EasyLAPS Dictionary

Version 1.47 — Updated on March 9, 2023

EasyLAPS is executed at installation and then automatically every hour.
However the password rotation is executed specifically according to the PASSWORDEXPIRATION value.
Each time EasyLAPS is executed, the management account is created if it is detected as missing or updated for some of its properties mentionned in this table.
The referenced picture (.png) must be embedded in the EasyLAPS-Content package.

Key	Type	Example
LICENSE	String	EasyLAPS license key
The EasyLAPS license key.		
DEBUGMODE	String	disabled
Set to "debug" or "debugverbose" (exactly) to enable EasyLAPS logging in /private/var/log/ as soon as the key is read and to create the debug flag accordingly. The files titled EasyLAPS-easylaps_*date* .log and EasyLAPS-easylaps_starter_*date* .log contain sensitive informations for troubleshooting purpose only and can be read by admin users only. The setting is ignored if the logging has been already enabled by the manual creation of a debug flag.		
TRACEMODE	String	disabled
Set to "enabled" (exactly) to enable EasyLAPS logging in /private/var/log/ as soon as the key is read. The file titled EasyLAPS-easylaps_trace.log does not contain sensitive informations, can be used to keep track of rotation history and can be read by any standard or admin user.		
MDMSOLUTION	String	Jamf Pro
The management solution for that location : "Jamf Pro", "Jamf School", "JumpCloud", "Meraki Systems Manager", "Microsoft Intune", "Mosyle Business", "Mosyle Manager", "SimpleMDM", "VMware Workspace ONE" (exact name from this list required). This string is visible in the name of the EasyLAPS Configuration profile (com.agnosys.config.MDMSOLUTION.MDMLOCATION.EasyLAPS.mobileconfig).		
MDMLOCATION	String	Paris
An arbitrary name associated to the EasyLAPS configuration. This string is visible in the name of the EasyLAPS Configuration profile (com.agnosys.config.MDMSOLUTION.MDMLOCATION.EasyLAPS.mobileconfig).		
APIURL	String	https://hostname.jamfcloud.com
The URL of the management solution to manage API calls. Jamf Pro : https://hostname.jamfcloud.com Jamf School : https://hostname.jamfcloud.com/api JumpCloud : https://console.jumpcloud.com/api Meraki Systems Manager : https://api.meraki.com/api/v1 Microsoft Intune : https://graph.microsoft.com/Beta (API 1.0 is not supported) Mosyle Business : https://businessapi.mosyle.com/v1 Mosyle Manager : https://managerapi.mosyle.com/v2 SimpleMDM : https://a.simplemdm.com/api/v1 VMware Workspace ONE : Groups & Settings > All Settings > System > Advanced > API > Rest API — General > REST API URL : https://asX.awmdm.com/api		
APIAUTHENTICATIONSTRING	String	RSA-encrypted_authentication_string

The string to be used to authenticate API calls. Jamf Pro : apisvcaccount:apisvcaccountpassword Jamf School : Network ID:API Key (School > Devices > Enroll Device(s) > On-device enrollment > Network ID / School > Settings > API > Add API Key > Name + Key > Apply) JumpCloud : API Key (Account > API Settings) Meraki Systems Manager : Organization > Configure > Settings > Dashboard API access > Enable access to the Cisco Meraki Dashboard API + Account > My Profile > API access > Generate new API key Microsoft Intune : concatenation of those 3 values separated with commas : tenant_domain,application_(client)_id,client_secret_value Mosyle Business : concatenation of those 3 values separated with commas : apisvcaccountemail,apisvcaccountpassword,accesstoken - API Service Account : Organization > Administrators > Add Administrator > Name / User ID / Email / Send welcome e-mail : unchecked / Password / Account type : Administrator > Save - Access Token : Organization > Integrations > Mosyle API Integration > Add new token > Profile name / Access Method : Public / Allowed Endpoint : Devices > Save > Access Token Mosyle Manager : Access Token (My School > Integrations > API Integration > Access Token) SimpleMDM : API Key (Account > API > Add API Key > name > Save > Secret Access Key > reveal) VMware Workspace ONE : concatenation of those 3 values separated with commas : username,password,API Key - Accounts > Administrators > List View > Username — Roles > Organization Group : Console Administrator / Custom Role — API > Authentication : User Credentials - Groups & Settings > All Settings > System > Advanced > API > Rest API — General > Enable API Access : Enabled / Service : AirWatchAPI | Account Type : Admin | API Key — Authentication > Basic : Enabled RSA encryption : use the script "easylaps_rsa_engine" to generate the full value including the "RSA-" prefix.		
JSON_PARSER	String	plutil
To enable JSON parsing with plutil, set the key to "plutil" (preferred method). To enable JSON parsing with JavaScript, set the key to "javascript". To enable JSON parsing with jq, set the key to "jq". When JQ cannot be installed correctly, alongside Rosetta on Apple silicon Mac, plutil is used as the fallback of jq. When macOS 11 and earlier is detected, JavaScript is used as the fallback of plutil.		
JQ_URL	String	https://github.com/stedolan/jq/releases/download/jq-1.6/jq-osx-amd64
Since EasyLAPS 1.46, JSON parsing with JQ is deprecated but is still supported. When jq is enabled, set the key to this download URL : https://github.com/stedolan/jq/releases/download/jq-1.6/jq-osx-amd64		
BLOCKEDLIST	String	/+O0Il
Set of characters disallowed to be used in the generated new password.		
SYMBOLSLIST	String	!@#$%
Set of symbols allowed to be used in the new generated password. The symbol Backslash \ is always excluded.		
SYMBOLSNUMBERMAX	Number	1
Maximum number of symbols that must be included in the new generated password replacing letters and digits. The symbols are both chosen at random in the symbols list and positioned at random in the new generated password.		
SYMBOLSNUMBERMIN	Number	1
Minimum number of symbols that must be included in the new generated password replacing letters and digits.		
MGTACCOUNT	String	ladmin
The local administrator account name whom password will be rotated. The management account name when it is created by EasyLAPS.		
MGTACCOUNTFULLNAME	String	Local Administrator
The management account full name when it is created by EasyLAPS. EasyLAPS updates the current management account full name with this value if it is detected as different.		
MGTACCOUNTUID	Number	600
The management account UID when it is created by EasyLAPS.		
MGTACCOUNTSHELL	String	/bin/zsh
The management account Shell when it is created by EasyLAPS. EasyLAPS updates the current management account Shell with this value if it is detected as different.		
MGTACCOUNTHOME	String	/Users/ladmin
The management account home folder when it is created by EasyLAPS.		

MGTACCOUNTPASSWORD	String	RSA-encrypted_mgt_account_password
The current password of the local administrator account used for the first rotation. RSA encryption : use the script "easylaps_rsa_engine" to generate the full value including the "RSA-" prefix.		
MGTACCOUNTPASSWORDDETERMINED	String	RSA-encrypted_mgt_account_determined_password
The determined password to be used instead of a randomized password. This key does not exist intentionally in the EasyLAPS configuration file template and must be added manually. The symbol Backslash \ is not supported. RSA encryption : use the script "easylaps_rsa_engine" to generate the full value including the "RSA-" prefix.		
MGTACCOUNTPICTURE	String	mgtaccount_picture.png
EasyLAPS updates the management account picture (.png file expected) with this picture if no custom picture has been already set.		
MGTACCOUNTHIDDEN	Boolean	false
Set to "true" to make the management account hidden and set to "false" to make it visible. When the management account is made hidden, the shared folder configurations including its name or its full name are automatically deleted.		
MGTACCOUNTENABLE	Boolean	true
Set to "true" to attempt to remediate Open Directory error -14167 eDSAuthAccountDisabled (first try) by the edition of two attributes : - accountPolicyData : reset the values failedLoginCount and failedLoginTimestamp to "0" - AuthenticationAuthority : remove the value ;DisabledUser;		
MGTACCOUNTREMEDIATE	Boolean	true
Set to "true" to attempt to remediate Open Directory errors -14167 eDSAuthAccountDisabled (second try), -14487 eDSServiceUnavailable and -14915 eParameterError. The remediation is performed by removing the management account from FileVault using the command fdesetup remove -user		
PASSWORDEXPIRATION	Integer	30
The number of days after which a rotation process is triggered until it is successful. Use "0" to force a rotation each time EasyLAPS is executed.		
PASSWORDLENGTH	Integer	12
Length of the generated new password.		
MDMPASSWORDENCRYPTIONKEY	String	public_key
The public key used to encrypt the generated new password when the EasyLAPS logic plans that it must be stored encrypted in the MDM. The existence of this key defines the activated EasyLAPS logic. Key configured > Logic #1 : the password is stored encrypted in MDM and is always stored in the System Keychain : the next rotation will use the locally stored password. Key deleted > Logic #2 : the password is stored in clear text in MDM and is not stored in the System Keychain (*) : the next rotation will use the remotely stored password. Use the script "easylaps_rsa_keygen_passwd" to generate the private / public key pair required by Logic #1 (the private key must be kept in restricted access). (*) Logic #2 plans that the password can be stored temporarily in the System Keychain if a failure makes it necessary (please refer to the Integration Guide for more information).		
MDMPASSWORDPREFIX	String	enabled
Set to "enabled" (exactly) to add the prefix "easylaps" before the password stored in MDM. The prefix will be added or removed at the next rotation. This key is ignored and the prefix is always added in the following contexts : - the management solution "Mosyle Business" or "Mosyle Manager" is used - the management solution "VMware Workspace ONE" is used with Logic #1 activated.		
MDMPASSWORDDATE	String	enabled
Set to "enabled" (exactly) to add the last rotation date after the password stored in MDM. The date will be added or removed at the next rotation.		
ADMINACCOUNTS	String	enabled-tom,jerry

Set to "enabled" (exactly) to enable the accounts status management capacity. EasyLAPS promotes to admin status the accounts added after the string "enabled-" and separated with commas. EasyLAPS demotes to standard status the accounts that are not listed. The management account does not need to be added to the list as it is included by default.		
SLACK_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the Slack integration defined by the SLACK_CONFIGURATION Dictionary.		
SLACK_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary
INCOMING_WEBHOOK_URL : RSA-encrypted_incoming_webhook_URL (refer to https://api.slack.com/messaging/webhooks) In the following examples, ":warning:" is an emoji (refer to https://www.webfx.com/tools/emoji-cheat-sheet/) and ":ModelName:" is an available variable for the specified message. STATUS_MESSAGE_ERROR : message sent when the status message is an error message :warning: :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: STATUS_MESSAGE_INFO : message sent when the status message is an informative message :information_source: :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: STATUS_MESSAGE_SUCCESS : message sent when the management account password was rotated successfully :white_check_mark: :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: RSA encryption : use the script "easylaps_rsa_engine" to generate the full value including the "RSA-" prefix.		
TEAMS_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the Teams integration defined by the TEAMS_CONFIGURATION Dictionary.		
TEAMS_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary
INCOMING_WEBHOOK_URL : RSA-encrypted_incoming_webhook_URL (refer to https://docs.microsoft.com/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook) In the following examples, "⚠" is an emoji (refer to https://unicode.org/emoji/charts/full-emoji-list.html) followed by a wide space and ":ModelName:" is an available variable for the specified message. STATUS_MESSAGE_ERROR : message sent when the status message is an error message ⚠ :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: STATUS_MESSAGE_INFO : message sent when the status message is an informative message ℹ :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: STATUS_MESSAGE_SUCCESS : message sent when the management account password was rotated successfully ✅ :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: RSA encryption : use the script "easylaps_rsa_engine" to generate the full value including the "RSA-" prefix.		
EXECUTION_PROBES	Dictionary	EXECUTION_PROBES — Dictionary -- MAC_APP_STORE_SOFTWARE_INSTALLATION — Boolean — true -- MACOS_SOFTWARE_INSTALLATION — Boolean — true -- MACOS_SOFTWARE_UPDATE — Boolean — false
MAC_APP_STORE_SOFTWARE_INSTALLATION : Set to "true" to prevent the rotation if a running Mac App Store software installation is detected based on installd or appinstalld consuming CPU. MACOS_SOFTWARE_INSTALLATION : Set to "true" to prevent the rotation if a running macOS software installation is detected based on system_installd consuming CPU, or osinstallersetupd started. MACOS_SOFTWARE_UPDATE : Set to "true" to prevent the rotation if a running macOS software update is detected based on softwareupdated or com.apple.MobileSoftwareUpdate.UpdateBrainService consuming CPU. When the key does not exist in the configuration file, the corresponding execution probe is enabled.		