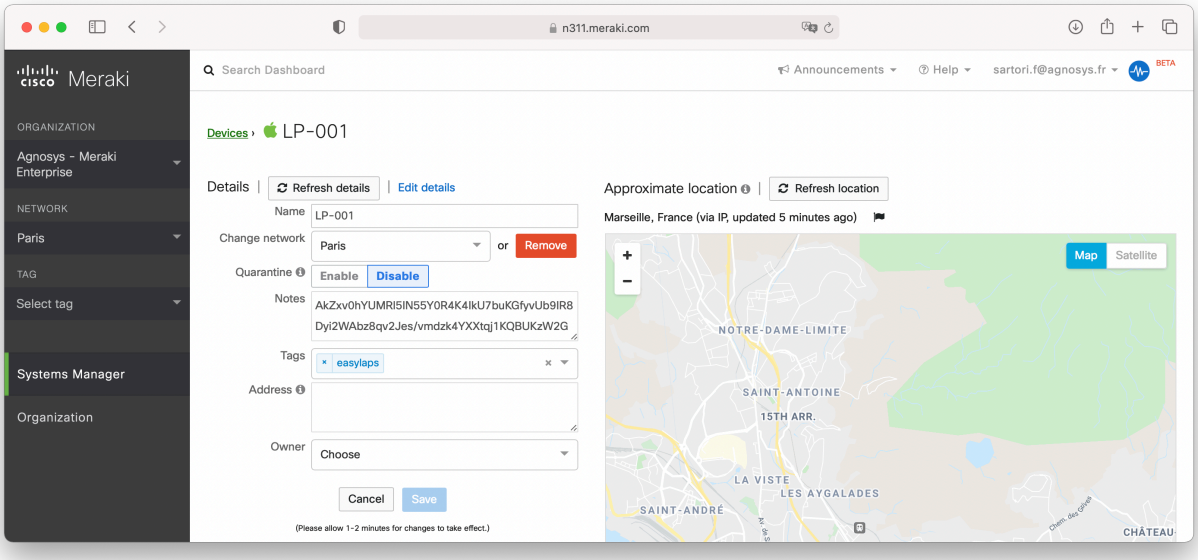
The EasyLAPS-Content package is provisioned with the following steps :
- Systems Manager > Manage > Apps
- Add app > macOS > Custom app
- Name : EasyLAPS-Content
- Identifier : com.agnosys.pkg.EasyLAPS-Content
- Vendor : Agnosys
- Type : Upload to the Meraki cloud
- Select the file : EasyLAPS-Content.pkg
- Auto-install : enabled

- Visible in SSP : disabled
- Scope > Manual > with ANY of the followings tags
- Device tags : easylaps
- Save

EasyLAPS-Core package

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

Result of a successful rotation



After the first successful rotation, the new password is visible in the field named "Notes". In this example, the password is stored in encrypted form.

Provisioning Microsoft Intune

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

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

General configuration

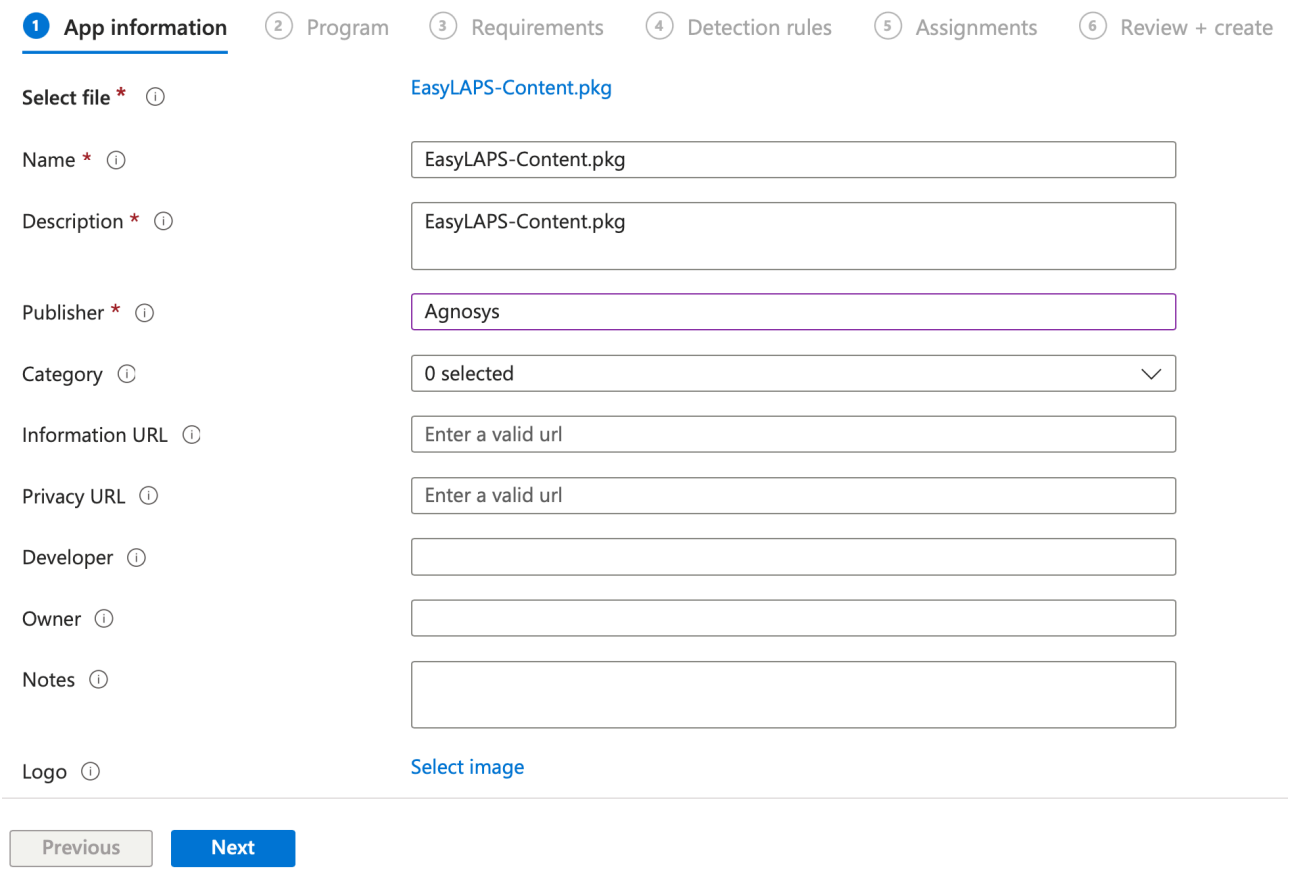
The scope of the components installation is here all devices.

Custom configuration profile

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

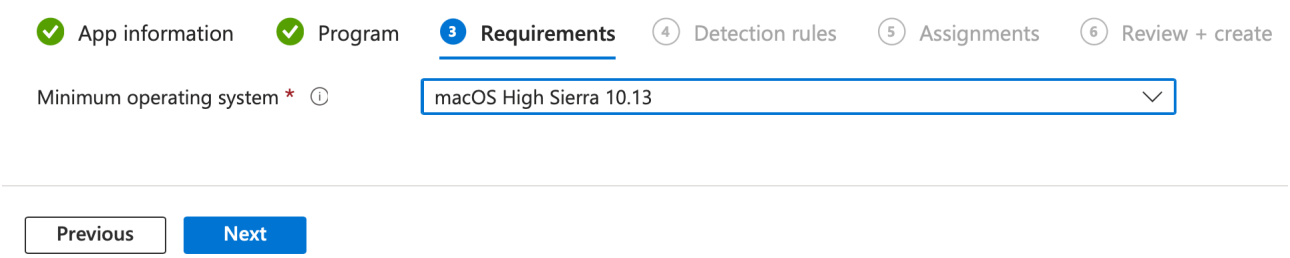
EasyLAPS-Content package

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

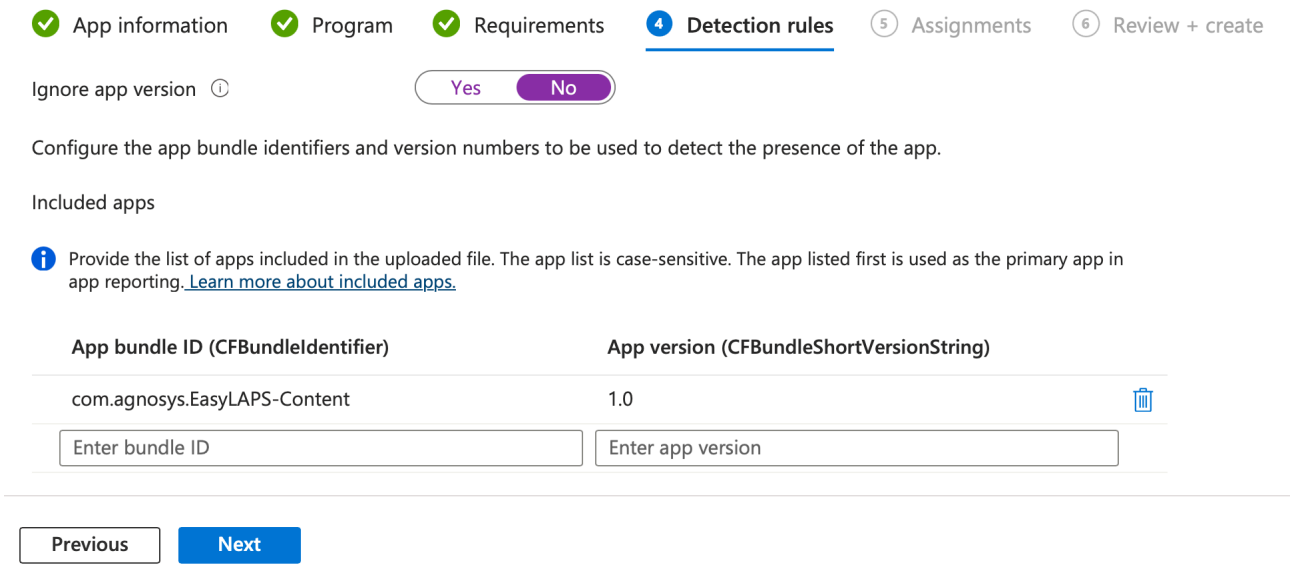


- App information
    - Select file > Select app package file
    - App package file > Select a file > EasyLAPS-Content.pkg > OK
    - Publisher : Agnosys

- Program : no scripts need to be configured



- Requirements
    - Minimum operating system : macOS High Sierra 10.13



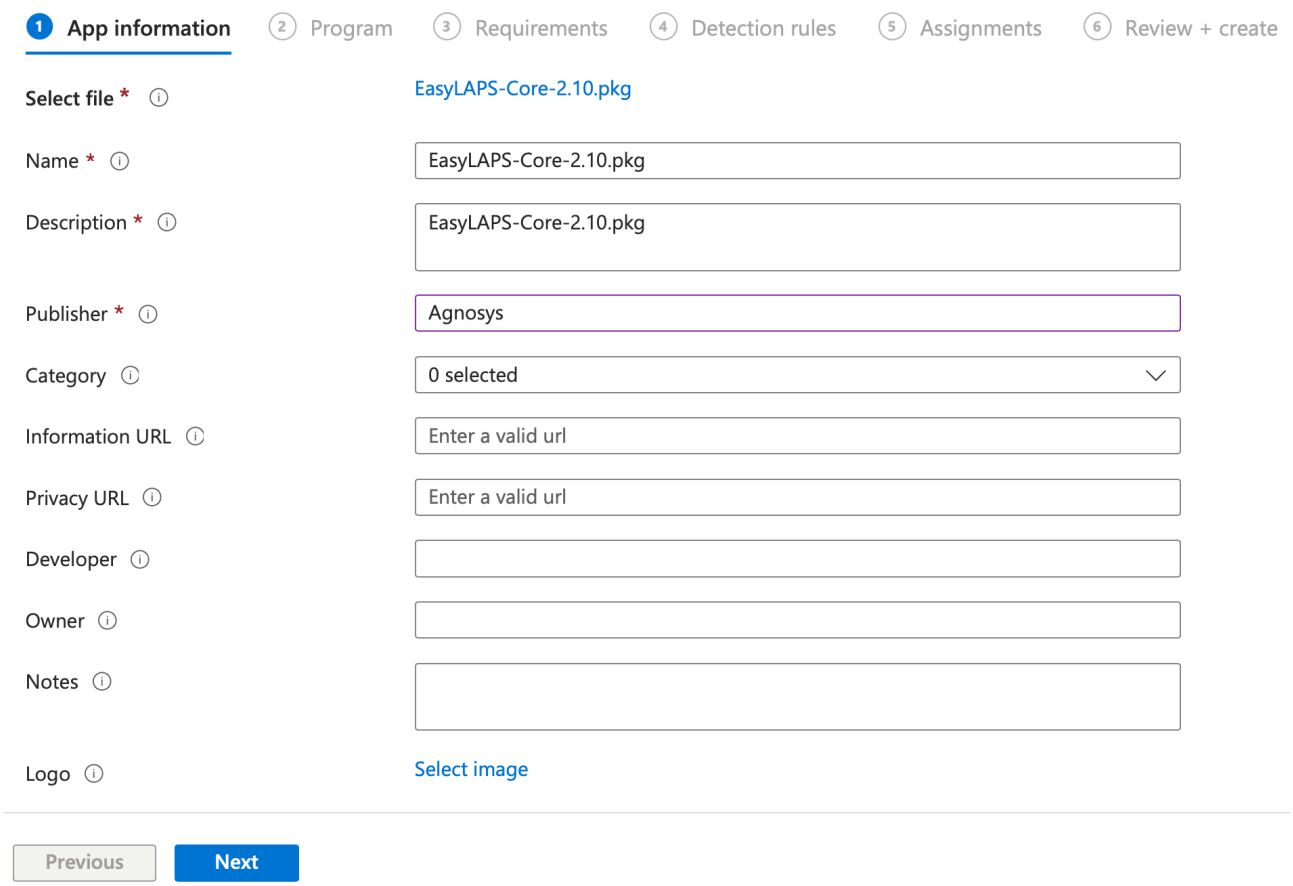
- Detection rules
    - Ignore app version : **No**
    - Detection method table :
        - App bundle ID : **com.agnosys.EasyLAPS-Content**
        - App version : keep current value (e.g. 1.0)

- Assignments
    - Required : Add all devices

- Review + create
    - Create

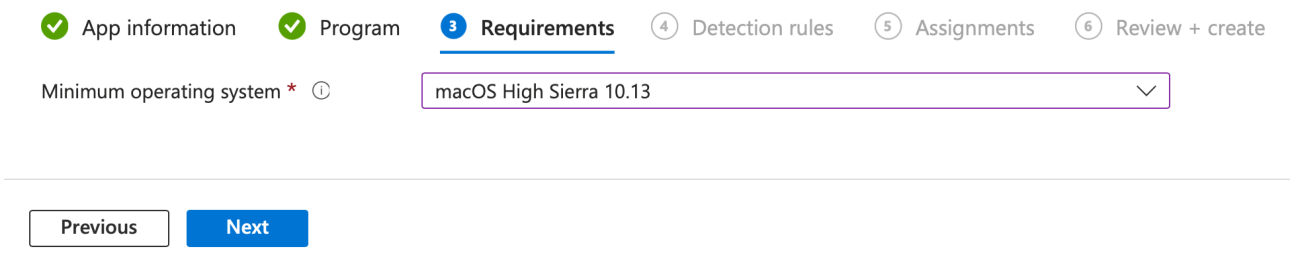
EasyLAPS-Core package

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

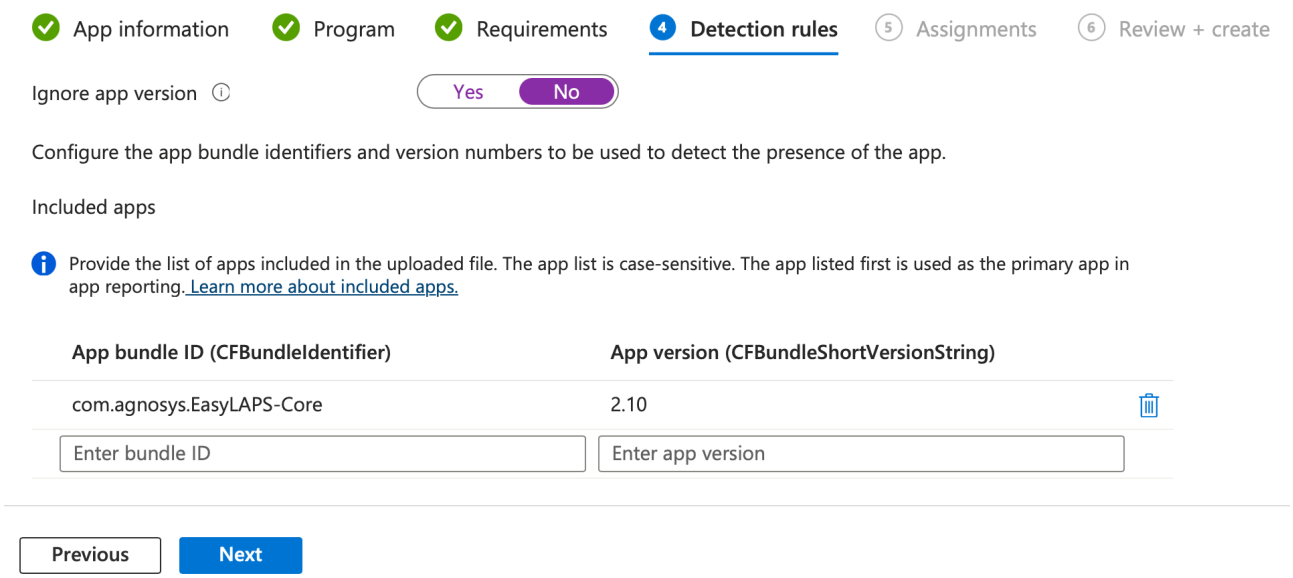


- App information
    - Select file > Select app package file
    - App package file > Select a file > EasyLAPS-Core.pkg > OK
    - Publisher : Agnosys

- Program : no scripts need to be configured



- Requirements
    - Minimum operating system : macOS High Sierra 10.13

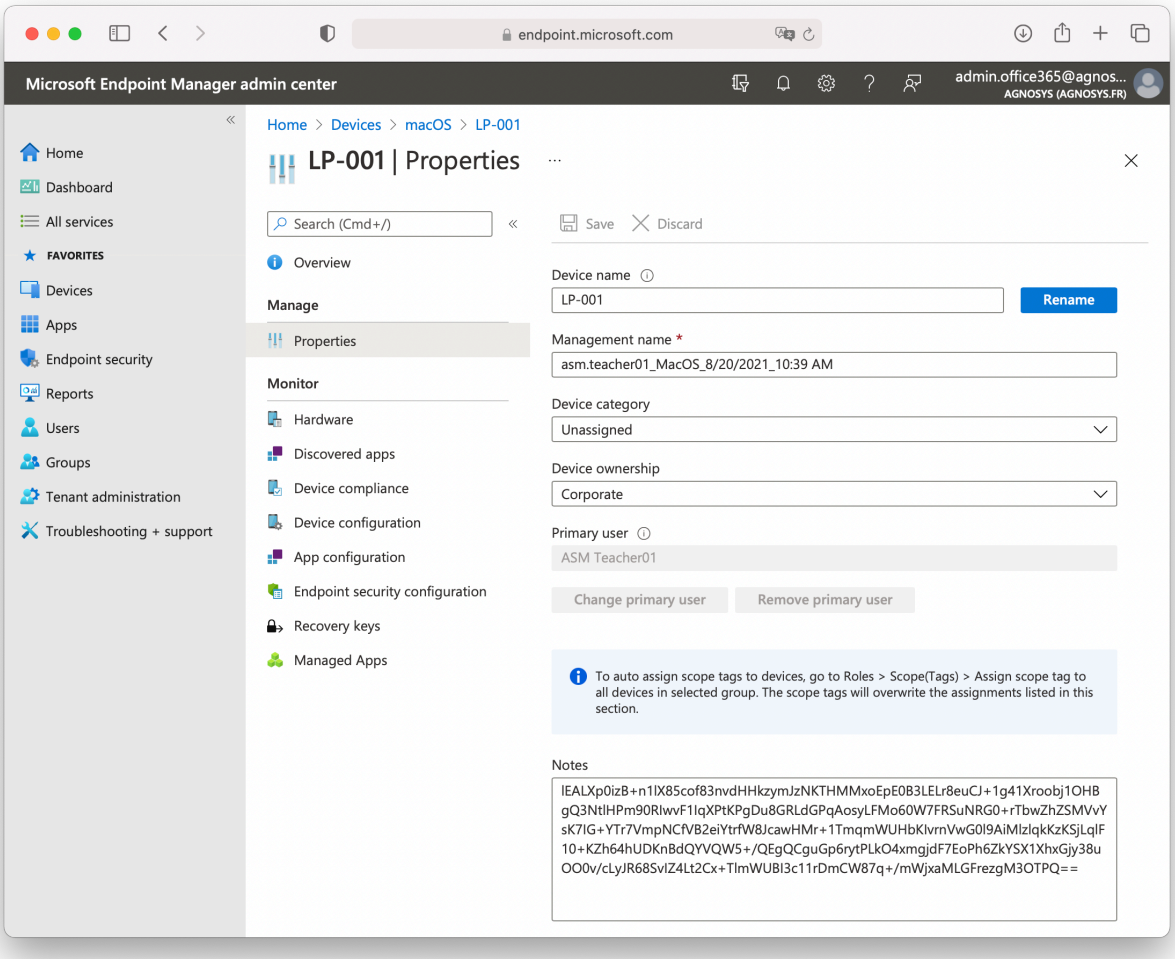


- Detection rules
    - Ignore app version : **No**
    - Detection method table :
        - App bundle ID : **com.agnosys.EasyLAPS-Core**
        - App version : keep current value (e.g. 2.10)

- Assignments
    - Required : Add all devices

- Review + create
    - Create

Result of a successful rotation



In this example, after the first successful rotation, the new password is visible in the field named "Notes" and the password is stored in encrypted form.

Provisioning Miradore

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

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.EasyLAPS.mobileconfig
- Name : EasyLAPS-Custom configuration profile > Create

EasyLAPS-Content package

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

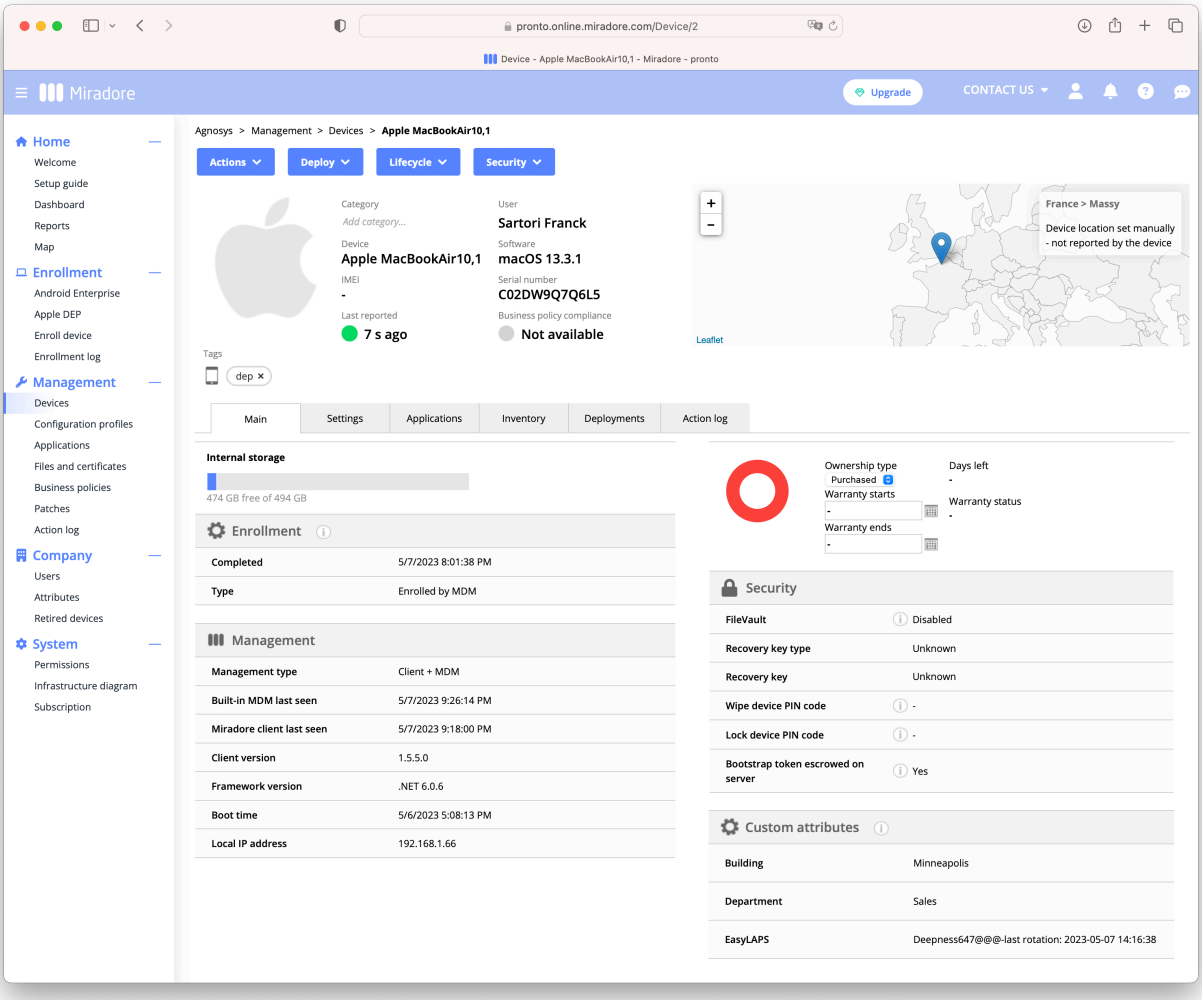
EasyLAPS-Core package

The EasyLAPS-Core package is defined with the following steps :
- Management > Applications > Applications tab > Add
- macOS application > PKG (Uploaded)
- File > Select file > EasyLAPS-Core.pkg
- Application name : EasyLAPS-Core
- Bundle identifier : com.agnosys.EasyLAPS-Core
- Version : the version imported (e.g. 1.49)
- 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 : EasyLAPS
- Double-click on the Business policy
- Add > Application > Check EasyLAPS-Content and EasyLAPS-Core > Add
- Add > Configuration profile > Check EasyLAPS-Custom configuration profile > Add
- Click on the Items tab and check the Business policy content
- Click on "Enable"

Result of a successful rotation



After the first successful rotation, the new password is visible in the Custom Attribute named "EasyLAPS". In this example, the password of type passphrase is stored in clear text.

Note that the EasyLAPS Custom Attribute is created automatically if missing.

Provisioning Mosyle Business

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

General configuration

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

Custom configuration profile

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

EasyLAPS-Content package

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

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

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

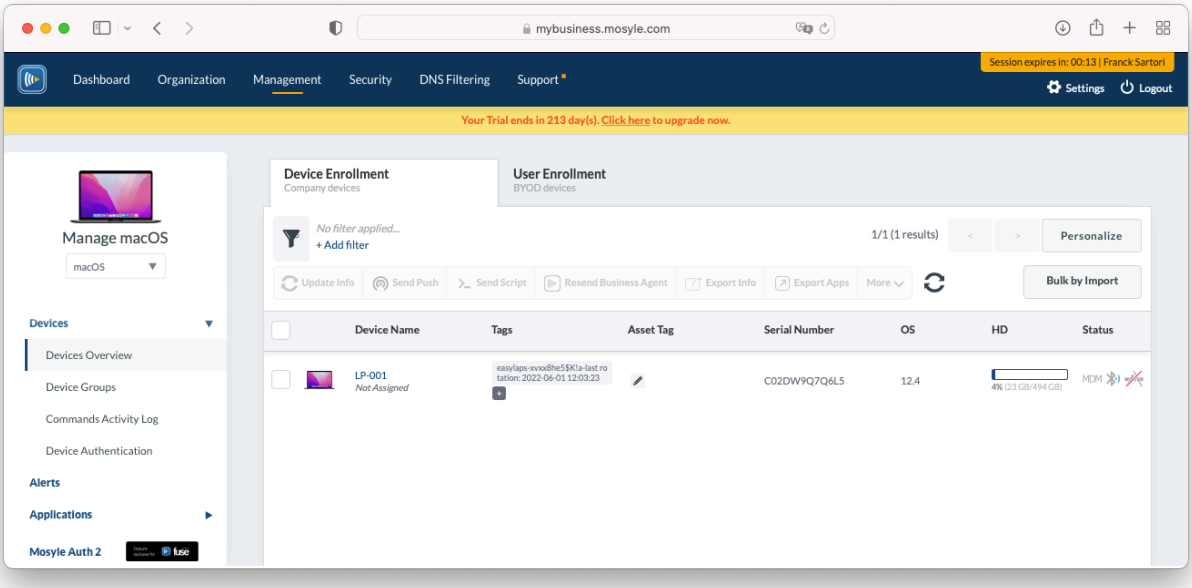
EasyLAPS-Core package

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

The EasyLAPS-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 > EasyLAPS-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.EasyLAPS-Core
- Enable "This app is Signed"
- Save

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

Result of a successful rotation



After the first successful rotation, the new password is visible as a Tag starting with the mandatory prefix "easylaps-". In this example, the password is stored in clear text.

Provisioning Mosyle Manager

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

General configuration

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

Custom configuration profile

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

EasyLAPS-Content package

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

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

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

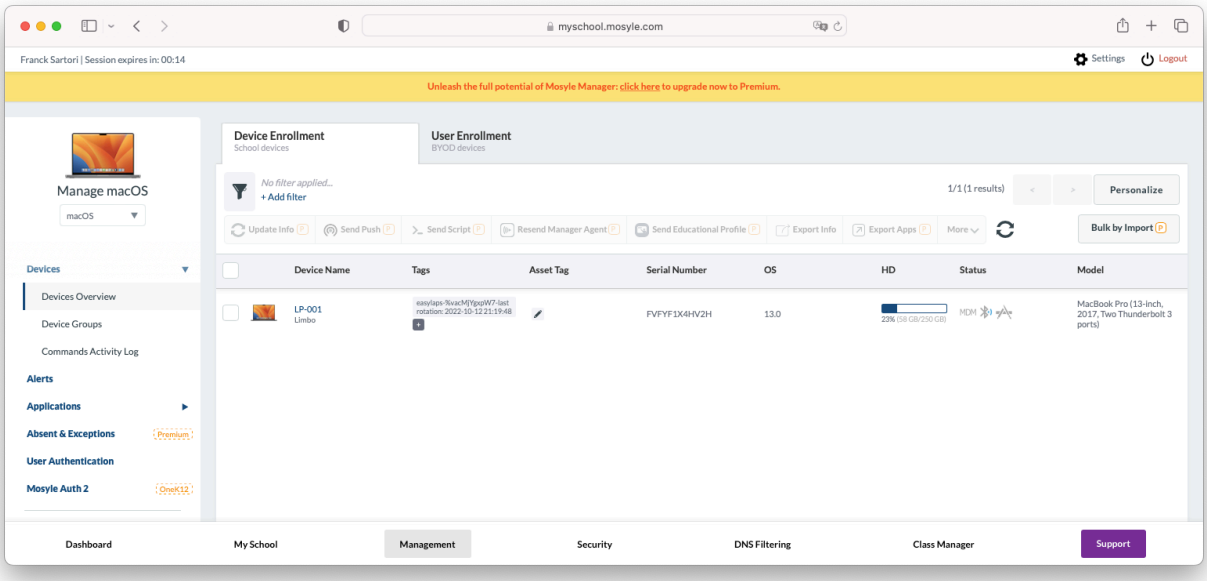
EasyLAPS-Core package

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

The EasyLAPS-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.EasyLAPS-Core
- Enable "This app is Signed"
- Save

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

Result of a successful rotation



After the first successful rotation, the new password is visible as a Tag starting with the mandatory prefix "easylaps-". In this example, the password is stored in clear text.

Provisioning SimpleMDM

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-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 EasyLAPS.

General configuration

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

Custom configuration profile

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

EasyLAPS-Content package

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

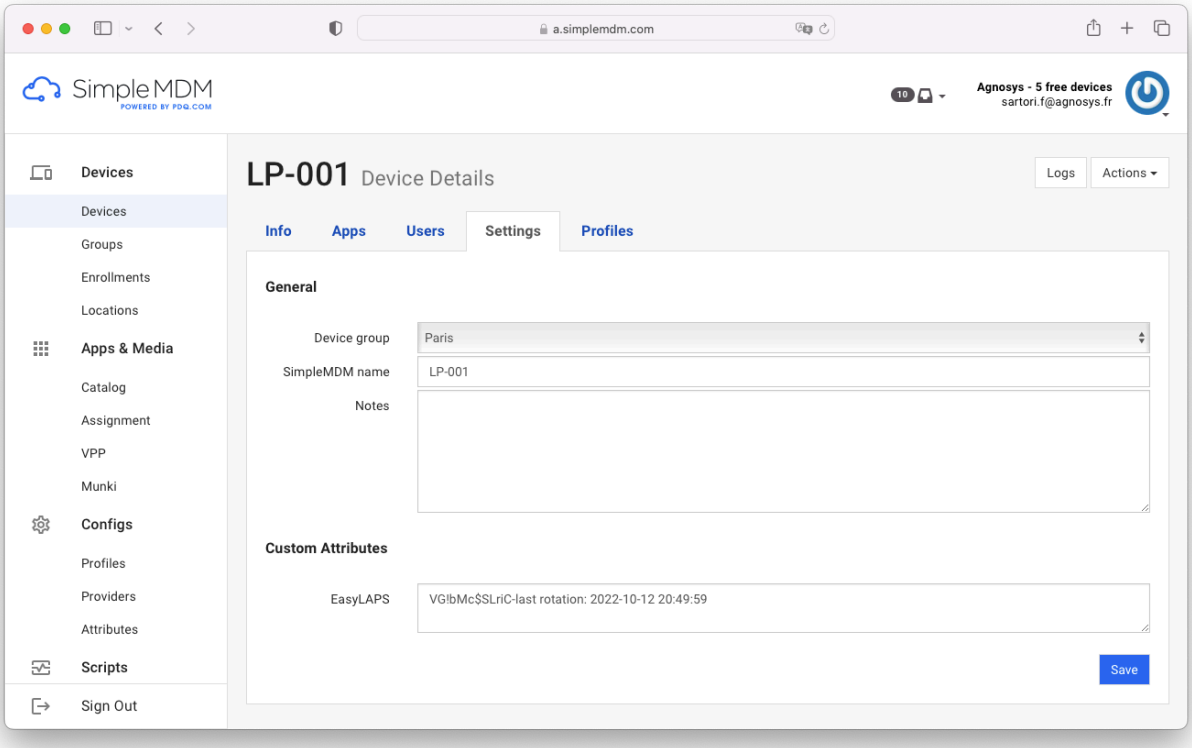
The EasyLAPS-Content package is provisioned with the following steps :
- Apps & Media > Assignment
- Create Assignment Group
    - Name : EasyLAPS
    - Type : Standard — Auto deploy enabled
    - Save
- EasyLAPS
    - Search for an app or media to add > EasyLAPS-Content.pkg
    - Search for a group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

EasyLAPS-Core package

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

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

Result of a successful rotation



After the first successful rotation, the new password is visible in the Custom Attribute named "EasyLAPS". In this example, the password is stored in clear text.

Note that the EasyLAPS Custom Attribute is created automatically if missing.

Provisioning VMware Workspace ONE

Three components must be automatically deployed to the devices :
- a Custom configuration profile
- an EasyLAPS-Content package
- the EasyLAPS-Core package.

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

General configuration

The scope of the components installation is here all devices.

Custom configuration profile

Open the VMware Workspace ONE console.

Go to Resources > Profiles & Baselines > Profiles.

Click on "Add" > "Add Profile".

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

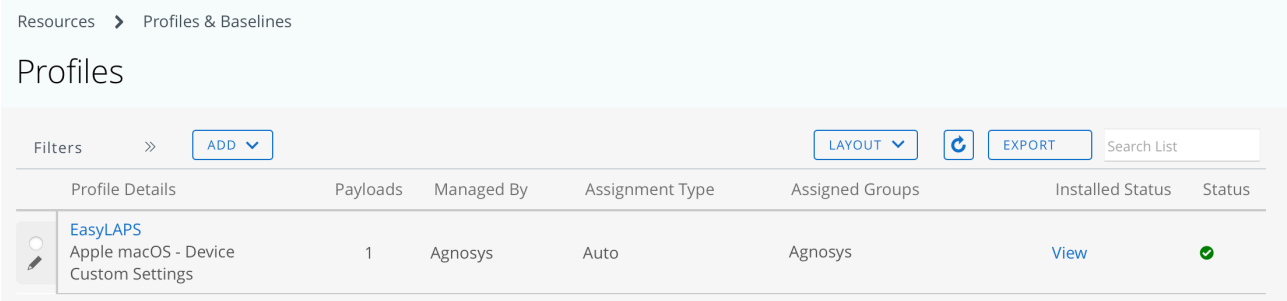
Name the configuration profile (e.g. "EasyLAPS") and optionally add a description (e.g. "EasyLAPS configuration").

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

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

Click on "Next".

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

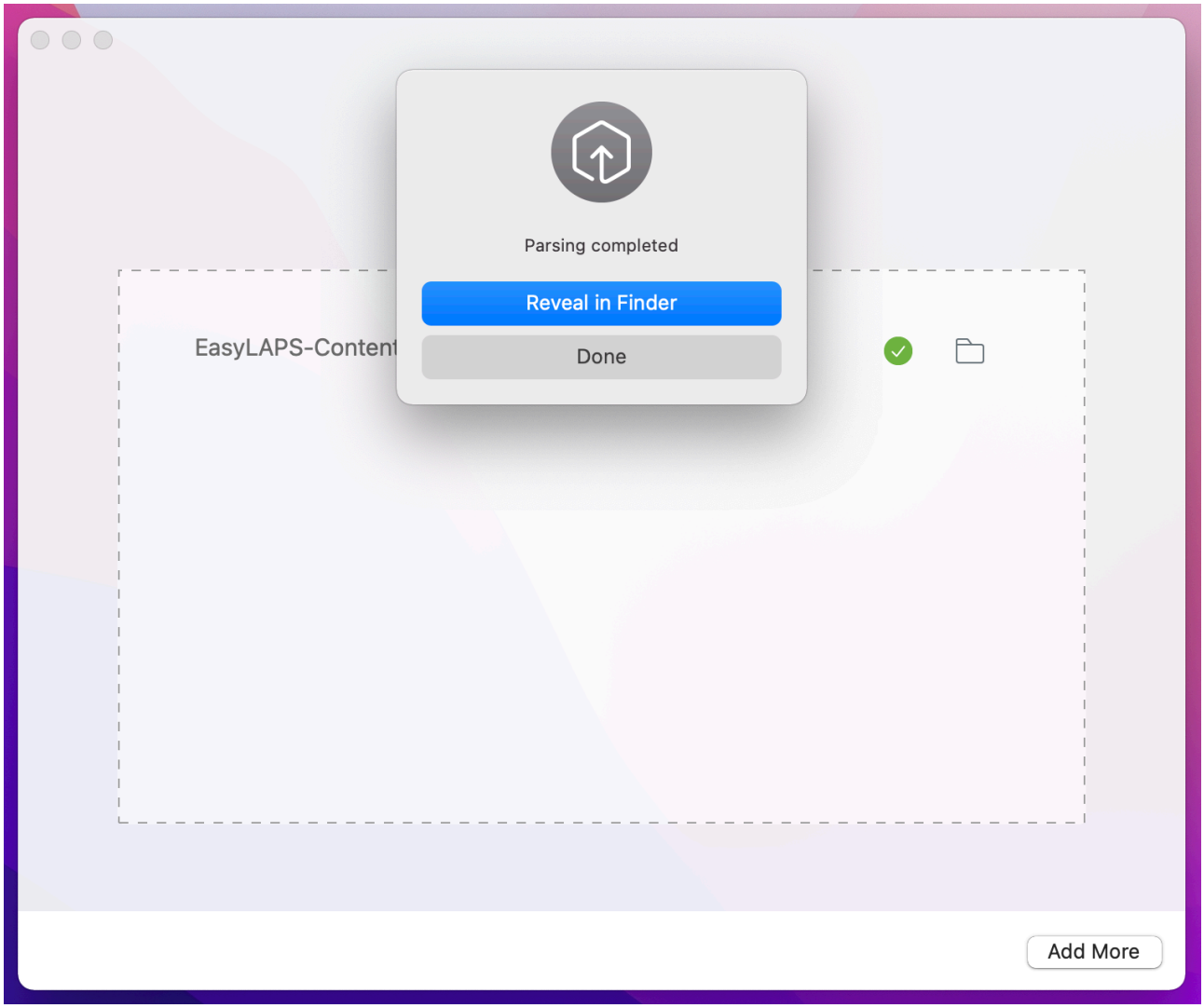


Check that the Custom configuration profile is published and assigned.

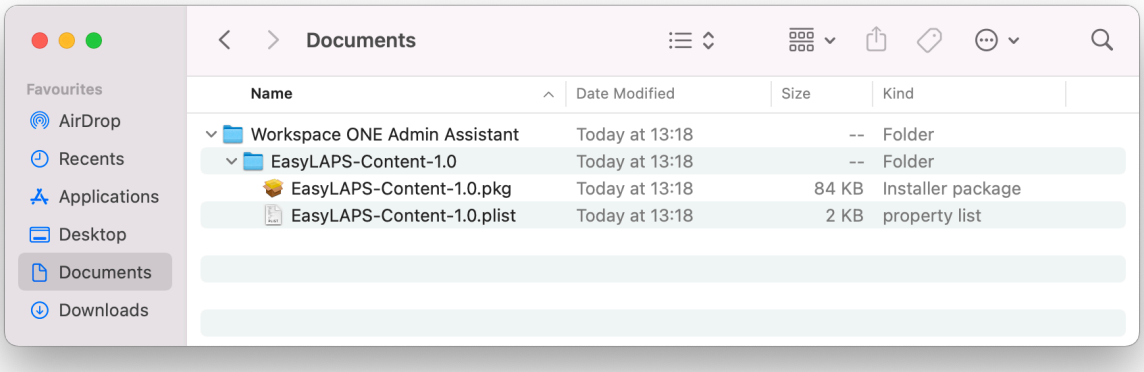
EasyLAPS-Content package

Open /Applications/Workspace ONE Admin Assistant.

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



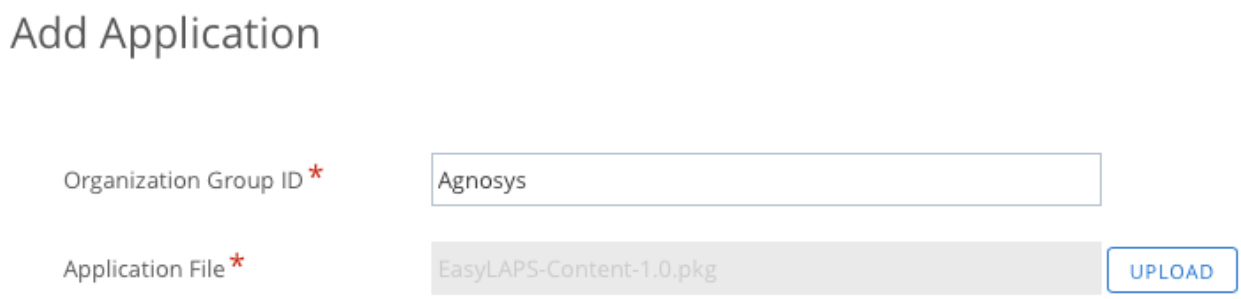
Once the parsing is completed, click on "Reveal in Finder".



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

Open the VMware Workspace ONE console.

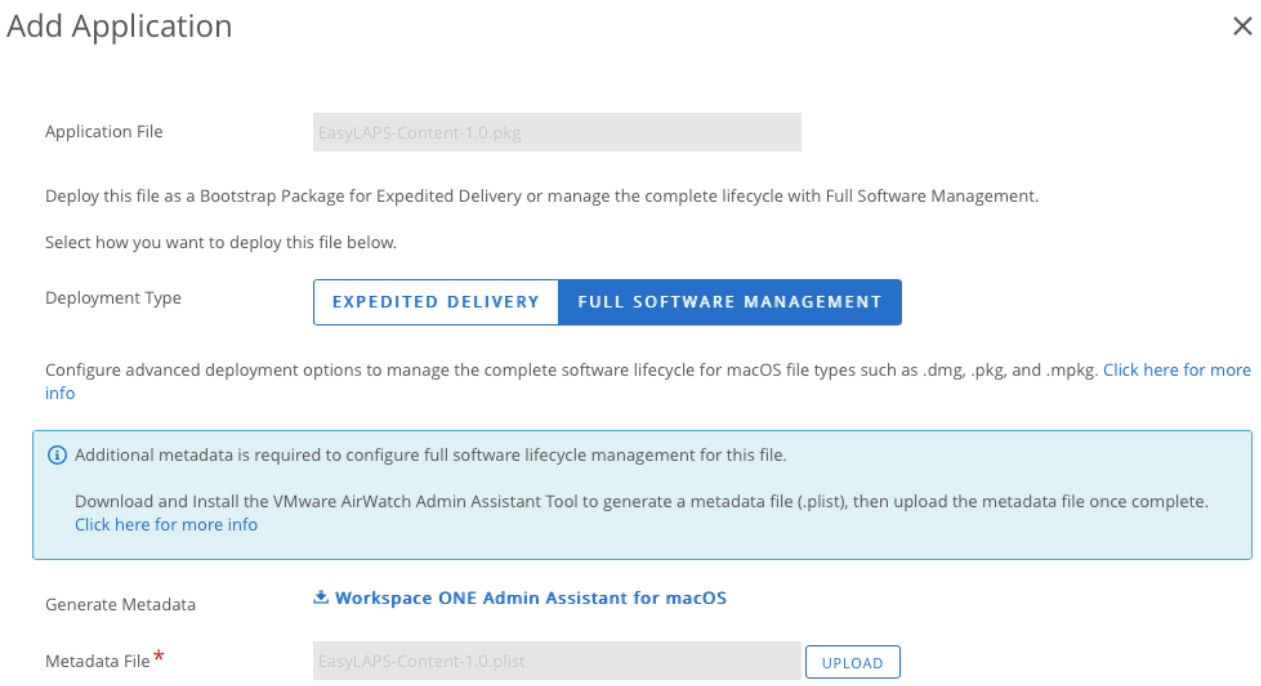
Go to Resources > Apps > Native.
Click on "Add" > "Application File".



Select the Organization Group that encompasses the devices that are to be installed with EasyLAPS.

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

Click on "Continue".

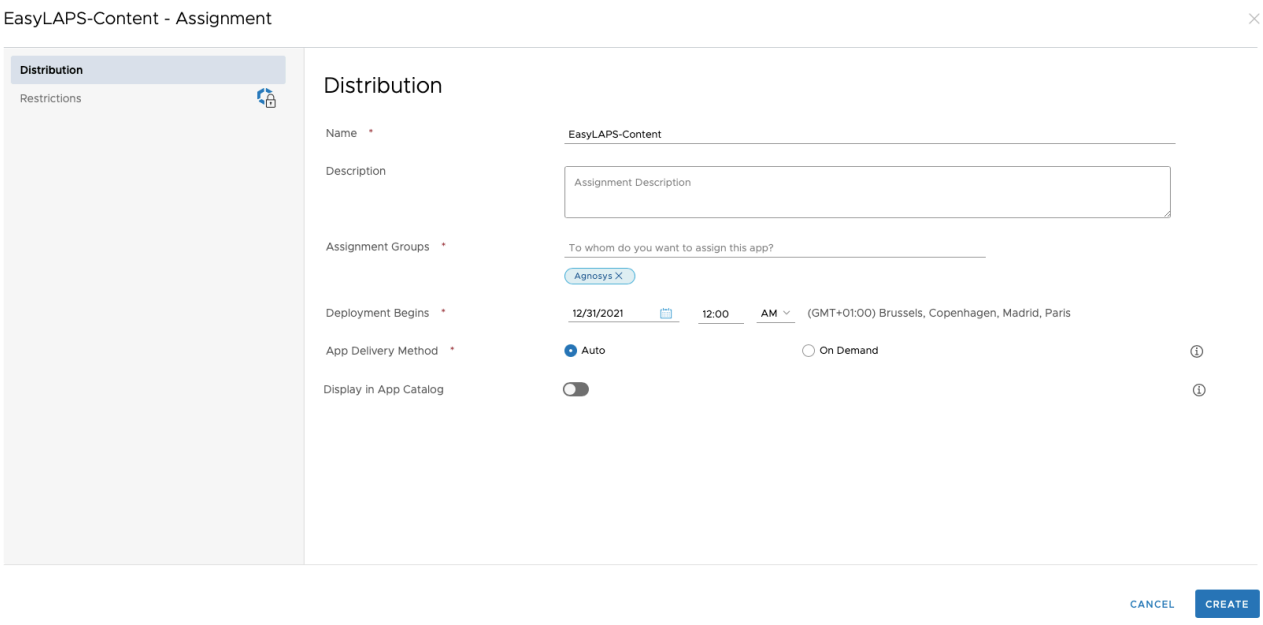


Select "Full Software Management".

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

Click on "Continue".

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



Complete the assignment form :
- Name : EasyLAPS-Content

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

Click on "Create".

In the Assignment pane, click on "Save".

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

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

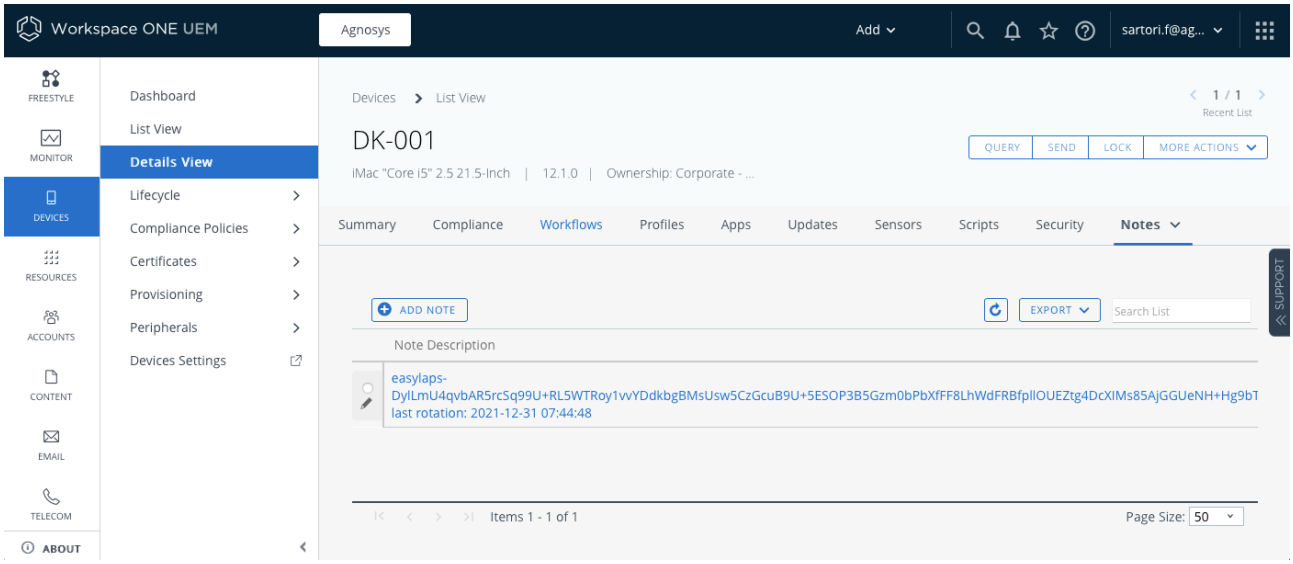
EasyLAPS-Core package

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

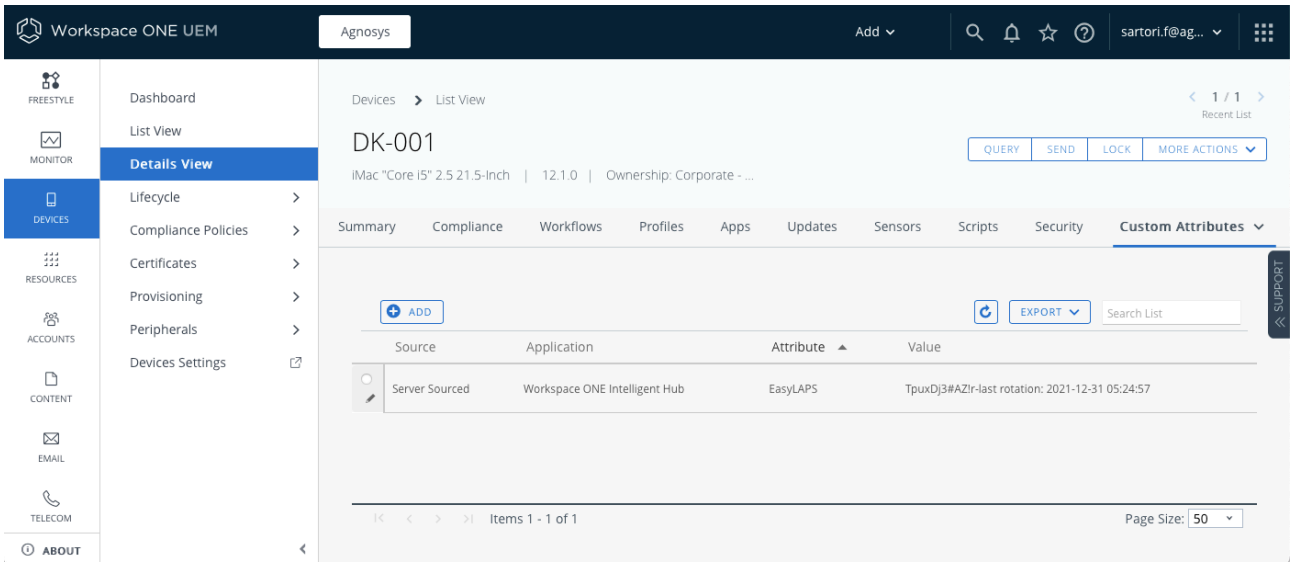
Go to Resources > Apps > Native and check that the application is published and assigned.

Result of a successful rotation

After the first successful rotation, the new password is visible at a place that depends of the EasyLAPS Logic activated.



With Logic #1 : the password is stored in encrypted form in a note within the "Notes".

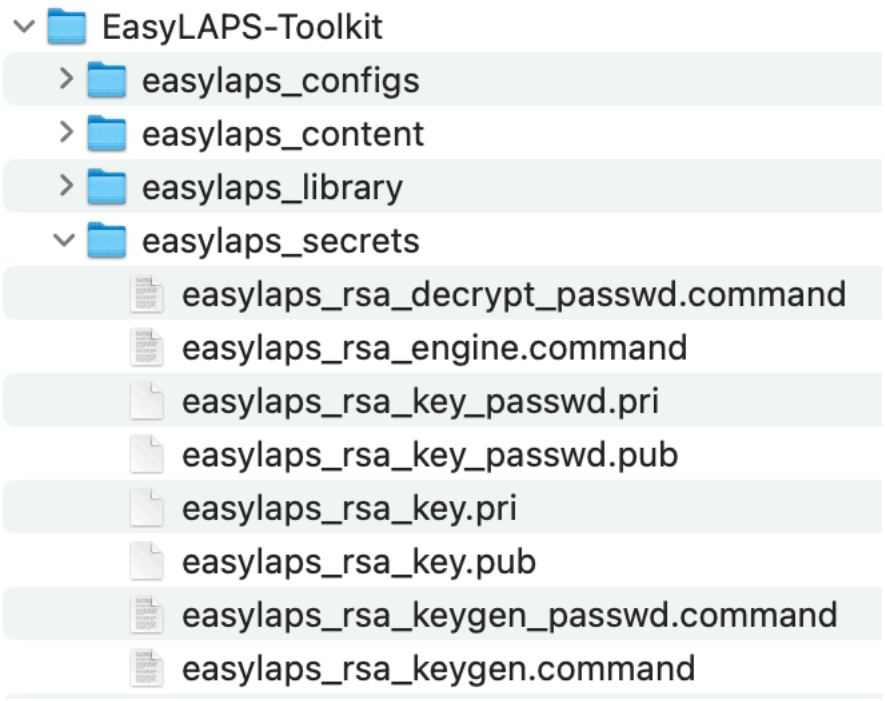


With Logic #2 : the password is stored in clear text in the EasyLAPS Custom attribute.

Revealing an encrypted password

First copy the encrypted password from the MDM (one-line string ending exactly with two "=" characters).

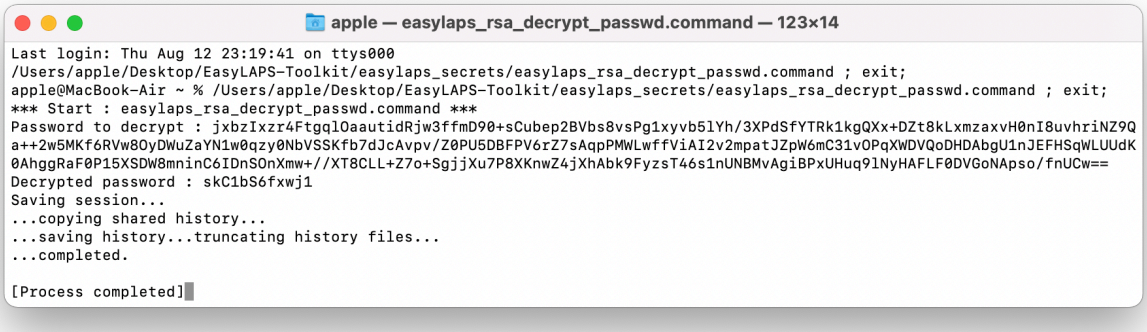
It is not required to strip the prefix "easylaps-" when it exists before the encrypted password.



Open the "EasyLAPS-Toolkit" folder.

Open the "easylaps_secrets" subfolder.

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



Paste the encrypted password and press the Return key.

The decrypted password is displayed at the line "Decrypted password".

Note that the only elements required in the EasyLAPS-Toolkit to reveal an encrypted password are those 2 files in the same folder :
- easylaps_rsa_decrypt_passwd.command
- easylaps_rsa_key_passwd.pri

Important notice

When EasyLAPS Logic #1 is enabled, it is crucial that the file "easylaps_rsa_key_passwd.pri" is not lost. Without the private key contained in this file, no password currently stored in encrypted form in the MDM can be decrypted. However, as the rotation does not rely on reading this password, generating a new key pair and deploying the new public key will remediate the loss of the initial private key when the next rotation will occur.

Renewing EasyLAPS license

An EasyLAPS license is valid for one year. An annual license can be purchased at any time before the current license expires. The message sent on completion of the order contains both the new license code and the new expiration date. The new license code can be used as soon as it is supplied. To apply the new license code, please follow these steps.

Editing the LICENSE key of the deployed Custom configuration profile

If your MDM solution offers an interface for directly modifying, and not just reading, the keys of the deployed Custom configuration profile, you can choose to carefully replace the current license code with the new license code in the LICENSE key.

Warning : Bear in mind that the EasyLAPS configuration file stored in the EasyLAPS Toolkit will still contain the current and probably soon-to-expire license code, unless you also update this file as well.

• **Jamf Pro**

The Custom configuration profile can be edited with the following steps :
- Computers > Content Management > Configuration Profiles
- Click on the name of the profile (e.g. EasyLAPS-Custom configuration profile)
- Application & Custom Settings > Upload
- Edit
- Carefully replace the current license code with the new license code in the LICENSE key.
- Save.

• **SimpleMDM**

The Custom configuration profile can be edited with the following steps :
- Configs > Profiles > EasyLAPS-Custom configuration profile
- Carefully replace the current license code with the new license code in the LICENSE key.
- Save.

• **VMware Workspace ONE**

Open the VMware Workspace ONE console.

Go to Resources > Profiles & Baselines > Profiles.

Click on the EasyLAPS profile to display its details then click on "Add version".

Click inside the "Custom Settings" payload then carefully replace the current license code with the new license code in the LICENSE key.

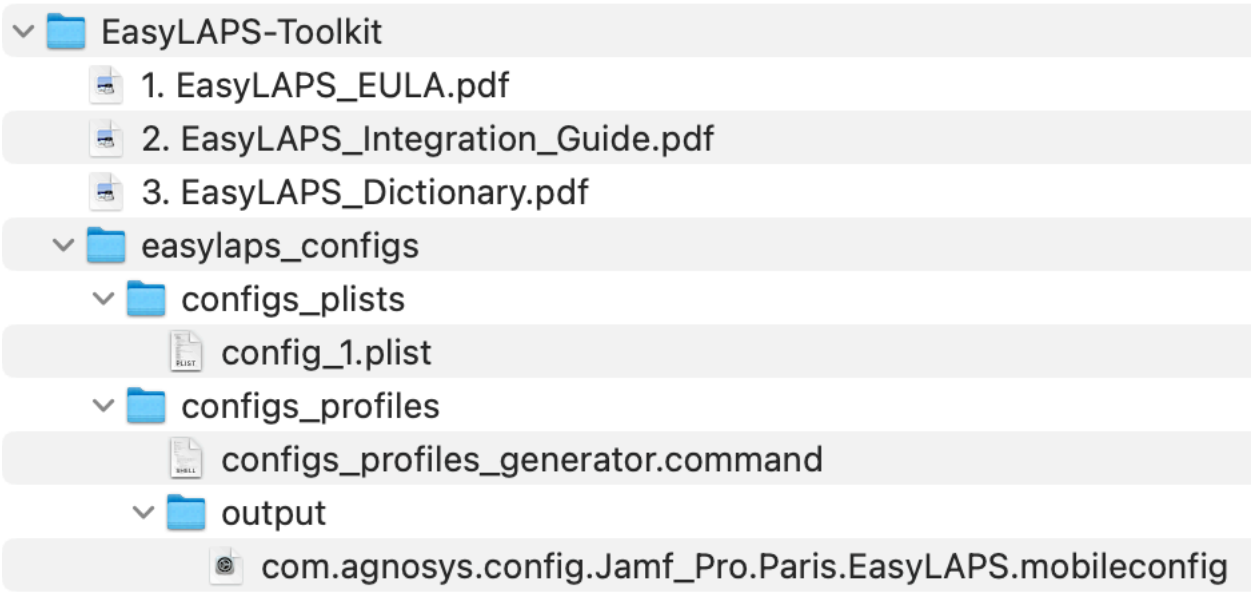
Click on "Next".

Click on "Save and Publish".

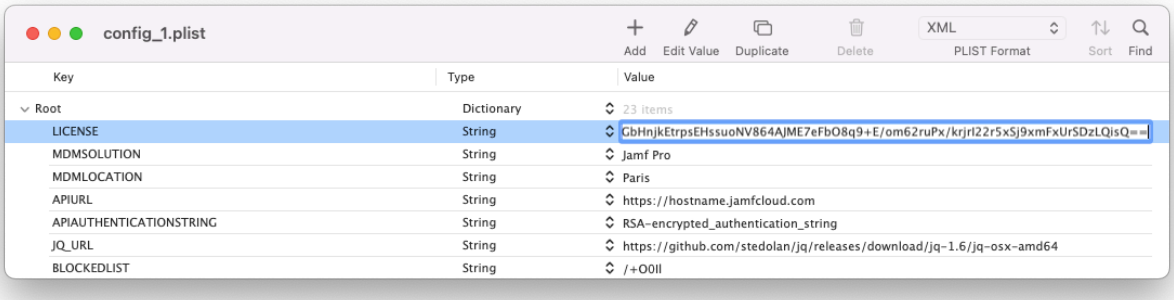
Editing the EasyLAPS configuration file(s)

If your MDM solution does not offer an interface for directly modifying, and not just reading, the keys of the deployed Custom configuration profile, follow these instructions.

First of all, backup your current EasyLAPS-Toolkit folder.



It contains particularly the EasyLAPS configuration file named by default "config_1.plist" and the current Custom configuration profile that was generated from the EasyLAPS configuration file using the script named "configs_profiles_generator.command".



Open the EasyLAPS configuration file and replace the current license code with the new license code in the LICENSE key. The license key is a one-line string ending exactly with two "=" characters.

Save the EasyLAPS configuration file, then follow these instructions :

1. Refer in this documentation to the section titled "EasyLAPS configuration files to Custom configuration profiles conversion" to convert your updated EasyLAPS configuration file to a Custom configuration profile, if applicable.

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, replacing the previous one.

Updating EasyLAPS

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

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

However, there is a shortcut. If you want to distribute a newer version of EasyLAPS without modifying the configuration, go directly to the "EasyLAPS Core package" section below.

EasyLAPS Toolkit

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

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

2. Download and install the updated version of EasyLAPS Toolkit

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

4. Copy from the previous folder the **.plist files** stored in easylaps_configs > configs_plists to the updated folder in easylaps_configs > configs_plists. Be sure to keep the updated template named "config_1.plist".

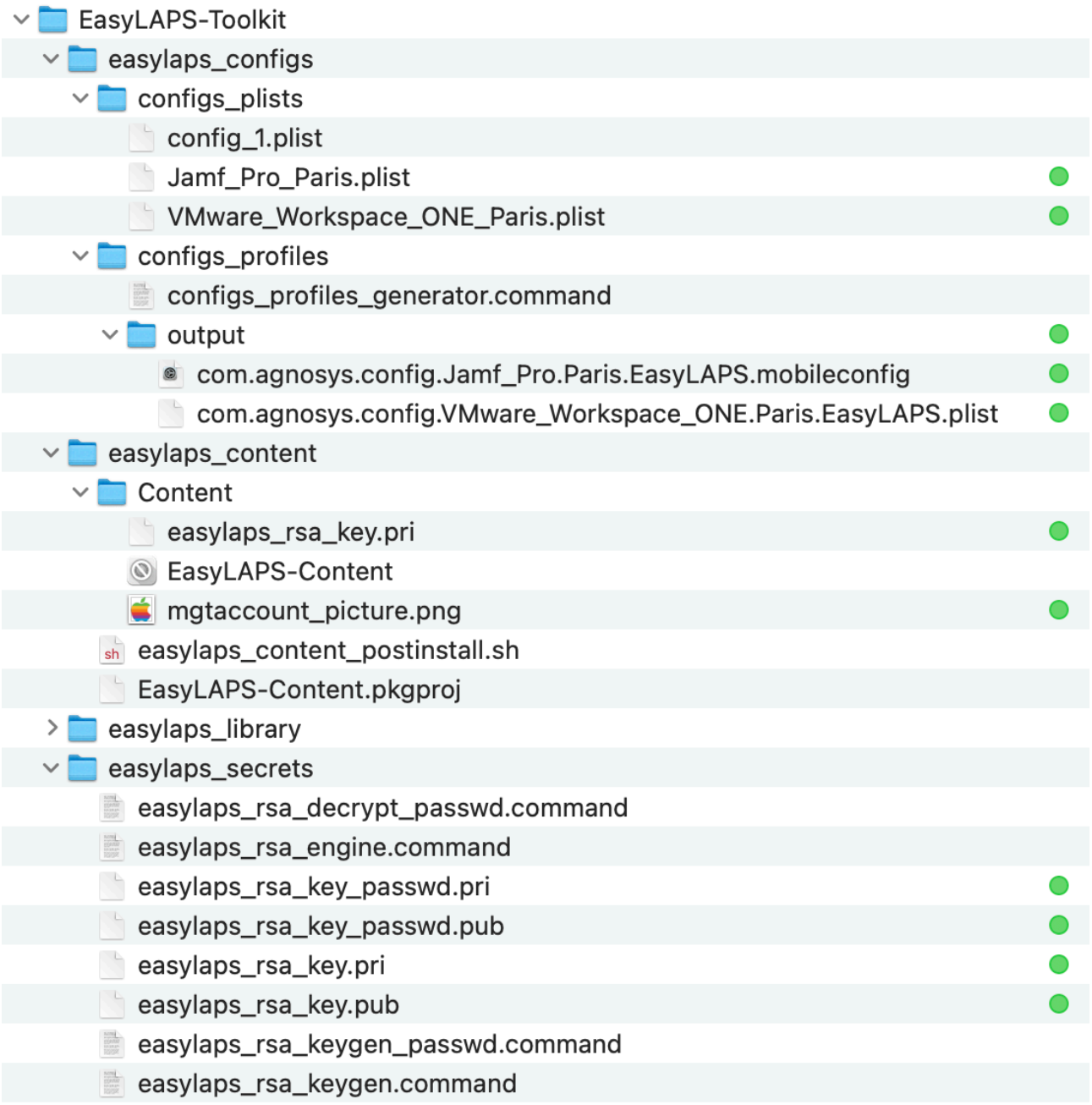
5. Copy from the previous folder the **.mobileconfig and .plist files** stored in easylaps_configs > configs_profiles > output to the updated folder in easylaps_configs > configs_profiles > output

6. Copy from the previous folder **the content of the folder** easylaps_content > Content except **EasyLAPS-Content.app** to the updated folder in easylaps_content > Content

7. Copy from the previous folder **the following 4 files** stored in easylaps_secrets to the updated folder in easylaps_secrets :

    - easylaps_rsa_key_passwd.pri (file created only when implementing logic #1)
    - easylaps_rsa_key_passwd.pub (file created only when implementing logic #1)
    - easylaps_rsa_key.pri
    - easylaps_rsa_key.pub

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


EasyLAPS-Toolkit
easylaps_configs
configs_plists
config_1.plist
Jamf_Pro_Paris.plist
VMware_Workspace_ONE_Paris.plist
configs_profiles
configs_profiles_generator.command
output
com.agnosys.config.Jamf_Pro.Paris.EasyLAPS.mobileconfig
com.agnosys.config.VMware_Workspace_ONE.Paris.EasyLAPS.plist
easylaps_content
Content
easylaps_rsa_key.pri
EasyLAPS-Content
mgtaccount_picture.png
easylaps_content_postinstall.sh
EasyLAPS-Content.pkgproj
easylaps_library
easylaps_secrets
easylaps_rsa_decrypt_passwd.command
easylaps_rsa_engine.command
easylaps_rsa_key_passwd.pri
easylaps_rsa_key_passwd.pub
easylaps_rsa_key.pri
easylaps_rsa_key.pub
easylaps_rsa_keygen_passwd.command
easylaps_rsa_keygen.command

EasyLAPS configuration file(s)

Complete your current .plist file(s) to implement as desired new capabilities of EasyLAPS, helping you with the updated EasyLAPS Dictionary and the updated config_1.plist file. The release notes indicate, for each version of EasyLAPS, which keys may have been modified, deprecated, or become obsolete. Do not hesitate to contact EasyLAPS support if you need any clarifications.

Warning : Ensure that your EasyLAPS configuration file(s) contain(s) your current EasyLAPS license, as it may have been updated directly in the MDM solution, but not in the EasyLAPS 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 EasyLAPS configuration file(s) using your preferred Property List editor to ensure no structural errors are introduced accidentally. The only key supported for direct modification is the license code.

Custom configuration profile(s)

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

EasyLAPS Content package

As the private key contained in the file "easylaps_rsa_key.pri" is static and if you didn't update the management account picture, no action is necessary.

If you updated the management account picture :
- refer to this documentation to build an updated EasyLAPS-Content package
- refer to this documentation and the MDM documentation to deploy the updated package.

EasyLAPS Core package

1. Download the updated version of EasyLAPS Core.

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

Edge cases

• The current password of the local administrator account is not unique on all the Mac deployed

Defining the current password of the local administrator account is a requirement for the execution of the first rotation. In the context where the current password of the local administrator account is not unique on all the Mac deployed, three solutions are offered.

Solution #1 : Generate a Custom configuration profile containing all known current passwords and distribute it to all Mac. All defined passwords in the array will be tested until the one matching the current password is found. Always put the most likely current password at index 0 to reduce authentication errors as much as possible.

Solution #2 : Generate a Custom configuration profile configured for Logic #2 and the most likely current password and distribute it to all Mac. The first rotation will fail on the couple of devices that use a different current password. For each of these devices, enter manually its known current password in its inventory details, in the same attribute as for the other devices. The value to be entered is only the password in clear text, with the mandatory prefix "easylaps-" (exactly) when using Mosyle Business or Mosyle Manager as the management solution. You may decide to migrate to Logic #1 once the first rotation has been successful on all the Mac.

Solution #3 : Generate one Custom configuration profile per different possible current password used by the devices. Use the MDMLOCATION key to differentiate each Custom configuration profile generated. Then distribute each generated Custom configuration profile to the group of devices that share the matching current password.

• The new password to be deployed on the Mac must be a determined one and not a randomized one

This case is managed by the usage of the MGTACCOUNTPASSWORDDETERMINED key. This key does not exist intentionally in the EasyLAPS configuration file template and must be added manually.

Choose a password that complies to the local account password policy that meets your organization's requirements and often enforced via a Passcode Configuration profile. Then use the script "easylaps_rsa_engine" to generate an encrypted version of this password and paste the full value including the "RSA-" prefix in the MGTACCOUNTPASSWORDDETERMINED key. This process is the same as the one used to populate the MGTACCOUNTPASSWORD key.

EasyLAPS will enforce the usage of this password instead of generating a randomized password. Note that this password is used "as is" and therefore is not transformed in any way by EasyLAPS.

Troubleshooting

The troubleshooting must be done from the opened session of an administrator account.

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.

Display the follow-up file

Open the Terminal utility located in /Applications/Utilities.

Type the following command :

```
sudo defaults read "/Library/Application Support/EasyLAPS/easylaps.plist"
```

The informations displayed are :

- LASTEXECUTIONDATE : last execution date in the format "YYYY-MM-DD HH:MM:SS"

- LASTEXECUTIONDATEEPOCHTIME : last execution date in the format "epoch time"

- LASTPASSWORDROTATIONDATE : last successful password rotation date in the format "YYYY-MM-DD HH:MM:SS"

- LASTPASSWORDROTATIONDATEEPOCHTIME : last successful password rotation date in the format "epoch time"

- MGTACCOUNTPICTUREFINGERPRINT : md5 fingerprint of the current management account picture

- ROTATIONDEFERRAL : "true" means that a rotation deferral is active

- SAFEMODE : "true" means that the new password has been forcibly stored in the EasyLAPS Keychain until the next rotation occurs successfully

- STATUSMESSAGE : exit message of the latest rotation triggered (raw message for a success, information or error event)

- FILEWAVESTATUSMESSAGE : exit message of the latest rotation triggered (success, information or error) defined by the optional FileWave Integration

- JAMFPROSTATUSMESSAGE : exit message of the latest rotation triggered (success, information or error) defined by the optional Jamf Pro Integration

- MICROSOFTINTUNESTATUSMESSAGE : exit message of the latest rotation triggered (success, information or error) defined by the optional Microsoft Intune Integration

- VMWAREWORKSPACEONESTATUSMESSAGE : exit message of the latest rotation triggered (success, information or error) defined by the optional VMware Workspace ONE Integration

Please refer to the EasyLAPS-Dictionary for more informations about :
- the FileWave Integration
- the Jamf Pro Integration and the Extension attributes provided in the EasyLAPS-Toolkit
- the Microsoft Intune Integration and the Custom attributes provided in the EasyLAPS-Toolkit
- the VMware Workspace ONE Integration and the Sensors / Custom attributes (to be used in Profiles) provided in the EasyLAPS-Toolkit.

Enable the debug logging manually

Open the Terminal utility located in /Applications/Utilities.

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

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

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

Enter your password.

The debug logs are written in /private/var/log.

The files titled EasyLAPS-easylaps_*date*.log and EasyLAPS-easylaps_starter_*date*.log contain sensitive informations for troubleshooting purpose only, must not be left unattended and can be read by admin users only.

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

Enable the debug logging with Custom configuration profile

Two levels of debug logging can be enabled, depending of the value of the DEBUGMODE key.

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

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

The debug logs are written in /private/var/log.

The files titled EasyLAPS-easylaps_*date*.log and EasyLAPS-easylaps_starter_*date*.log contain sensitive informations for troubleshooting purpose only, must not be left unattended and can be read by admin users only.

The corresponding debug flag is automatically created in /Library/Application Support/EasyLAPS.

Warning : Do not forget to disable the debug logging then delete the EasyLAPS debug logs and the debug flag created once the log analysis is completed.

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

Display the debug logs from the Console utility

Open the Console utility located in /Applications/Utilities.

Select Reports > Log Reports > a file named EasyLAPS-easylaps_*date*.log

Display the debug 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 file named EasyLAPS-easylaps_*date*.log

Enter your password.

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

Run the rotation manually

Open the Terminal utility located in /Applications/Utilities.

Type one of the following command and enter your password when prompted.

To get EasyLAPS options :

```
sudo sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh" --help
```

To trigger the password rotation inside of the rotation schedule :

```
sudo sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh"
```

To trigger the password rotation inside of the rotation schedule ignoring the execution intervals :

```
sudo sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh" --
ignoreintervals
```

To force the password rotation outside of the rotation schedule :

```
sudo sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh" --force
```

When the password rotation is forced, execution probes enabled by the EXECUTION_PROBES Dictionary and the safeguard that prevents rotation when the management account is currently logged in are bypassed.

To roll the management account's password back to the initial password defined in the EasyLAPS configuration file :

```
sudo sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh" --
rollback
```

Enable the trace log with Custom configuration profile

To enable the trace log for informative purposes, set the TRACEMODE key with one of these values :
- "enabled-lf" or "enabled" (exactly) to log in the log file /private/var/log/EasyLAPS-easylaps_trace.log
- "enabled-ul" to log in the Unified Logging under the process "logger"
- "enabled-lf,ul" to log to both destinations (the two options can be placed in any order but must be separated by a comma).

These logs do not contain sensitive informations, can be used to keep track of rotation history and can be read by any standard or admin user.

Display the trace log of type "log file" from the Console utility

Open the Console utility located in /Applications/Utilities.

Select Reports > Log Reports > EasyLAPS-easylaps_trace.log

Display the trace log of type "Unified Logging" from the Terminal utility

Open the Terminal utility located in /Applications/Utilities.

Type the following command to get the log.

```
log show --predicate 'process="logger" and eventMessage contains
"EasyLAPS"'
```

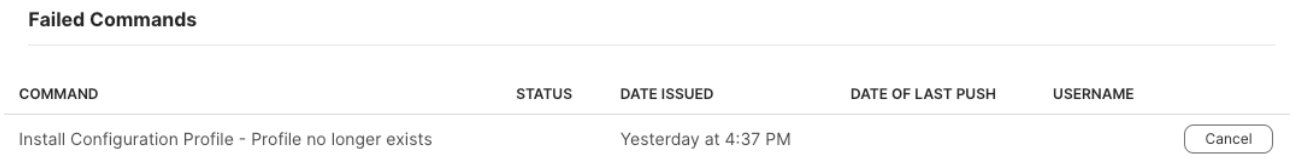
To get the log for the last day only, add the option "--last 1d".

To get the log for the last 60 minutes only, add the option "--last 60m".

Resolve a Custom configuration profile deployment failure

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

In Jamf Pro, open the inventory record of a computer that fails to install the Custom configuration profile then click on the "Management" tab.



If you see this error, you might be in a context where the value of the SYMBOLSLIST key must be encoded.

1. Open the EasyLAPS configuration file and get the current value of the SYMBOLSLIST key, e.g. **!@#$%**

2. Open the Terminal utility located in /Applications/Utilities.

3. Type the following command to generate the encoded value :

```
printf "%s" "base64-$(printf "%s" "!@#$%" | base64)"
```

For the string of symbols **!@#$%** between double quotes, the generated value is **base64-IUAjJCU=**

4. In the EasyLAPS configuration file, replace the current value of the SYMBOLSLIST key with the generated value, including the prefix "base64-".

5. Save the EasyLAPS configuration file.

6. Refer in this documentation to the section titled "EasyLAPS configuration files to Custom configuration profiles conversion" to convert your updated EasyLAPS configuration file to a Custom configuration profile, if applicable.

7. 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, replacing the previous one.

Info code matrix

This matrix does not exempt from reading this Integration Guide and is designed to be an help before contacting EasyLAPS support.

The issues associated with the Info codes referenced in the matrix are expected to be transient.

For each key indicated in this matrix, please refer to the EasyLAPS Dictionary for the expected value.

Info	Message	Details
2	EasyLAPS script executed with option --rollback and current password is already the initial password. No rotation required.	The current management account password is the initial password ; therefore, no rotation to this password is due.
3	Current password is already the determined password. No rotation required.	The current management account password is the determined password ; therefore, no rotation to this password is due.
4	Management account password not expired. No rotation required.	No password rotation has been defined as being due.
6	Management account password collected.	The management account password has been successfully collected and written to storage for use by a script.
9	EasyLAPS execution interval not exceeded.	EasyLAPS wakes up every hour, and upon this wake-up, it has determined that the number of seconds defined by the EXECUTION_INTERVAL key has not yet passed since the last execution.
71	Rotation deferral : active. Initial password : yes. [...]	The grace period is active, and the message indicates the number of days remaining before the first rotation. The grace period settings are defined in the ROTATION_DEFERRAL dictionary, with a default of 7 days after the first installation of EasyLAPS.
183	Directory Service is unavailable during execution probes.	The Directory Service is unavailable while execution probes are running. The scheduled rotation will be retried during the next EasyLAPS execution.
185	Low Battery Charge detected.	The laptop battery has less than 2% charge remaining. The scheduled rotation will be retried during the next EasyLAPS execution, provided the remaining charge exceeds 2% at that time.
187	Running Mac App Store Software Installation.	An execution probe has detected that a Mac App Store software installation is in progress, by monitoring the installd and appinstalld processes. The scheduled rotation will be retried during the next EasyLAPS execution, provided these processes are no longer running. Although not recommended, this execution probe can be disabled by setting the EXECUTION_PROBES > MAC_APP_STORE_SOFTWARE_INSTALLATION key to "false".
188	Running macOS Software Installation detected.	An execution probe has detected that a macOS Software Installation is in progress by monitoring the system_installd and osinstallersetupd processes. The scheduled rotation will be retried during the next EasyLAPS execution, provided these processes are no longer running. Although not recommended, this execution probe can be disabled by setting the EXECUTION_PROBES > MACOS_SOFTWARE_INSTALLATION key to "false".
189	Running macOS Software Update detected.	An execution probe has detected that a macOS Software Update is in progress by monitoring the softwareupdated and com.apple.MobileSoftwareUpdate.UpdateBrainService. The scheduled rotation will be retried during the next EasyLAPS execution, provided these processes are no longer running. Although not recommended, this execution probe can be disabled by setting the EXECUTION_PROBES > MACOS_SOFTWARE_UPDATE key to "false".

190	Sleep State detected.	An execution probe has detected that the Mac is sleeping by parsing the output of the pmset -g log command. The scheduled rotation will be retried during the next EasyLAPS execution, provided the sleep state is no longer detected. Although not recommended, this execution probe can be disabled by setting the EXECUTION_PROBES > SLEEP_STATE key to "false".
191	Running MacOnboardingMate Workflow detected.	An execution probe has detected that a MacOnboardingMate workflow is in progress by monitoring the com.agnosys.mom LaunchDaemon. The scheduled rotation will be retried during the next EasyLAPS execution, provided the MacOnboardingMate workflow is completed.
193	Postponed MacOnboardingMate Workflow detected.	An execution probe has detected that a MacOnboardingMate workflow is pending by monitoring the com.agnosys.mom_supervisor LaunchDaemon. The scheduled rotation will be retried during the next EasyLAPS execution, provided the MacOnboardingMate workflow is completed.
195	Postponed MacOnboardingMate Action detected.	An execution probe has detected that a MacOnboardingMate action is pending. The scheduled rotation will be retried during the next EasyLAPS execution, provided the MacOnboardingMate action is completed.
197	Running Jamf Pro Policy detected.	An execution probe has detected that a Jamf Pro policy is in progress by monitoring the Jamf Binary activity. The scheduled rotation will be retried during the next EasyLAPS execution, provided the Jamf policy execution is completed. Although not recommended, this execution probe can be disabled by setting the EXECUTION_PROBES > JAMF_PRO_POLICY_RUNNING key to "false".

Error code matrix

This matrix does not exempt from reading this Integration Guide and is designed to be an help before contacting EasyLAPS support.

For each key indicated in this matrix, please refer to the EasyLAPS Dictionary for the expected value.

Error	Message	Troubleshooting
1	An issue occurred.	Contact EasyLAPS support with a log generated in debugverbose mode.
11	The license policy is unknown.	Contact EasyLAPS support to obtain the license code.
12	The license policy is missing.	Contact EasyLAPS support to obtain the license code.
13	The license has expired.	Contact EasyLAPS support to renew the license code.
17	The integrity of the EasyLAPS configuration cannot be verified.	Root cause : the integrity of the PLIST file "/Library/Managed Preferences/com.agnosys.config.EasyLAPS.plist" could not be verified. If the problem persists after several attempts at rotation, contact EasyLAPS support with a log generated in debugverbose mode.
19	No MDM Solution defined.	Assign the MDMSOLUTION key the name of a supported management solution.
21	MDM Solution [*mdm*] not supported.	Assign the MDMSOLUTION key the name of a supported management solution.
23	EasyLAPS is configured for [*mdm_a*] whereas MacOnboardingMate has enrolled the device in [*mdm_b*].	Assign the MDMSOLUTION key the name of the management solution in which MacOnboardingMate has enrolled the device. In the context of an MDM switching to another supported solution, please contact EasyLAPS support to define an action plan.
25	No API URL defined.	Assign the APIURL key the URL of the management solution to manage API calls.
27	No API Authentication defined.	Assign the APIAUTHENTICATIONSTRING key the string to be used to authenticate API calls.
29	No management account defined.	Assign the MGTACCOUNT key the management account name whom password will be rotated.
31	Management account determined password contains an unsupported character.	Assign the MGTACCOUNTPASSWORDDETERMINED key a string that does not include the backslash character.
33	Directory Service is unavailable.	1. If the problem persists after several attempts at rotation, restart the device. 2. Set the MGTACCOUNTREMEDIATE key to "true" to attempt to remediate Open Directory error -14487 eDSServiceUnavailable at the next rotation attempt. 3. Contact EasyLAPS support with a log generated in debugverbose mode. 4. Once checked the remediation cannot fix the issue, execute a policy that deletes the management account and forces a rotation.
35	Management account creation failed.	1. Assign the MGTACCOUNTUID key a number greater than 501 that is confirmed as not already being used for another account. Assign the MGTACCOUNTSHELL key the string "/bin/zsh". Assign the MGTACCOUNTHOME key a full path than can be used for a local home directory (e.g. /Users/mgtaccount, /private/var/mgtaccount). 2. Try creating the account manually using the expected password to reproduce the problem outside of EasyLAPS. If the problem is reproducible, investigate a macOS case. 3. Contact EasyLAPS support with a log generated in debugverbose mode.

37	Validation of public key used to encrypt password stored in MDM failed.	Applicable to Logic #1 only. Execute the "easylaps_rsa_keygen_passwd" script to display the encoded RSA Public Key used to encrypt the password stored in the management solution and ensure that the displayed encoded RSA Public Key is correctly assigned to the MDMPASSWORDENCRYPTIONKEY key.
39	Account statuses management was aborted because the decryption of exclusions failed.	Execute the "easylaps_rsa_engine" script with the value stored in the ADMINACCOUNTS key after the prefix "enabled-" to ensure that the exclusions are correctly defined.
49	Undefined Open Directory error.	1. If the problem persists after several attempts at rotation, restart the device. 2. Contact EasyLAPS support with a log generated in debugverbose mode.
51	Management account is currently logged in.	1. Logout the management account. 2. If the logout is not possible or wishable, force the rotation executing EasyLAPS with the "--force" option.
53	Management account is disabled.	1. Set the MGTACCOUNTUNLOCK key to "true" to attempt to remediate Open Directory error -14167 eDSAuthAccountDisabled (first method tried when enabled) at the next rotation attempt. 2. Set the MGTACCOUNTENABLE key to "true" to attempt to remediate Open Directory error -14167 eDSAuthAccountDisabled (second method tried when enabled) at the next rotation attempt. 3. Set the MGTACCOUNTREMEDIATE key to "true" to attempt to remediate Open Directory error -14167 eDSAuthAccountDisabled (third method tried when enabled) at the next rotation attempt. 4. Contact EasyLAPS support with a log generated in debugverbose mode. 5. Once checked the remediation cannot fix the issue, execute a policy that deletes the management account and forces a rotation.
55	Management account creation failed because initial password defined not compliant with local account password policy.	1. Assign the MGTACCOUNTPASSWORD key the current password of the management account which must be compliant with the local account password policy. 2. Temporarily disable the local account password policy until the account is created and the first rotation to a complex password is successful.
57	Current password for management account could not be defined.	Root cause : the current password of the management account is not the initial password, nor the password stored in the management solution, nor the password stored in the EasyLAPS Keychain, nor the determined password. 1. Consider that the password may have been reset on the device outside of EasyLAPS ; ask people who may have performed this action. 2. If possible, reset the password to the initial password or type the probable password in the field used by EasyLAPS in the device inventory (clear text). 3. Contact EasyLAPS support with a log generated in debugverbose mode. 4. Once checked the password is unknown, execute a policy that deletes the management account and forces a rotation.
59	New password defined not compliant with local account password policy.	Assign the following keys the values required to comply with the local account password policy : - Password : PASSWORDLENGTH key, SYMBOLSNUMBERMAX and SYMBOLSNUMBERMIN keys - Passphrase : PASSPHRASELENGTH key, SYMBOLSNUMBERMAX and SYMBOLSNUMBERMIN keys, PASSPHRASECAPSMODE key, PASSPHRASEDIGITSNUMBERMAX and PASSPHRASEDIGITSNUMBERMIN keys.
61	Password validation in local directory failed. Safe mode enabled.	Root cause : the current password of the management account was changed to the new password in the local directory but this last cannot be verified right after the change. - Logic #1 : the new password is escrowed as ever in the EasyLAPS Keychain and another rotation will be attempted at the next EasyLAPS execution. - Logic #2 : the new password is escrowed temporarily in the EasyLAPS Keychain and another rotation will be attempted at the next EasyLAPS execution. In the waiting, the password stored in the management solution does not match the current password.

63	Attempting to change password failed.	Root cause : the current password of the management account was not changed to the new password in the local directory with a returned error. 1. Set the MGTACCOUNTREMEDIATE key to "true" to attempt to remediate Open Directory error -14915 eParameterError at the next rotation attempt. 2. Contact EasyLAPS support with a log generated in debugverbose mode. 3. Once checked the remediation cannot fix the issue, execute a policy that deletes the management account and forces a rotation.
67	Password read from MDM does not match password written in MDM and password reversion has succeeded.	Applicable to Logic #1 only. The value that was written in the management solution is read and the collected value does not match the expected value ; the password is reversed to the previous one and another rotation will be attempted at the next EasyLAPS execution. In the waiting, the password stored in the management solution possibly does not match the new password.
68	Password read from MDM does not match password written in MDM and password reversion has failed. Safe mode enabled.	Applicable to Logic #1 only. The value that was written in the management solution is read and the collected value does not match the expected value ; as the local account password policy prevents the password to be reversed, Safe mode is enabled ; the new password is escrowed as ever in the EasyLAPS Keychain and another rotation will be attempted at the next EasyLAPS execution. In the waiting, the password stored in the management solution does not match the new password.
69	Password read from MDM is neither the current password nor the new password. Safe mode enabled.	Applicable to Logic #2 only. The value that was written in the management solution is read and the collected value is neither the current password nor the new password. Safe mode is enabled. The new password is escrowed temporarily in the EasyLAPS Keychain and another rotation will be attempted at the next EasyLAPS execution. In the waiting, the password stored in the management solution possibly does not match the new password.
70	Password read from MDM still does not match password written in MDM after [*x*] seconds. Safe mode maintained.	The value that was written in the management solution is read and the collected value is still the current password after the waiting period. The issue may be due to replication lag between MDM cluster instances. The Safe Mode, enabled due to suspected lag, is maintained. The new password is escrowed temporarily in the EasyLAPS Keychain and another rotation will be attempted at the next EasyLAPS execution. In the waiting, the password stored in the management solution does not match the new password.
73	Rotation deferral : active. Initial password : yes. [...] Writing the rotation deferral message in MDM failed.	1. Check that the device is enrolled in the management solution. 2. Assign the APIURL key the URL of the management solution to manage API calls. 3. Check the credentials used to authenticate API calls with the management solution. 4. Assign the APIAUTHENTICATIONSTRING key the string containing the confirmed credentials. 5. Check that the "easylaps_rsa_key.pri" file installed on the device by the EasyLAPS-Content package in /Library/Application Support/EasyLAPS/Content is the file present in the "easylaps_secrets" subfolder of the EasyLAPS-Toolkit.
101	Device ID not detected during a password rotation.	1. Check that the device is enrolled in the management solution. 2. Assign the APIURL key the URL of the management solution to manage API calls. 3. Check the credentials used to authenticate API calls with the management solution. 4. Assign the APIAUTHENTICATIONSTRING key the string containing the confirmed credentials. 5. Check that the "easylaps_rsa_key.pri" file installed on the device by the EasyLAPS-Content package in /Library/Application Support/EasyLAPS/Content is the file present in the "easylaps_secrets" subfolder of the EasyLAPS-Toolkit.
102	Azure Active Directory Device ID not detected during a password rotation.	This error is likely transient. If the problem persists after several attempts at rotation, contact EasyLAPS support with a log generated in debugverbose mode.
103	Device ID not detected during a password collect.	1. Check that the device is enrolled in the management solution. 2. Assign the APIURL key the URL of the management solution to manage API calls. 3. Check the credentials used to authenticate API calls with the management solution. 4. Assign the APIAUTHENTICATIONSTRING key the string containing the confirmed credentials. 5. Check that the "easylaps_rsa_key.pri" file installed on the device by the EasyLAPS-Content package in /Library/Application Support/EasyLAPS/Content is the file present in the "easylaps_secrets" subfolder of the EasyLAPS-Toolkit.

104	Azure Active Directory Device ID not detected during a password collect.	This error is likely transient. If the problem persists after several attempts at collection, contact EasyLAPS support with a log generated in debugverbose mode.
108	External connectivity through the proxy has not been verified.	1. Check the parameters of the PROXY_CONFIGURATION Dictionary. 2. Validate that the URL defined by the URL_PROBE key is accessible behind the Proxy. 3. In the debugging log, isolate the line that makes a curl using the --proxy option. 4. Try to reproduce the curl manually, in consultation with the Proxy team. 5. Contact EasyLAPS support with a successful command in your environment.
109	External connectivity through the Kerberized proxy has not been verified.	1. Check the parameters of the PROXY_CONFIGURATION Dictionary. 2. Validate that the URL defined by the URL_PROBE key is accessible behind the Proxy. 3. In the debugging log, isolate the line that makes a curl using the --proxy-negotiate --proxy options 4. Try to reproduce the curl manually, in consultation with the Proxy team. 5. Contact EasyLAPS support with a successful command in your environment.
113	Extension Attribute ID undefined.	1. Check that the Privileges assigned to the Jamf Pro API client (OAuth authentication) or service account (Basic authentication) allow the creation of the "EasyLAPS" Computer Extension Attribute. 2. Create the "EasyLAPS" Computer Extension Attribute" manually.
115	Custom Attribute creation failed.	1. Check that the Permissions assigned to the SimpleMDM API Key allow writing Custom Attributes. 2. Create the "EasyLAPS" Custom Attribute manually.
151	Jamf Pro hosted in Jamf Cloud is not available.	Check the connectivity with Jamf Pro using the Health Check Page. Refer to https://learn.jamf.com/bundle/jamf-pro-documentation-current/page/Jamf_Pro_Health_Check_Page.html for details. The expected status is "[ ]".
153	Jamf Pro is not available.	Check the connectivity with Jamf Pro from the device.
155	Timeout while getting bearer token.	Check the connectivity with Jamf Pro from the device.
157	Error while getting bearer token. Returned status code : [*http_code*].	Check the credentials used to get a Bearer Token with Jamf Pro and VMware Workspace ONE.
158	Error while getting device details. Returned status code : [*http_code*].	This error is likely transient. If the problem persists after several attempts at rotation, contact EasyLAPS support with a log generated in debugverbose mode.
159	Jamf Pro Version not detected.	Contact EasyLAPS support with a log generated in debugverbose mode.
161	An error occurred while validating remote service client credentials or user not found.	1. Check the credentials used to authenticate API calls with VMware Workspace ONE. 2. Assign the APIAUTHENTICATIONSTRING key the string containing confirmed credentials.
162	An error occurred while retrieving the password from the MDM. Returned status code : [*http_code*].	This error is likely transient. If the problem persists after several attempts at rotation, contact EasyLAPS support with a log generated in debugverbose mode.
163	Maximum API calls per day reached.	Adjust the maximum number of API calls allowed per day on your VMware Workspace ONE instance.
165	API account password is expired or password should be changed.	1. Check the credentials used to authenticate API calls with VMware Workspace ONE 2. Assign the APIAUTHENTICATIONSTRING key the string containing confirmed credentials.
167	VMware Workspace ONE is not available.	Check the maintenance status of your instance.
186	Date Incoherence detected.	The device's date has been set to a time earlier than the last EasyLAPS execution. Ensure the date is not set to a significantly outdated time, such as 1/1/1970 (the Unix epoch start), or another year far in the past.

201	This tool requires macOS Tahoe (macOS 26), macOS Sequoia (macOS 15), macOS Sonoma (macOS 14), macOS Ventura (macOS 13), macOS Monterey (macOS 12), macOS Big Sur (macOS 11), macOS Catalina (macOS 10.15), macOS Mojave (macOS 10.14) or macOS High Sierra (macOS 10.13).	Update macOS to macOS 10.13.4 and later.
203	This tool requires macOS High Sierra 10.13.4 and later.	Update macOS to macOS 10.13.4 and later.
221	Password collect for any device not allowed.	Assign the ALLOWCOLLECTFORANYDEVICE key the value "true".
222	No value for criterion Serial Number passed to EasyLAPS.	When using the command easylaps.sh --collect, the option --serialnumber must be followed by the Serial Number of a device.
223	No value for criterion UUID passed to EasyLAPS.	When using the command easylaps.sh --collect, the option --uuid must be followed by the UUID of a device.
224	Password collect for any device not supported with [*mdm*].	Contact EasyLAPS support to express your interest in having this capability supported by your management solution.
225	Password collect for any device by UUID not supported with [*mdm*].	When using the command easylaps.sh --collect, the option --uuid is not supported by your management solution. Use the option --serialnumber followed by the Serial Number of a device.

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

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

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

VMware Workspace ONE - Distribute an updated Custom configuration profile

This section only applies if :
- the management solution is VMware Workspace ONE
- the current Custom configuration profile was uploaded as a pre-built Custom configuration profile (.mobileconfig file) according to the legacy provisioning.

The updated Custom configuration profile must be provisioned using the new method detailed in the section titled "Custom Configuration Profile" in the chapter titled "Provisioning VMware Workspace ONE".

The known issue is that you may not be able to delete the existing Custom configuration profile until the last device managed by the MDM has it installed. To circumvent this, EasyLAPS includes a mechanism that allows reading an updated Custom configuration profile while ignoring the existing one that is still installed.

To achieve this result, follow these instructions.

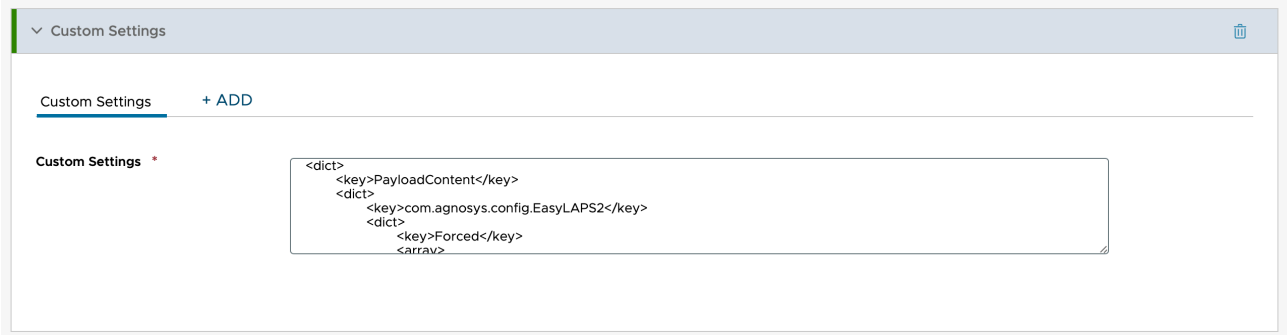
1/ Distribute EasyLAPS version 2.08 and later to Macs installed with EasyLAPS. This version is the first to include the aforementioned mechanism. This new version will continue to use the existing custom configuration profile until it is updated.

2/ Update your current EasyLAPS Toolkit following the instructions in the section titled "EasyLAPS Toolkit" in the chapter titled "Updating EasyLAPS". The Custom configuration profile for VMware Workspace ONE still uses the ".mobileconfig" extension, which is expected at this stage.

3/ Update the EasyLAPS configuration file as needed, such as with a new license code.

4/ Proceed to the conversion of the EasyLAPS configuration file to a Custom configuration profile by executing the "configs_profiles_generator" script (select the script > right-click > Open). Note that the Custom configuration profile for VMware Workspace ONE now uses the ".plist" extension.

5/ Provision VMware Workspace ONE with the updated Custom configuration profile following the instructions in the section titled "Custom Configuration Profile" in the chapter titled "Provisioning VMware Workspace ONE", **noting this critical difference**.



After pasting the whole content in the XML field, rename the key originally named "com.agnosys.config.EasyLAPS" to "com.agnosys.config.EasyLAPS2" (or any number greater than 0).

Once the updated Custom configuration profile is distributed, EasyLAPS will discover in the "/Library/Managed Preferences" folder two files named "com.agnosys.config.EasyLAPS.plist" and "com.agnosys.config.EasyLAPS2.plist". It will use the file with the highest version number, ignoring any others.

If you need clarification about this process, do not hesitate to open an EasyLAPS support ticket.

Collect the password for developments

Both EasyLAPS Logic #1 and EasyLAPS Logic #2 makes the current management account's password available for the organization's developments.

All commands in this section must be inserted into a script executed by root.

• **EasyLAPS Logic #1**

The management account's password is stored in encrypted form in the EasyLAPS Keychain.

To get the password in clear text with EasyLAPS :

```
sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh" --collect
```

The collected password is stored in a file located at
/Library/Application Support/EasyLAPS/easylaps_passwd_collected

The file hidden in the Finder is owned by root, associated to the wheel group, with read and write permissions for root only.

Important notice

The script which triggers the password collect must check the existence and the content of the file after the command is executed to determine if the password was correctly collected. Once the password is read, the script is expected to delete the file immediately. Note that the file is automatically deleted each time EasyLAPS is executed.

To get the password in clear text directly from the EasyLAPS Keychain :

```
security unlock-keychain -p "$(cat "/Library/Application Support/
EasyLAPS/easylaps.keychain.passwd")" "/Library/Application Support/
EasyLAPS/easylaps.keychain"

security find-generic-password -w -a "management_account" -s EasyLAPS "/
Library/Application Support/EasyLAPS/easylaps.keychain" | base64 -D
```

Please note that the string "management_account" must be kept as is.

• **EasyLAPS Logic #2**

The management account's password is stored in clear text in the MDM.

To get the password in clear text with EasyLAPS :

```
sh "/Library/Application Support/EasyLAPS/Core/easylaps.sh" --collect
```

The collected password is stored in a file located at /Library/Application Support/EasyLAPS/easylaps_passwd_collected

With Jamf Pro, the command can be augmented with the option "`--serialnumber <serial_number>`" or "`--uuid <hardware uuid>`" to collect the management account's password for any device other than the local device. Note that the ALLOWCOLLECTFORANYDEVICE key must be set to "true" to allow this capability.

The collected password is stored in a file located at /Library/Application Support/EasyLAPS/easylaps_passwd_collected

The file hidden in the Finder is owned by root, associated to the wheel group, with read and write permissions for root only.

Important notice

The script which triggers the password collect must check the existence and the content of the file after the command is executed to determine if the password was correctly collected. Once the password is read, the script is expected to delete the file immediately. Note that the file is automatically deleted each time EasyLAPS is executed.

When the LOCALPASSWORDESCROW key is set to "true", the management account's password is always escrowed in encrypted form in the EasyLAPS Keychain. In addition to read the password from MDM as indicated above, the password can also be read directly from the EasyLAPS Keychain.

To get the password in clear text :

```
security unlock-keychain -p "$(cat "/Library/Application Support/
EasyLAPS/easylaps.keychain.passwd")" "/Library/Application Support/
EasyLAPS/easylaps.keychain"

security find-generic-password -w -a "management_account" -s EasyLAPS "/
Library/Application Support/EasyLAPS/easylaps.keychain" | base64 -D
```

Please note that the string "management_account" must be kept as is.

Support

Paid support included in EasyLAPS offers

Send your support request to easylaps.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/C02ATFA85B7

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.

EasyLAPS 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.