mCS is executed during installation and then, by default, automatically every day when the computer is awake.

Key	Type	Example
LICENSE	String	mCS license key
The mCS license key.		
DEBUGMODE	String	disabled
This setting offers to enable mCS logging for troubleshooting purposes. Set to "debug" or "debugverbose" (exactly) to enable the corresponding level of logging. Log files are created in /private/var/log/ and titled mCS-mcs_*date*.log and mCS-mcs_starter_*date*.log. They contain sensitive informations, must not be left unattended and can be read by admin users only. The corresponding debug flag is automatically created in /Library/Application Support/mCS. The setting is ignored if the logging has been already enabled by the manual creation of a debug flag.		
TRACEMODE	String	disabled
This setting offers to enable mCS logging for informative purposes. Set to "enabled-lf" or "enabled" (exactly) to log in the log file /private/var/log/mCS-mcs_trace.log. Set to "enabled-ul" to log in the Unified Logging under the process "logger" (refer to the Integration Guide for the display of the log). Set to "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 execution history and can be read by any standard or admin user.		
EXECUTION_INTERVAL	Integer	3600
This key offers to slow down mCS iterations. mCS is still executed by launchd every hour when the computer is awake, but exits at an early stage when the current time is before than the last execution time plus the specified execution interval. The value in seconds can be set between 3600 (1 hour) and 2592000 (30 days).		
MDMSOLUTION	String	Jamf Pro
The management solution for that location : "FileWave", "Jamf Pro", "Jamf School", "JumpCloud", "Meraki Systems Manager", "Microsoft Intune", "Miradore", "Mosyle Business", "Mosyle Manager", "SimpleMDM", "VMware Workspace ONE" (exact name from this list required). This string is visible in the name of the mCS Configuration profile (com.agnosys.config.MDMSOLUTION.MDMLOCATION.mCS.mobileconfig).		
MDMLOCATION	String	Paris
An arbitrary name associated to the mCS configuration. Meraki Systems Manager : the name of the location must be the exact name of a Network defined inside the Organization for the API calls to be functional. This string is visible in the name of the mCS Configuration profile (com.agnosys.config.MDMSOLUTION.MDMLOCATION.mCS.mobileconfig).		
APIURL	String	https://hostname.jamfcloud.com
The URL to make API calls with the management solution. FileWave : https://hostname.filewave.net (API v1 and v2 usage) Jamf Pro : https://hostname.jamfcloud.com (usage of the Jamf Pro API instead of the Classic API with Jamf Pro 10.50 and later) Microsoft Intune : https://graph.microsoft.com/Beta (API 1.0 is not supported) 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. FileWave : FileWave Admin > Assistants > Manage Administrators > + Local Account > User details : Login Name - Set password / Application tokens : Token (base64) Jamf Pro (API Roles and Clients) : concatenation of those 2 values separated with a colon : Client ID:Client Secret (refer to the Integration Guide for the details) Jamf Pro (User account / deprecated) : concatenation of those 2 values separated with a colon : apisvcaccount:apisvcaccountpassword Microsoft Intune : concatenation of those 3 values separated with commas : tenant_domain,application_(client)_id,client_secret_value VMware Workspace ONE (OAuth2 authentication) : concatenation of those 3 values separated with commas : Token URL,Client ID,Client Secret - Token URL : refer to https://docs.omnissa.com/bundle/WorkspaceONE-UEM-Console-BasicsVSaaS/page/UsingUEMFunctionalityWithRESTAPI.html - Groups & Settings > Configurations > OAuth Client Management > Name, Description, Organization Group, Role : Console Administrator / Custom Role, Status : Enabled > Client ID, Client Secret VMware Workspace ONE (Basic authentication / deprecated) : 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 "mcs_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, plutil is used as the fallback. When macOS 11 and earlier is detected, JavaScript is used as the fallback of plutil. When Jamf Pro API is enabled, API calls are forcibly made using plutil (macOS 12 and later), JavaScript (macOS 10.15 and macOS 11) and jpt (https://github.com/brunerd/jpt).		
JQ_URL	String	https://github.com/jqlang/jq/releases/download/jq-1.7.1/jq-macos-arm64
JSON parsing with JQ is deprecated but is still supported. When jq is enabled, set the key to this download URL : https://github.com/jqlang/jq/releases/download/jq-1.7.1/jq-macos-arm64 The URL for the arm64 or the x86_64 architecture is automatically derived from any given URL.		
GUI_MODE	String	interactive
Set the visibility level of the graphical user interface : - none : no interface is displayed - informative : only notifications are displayed - interactive : the complete interface is displayed.		
UIHELPER_NOTIFICATION_TITLE	String	macOS Compliance Spotter
The title to be displayed in a notification.		
UIHELPER_NOTIFICATION_ICON	String	mcs-icon.png
The icon to be displayed in a notification (.png file expected).		
UIHELPER_PICTURE_WELCOME	String	mcs-icon.png
The picture to be displayed in the welcome pane (.png file expected).		
UIHELPER_MAIN_TITLE_WELCOME	String	Discover macOS Compliance Spotter
The title to be displayed in the welcome pane.		
UIHELPER_MAIN_TEXT_WELCOME	String	This tool remediates detected compliance issues to align the system with security standards, then conducts a compliance scan to ensure all measures are met.
The text to be displayed in the welcome pane. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).		
UIHELPER_PICTURE_HELP **QR code - except mailto URI scheme**	Dictionary	TYPE — String — qrcode QRCODE_DATA — String — http://www.compliancespotter.com QRCODE_COLOR — String — rgb(159,73,190)
• TYPE : set to "qrcode" • QRCODE_DATA : the string to encode within the QR code, such as a URL beginning with "http(s)://" (see below for an email address using "mailto:") • QRCODE_COLOR : the QR code's color in RGB format, for example, rgb(0,0,0) for black This feature is only supported when the UI Helper is swiftDialog 2.5.3 and later, and requires a text display in the help pane.		
UIHELPER_PICTURE_HELP **QR code - mailto URI scheme**	Dictionary	TYPE — String — qrcode QRCODE_DATA — String — mailto:mcs.support@agnosys.fr QRCODE_COLOR — String — rgb(159,73,190) MAILTO — Dictionary -- SUBJECT — String — Help Request -- BODY — String — Please provide assistance with the following issue: -- PLACEHOLDERS — Array -- -- Item 0 — String — Configuration : Discover macOS Compliance Spotter -- -- Item 1 — String — Computer Name : :ComputerName: -- -- Item 2 — String — Serial Number : :SerialNumber: -- -- Item 3 — String — Model Name : :ModelName: -- -- Item 4 — String — Hardware UUID : :HardwareUUID: -- -- Item 5 — String — macOS Version : :macOSVersion:

• TYPE : set to "qrcode" • QRCODE_DATA : an email address using "mailto:" to encode within the QR code • QRCODE_COLOR : the QR code's color in RGB format, for example, rgb(0,0,0) for black • MAILTO : - SUBJECT and BODY keys : the subject and the body of the email, which will be automatically populated - PLACEHOLDERS : optional information that will be inserted before the body text ; the example provides a list of all supported variables ; each item should be considered a separate line, separated by a empty line, and each line can contain any desired text and variables. This feature is only supported when the UI Helper is swiftDialog 2.5.3 and later, and requires a text display in the help pane.		
UIHELPER_PICTURE_HELP **Standard picture**	Dictionary	TYPE — String — file FILENAME — String — help.png
• TYPE : set to "file" • FILENAME : the picture to be displayed in the help pane (.png file expected) This feature is only supported when the UI Helper is swiftDialog 2.5.3 and later, and requires a text display in the help pane.		
UIHELPER_MAIN_TEXT_HELP	String	**ACME IT Support**\n\nUse your mobile device to scan the QR code. \nThis will take you directly to our support page.
The text to be displayed in the help pane. The string accepts markdown for message formatting. Use exactly two spaces followed by \n for a line break and \n\n for a line break followed by an empty line. Set to "undefined" to ignore the key.		
UIHELPER_BUTTON_LABEL_HELP	String	Close
The label to be displayed in the button of the help pane. This feature is only supported when the UI Helper is swiftDialog 2.5.5 and later, and requires a text display in the help pane.		
UIHELPER_MAIN_TEXT_LANDING	String	All tasks outlined have been completed, and IT Support will be automatically notified of the results.\r\rThank you for your assistance in enhancing the compliance of our devices.
The text to be displayed in the landing pane. Use exactly \r for a line break and \r\r for a line break followed by an empty line (no spaces around).		
SWIFTDIALOG_URL	String	https://github.com/swiftDialog/swiftDialog/releases/download/v2.5.5/dialog-2.5.5-4802.pkg
The URL used to download the swiftDialog package (dialog*.pkg file expected). When macOS 11 is detected, the URL is forcibly set to https://github.com/swiftDialog/swiftDialog/releases/download/v2.2.1/dialog-2.2.1-4591.pkg as version 2.2.1 is the newest version compatible. When macOS 12 is detected, the URL is forcibly set to https://github.com/swiftDialog/swiftDialog/releases/download/v2.4.2/dialog-2.4.2-4755.pkg as version 2.4.2 is the newest version recommended.		
FILEWAVE_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the FileWave integration defined by the FILEWAVE_CONFIGURATION Dictionary.		
FILEWAVE_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary
STATUS_MESSAGE_ERROR : message built when the status message is an error message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_INFO : message built when the status message is an informative message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_SUCCESS : message built when the execution is successful : :Date: :Time: :StatusMessage: Execution date : :ExecutionDate:. mSCP baseline name : :mSCPBaselineName:. mSCP compliance score : :mSCPComplianceScore:%. UPLOAD_KEYS : remove the "disabled-" prefix before each mCS property name whose value must be uploaded using API calls to the named Custom Fields, for Immediate reporting. The Custom Field that store status messages must have Data Type "String". The Custom Field that stores the execution date must have Data Type "Date/Time". The Custom Field that stores the mSCP compliance score must have Data Type "Integer". When creating a Custom Field, select "Administrator" from the "Provided By" menu and check the box "Assigned to all devices".		
JAMF_PRO_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the Jamf Pro integration defined by the JAMF_PRO_CONFIGURATION Dictionary.		
JAMF_PRO_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary

STATUS_MESSAGE_ERROR : message built when the status message is an error message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_INFO : message built when the status message is an informative message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_SUCCESS : message built when the execution is successful : :Date: :Time: :StatusMessage: Execution date : :ExecutionDate:. mSCP baseline name : :mSCPBaselineName:. mSCP compliance score : :mSCPComplianceScore:%. UPDATE_INVENTORY : set to "true" to trigger an Inventory Update at the "Device details update". The following Extension attributes are provided in the "mcs_library > Jamf Pro - Extension attributes" folder of the mcs-Toolkit to retrieve values from the follow-up file at the next inventory update : - mCS - Last Jamf Pro status message.xml : to collect the Jamf Pro status message defined by the keys listed above - mCS - Last execution date.xml : to collect the last execution date - mCS - Last mSCP compliance score.xml : to collect the mSCP compliance score - mCS - Last status message.xml : to collect the status message (raw message for a success, informative or error event). UPLOAD_KEYS : remove the "disabled-" prefix before each mCS property name whose value must be uploaded using API calls to the named Extension attributes, for Immediate reporting. Values of mCS property names uploaded using API calls to Extension attributes must not also be uploaded using the Extension attributes listed above, and vice versa. The Extension attributes that store status messages must have Data Type "String". The Extension attribute that stores the execution date must have Data Type "Date". The Extension attribute that stores the mSCP compliance score must have Data Type "Integer". In the context of Immediate reporting, their Input Type is "Text Field".		
MICROSOFT_INTUNE_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the Microsoft Intune integration defined by the MICROSOFT_INTUNE_CONFIGURATION Dictionary.		
MICROSOFT_INTUNE_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary
STATUS_MESSAGE_ERROR : message built when the status message is an error message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_INFO : message built when the status message is an informative message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_SUCCESS : message built when the execution is successful : :Date: :Time: :StatusMessage: Execution date : :ExecutionDate:. mSCP baseline name : :mSCPBaselineName:. mSCP compliance score : :mSCPComplianceScore:%. The following Custom attributes are provided in the "mcs_library > Microsoft Intune - Custom attributes" folder of the mCS-Toolkit to retrieve values from the follow-up file at their next execution : - mCS - Last Microsoft Intune status message.sh : to collect the Microsoft Intune status message defined by the keys listed above - mCS - Last execution date.sh : to collect the last execution date - mCS - Last mSCP compliance score.sh : to collect the mSCP compliance score - mCS - Last status message.sh : to collect the status message (raw message for a success, informative or error event). UPLOAD_KEYS : - remove the "disabled-" prefix before each mCS property name whose value must be uploaded using API calls to the numbered Extension attributes, for Immediate reporting - each value must include "extensionAttribute*N*" (*N* is an number between 1 and 15) and optionally after a comma, a string added before the value of the mCS property name. Extension attributes are visible in Microsoft Entra admin center > Identity > Devices > All devices > Device > Properties > Extension attributes. Be careful not to use an Extension attribute that already contains useful data. Values of mCS property names uploaded using API calls to Extension attributes must not also be uploaded using the Custom attributes listed above, and vice versa.		
MSCP_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the mSCP integration defined by the MSCP_CONFIGURATION Dictionary.		
MSCP_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary

COMPLIANCE_REMEDIATION : set to "true" to trigger the remediation planned by the compliance script before a scan COMPLIANCE_REMEDIATION_METHOD : For each macOS version supported in your environment, specify the method to use for executing the script for compliance remediation. Example of a value : - `script:cis_lvl1_compliance.sh` : name of the script embedded in the mCS-Content - `event:Sequoia_cis_lvl1-fix` : name of the Jamf Pro policy custom trigger - `id:100` : Jamf Pro policy ID (alternative to a custom trigger) COMPLIANCE_REMEDIATION_SETTINGS > PREFER_PRIVILEGED_HELPER : set to "true" to delegate the execution of the script to the mCS Privileged Helper COMPLIANCE_SCAN : set to "true" to trigger a scan COMPLIANCE_SCAN_METHOD : For each macOS version supported in your environment, specify the method to use for executing the script for compliance scan. Example of a value : - `script:cis_lvl1_compliance.sh` : name of the script embedded in the mCS-Content - `event:Sequoia_cis_lvl1-check` : name of the Jamf Pro policy custom trigger - `id:101` : Jamf Pro policy ID (alternative to a custom trigger) COMPLIANCE_SCAN_SETTINGS > PREFER_PRIVILEGED_HELPER : set to "true" to delegate the execution of the script to the mCS Privileged Helper COMPLIANCE_SCORE_FAILURE : percentage of compliance score below which a failure message is processed by the Compliance report and webhook alerts COMPLIANCE_SCORE_WARNING : percentage of compliance score below which a warning message is processed by the Compliance report and webhook alerts		
PROXY_INTEGRATION (inside INTEGRATIONS Dictionary)	Boolean	true
Set to "true" to enable the Proxy integration defined by the PROXY_CONFIGURATION Dictionary.		
PROXY_CONFIGURATION (inside INTEGRATIONS Dictionary)	Dictionary	Refer to the template for the structure of the Dictionary
KERBEROS_REALM : Kerberos realm name visible in the Ticket Granting Service (TGS) of the Proxy Service Principal ; set the key to "undefined" (exactly) if the Proxy is not configured for Kerberos authentication PROXY_URL : URL of the Proxy beginning with http:// PROXY_PORT : port of the Proxy URL_PROBE : URL of an external website that returns a "body" content only when the connectivity through the Proxy is verified The configuration is triggered for the current execution only when the URL defined by the URL_PROBE key cannot be accessed directly without Proxy.		
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) RSA encryption : use the script "mcs_rsa_engine" to generate the full value including the "RSA-" prefix. In the following examples, ":warning:" is an emoji (refer to https://www.webfx.com/tools/emoji-cheat-sheet/) and ":Date:" 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 execution is successful :white_check_mark: :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: Execution date : :ExecutionDate: MESSAGE_FLIGHT_RECORDER : message sent when the Flight recorder has recorded at least one error during the workflow :warning: Date : :Date: :Time:\rModel Name : :ModelName:\rSerial Number : :SerialNumber:\rComputer Name : :ComputerName:\rLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)\rmacOS Version : :macOSVersion:\rFlight Recorder Report :\r:FlightRecorderReport: MESSAGE_MSCP_COMPLIANCE : message sent for the compliance report generated by the mSCP integration Date : :Date: :Time:\rModel Name : :ModelName:\rSerial Number : :SerialNumber:\rComputer Name : :ComputerName:\rLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)\rmacOS Version : :macOSVersion:\rmSCP Compliance Report :\r:mSCPComplianceReport: FILTERED_MESSAGES : list of message IDs separated with commas which should not trigger a notification		
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 the Integration Guide for the details) RSA encryption : use the script "mcs_rsa_engine" to generate the full value including the "RSA-" prefix. In the following examples, "⚠" is an emoji (refer to https://unicode.org/emoji/charts/full-emoji-list.html) followed by a wide space and ":Date:" 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 execution is successful ✅ :Date: :Time: :ModelName: :SerialNumber: :HardwareUUID: :ComputerName: - Status message : :StatusMessage: Execution date : :ExecutionDate: MESSAGE_FLIGHT_RECORDER : message sent when the Flight recorder has recorded at least one error during the workflow ⚠ Date : :Date: :Time:\n\nModel Name : :ModelName:\n\nSerial Number : :SerialNumber:\n\nComputer Name : :ComputerName:\n\nLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:) \n\nmacOS Version : :macOSVersion:\n\nFlight Recorder Report :\n\n:FlightRecorderReport: MESSAGE_MSCP_COMPLIANCE : message sent for the compliance report generated by the mSCP integration Date : :Date: :Time:\n\nModel Name : :ModelName:\n\nSerial Number : :SerialNumber:\n\nComputer Name : :ComputerName:\n\nLogged In Account : :LoggedInAccountRealName: (:LoggedInAccount:)\n\nmacOS Version : :macOSVersion:\n\nmSCP Compliance Report :\n\n:mSCPComplianceReport: FILTERED_MESSAGES : list of message IDs separated with commas which should not trigger a notification		
VMWARE_WORKSPACE_ONE_INTEGRATION **(inside INTEGRATIONS Dictionary)**	Boolean	true
Set to "true" to enable the VMware Workspace ONE integration defined by the VMWARE_WORKSPACE_ONE_CONFIGURATION Dictionary.		
VMWARE_WORKSPACE_ONE_CONFIGURATION **(inside INTEGRATIONS Dictionary)**	Dictionary	Refer to the template for the structure of the Dictionary
STATUS_MESSAGE_ERROR : message built when the status message is an error message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_INFO : message built when the status message is an informative message : :Date: :Time: :StatusMessage: STATUS_MESSAGE_SUCCESS : message built when the execution is successful : :Date: :Time: :StatusMessage: Execution date : :ExecutionDate:. mSCP baseline name : :mSCPBaselineName:. mSCP compliance score : :mSCPComplianceScore:%. The following Sensors / Custom attributes (to be used in Profiles) are provided in the "mcs_library > VMware Workspace ONE - Sensors or Custom attributes" folder of the mCS-Toolkit to retrieve values from the follow-up file at their next execution : - mcs_last_vmwareworkspaceone_status_message.sh : to collect the VMware Workspace ONE status message defined by the keys listed above - mcs_last_execution_date.sh : to collect the last execution date - mcs_last_mscp_compliance_score.sh : to collect the mSCP compliance score - mcs_last_status_message.sh : to collect the status message (raw message for a success, informative or error event). UPLOAD_KEYS : remove the "disabled-" prefix before each mCS property name whose value must be uploaded using API calls to the named Custom attributes, for Immediate reporting. Values of mCS property names uploaded using API calls to Custom attributes must not also be uploaded using the Sensors / Custom attributes (to be used in Profiles) listed above, and vice versa.		
ACCOUNT_STATUSES **(inside NATIVE_MODULES Dictionary)**	Dictionary	ENABLED — Boolean — true DEMOTING_EXCEPTIONS — String — cadmin,tom,jerry,/^admin.+/,group:devs

ENABLED : set to "true" to enable the accounts status management capability.
DEMOTING_EXCEPTIONS : optional accounts and groups (prefixed with "group:") separated with commas.
Disclaimer : do not forget to add the admin account(s) used by IT Support to the list, if applicable.
Accounts and members of groups that are listed retain their admin status or are promoted to admin status.
Accounts and members of groups that are not listed are demoted to standard status.
Accounts can be validated using a regular expression functional in a shell script and enclosed within double slashes, as shown in these examples :
- /^admin.*/ : to match accounts that start with "admin" followed by any sequence of characters
- /^admin.+/ : to match accounts that start with "admin" followed by one or more of any characters
- /^admin[0-9]*$/ : to match accounts that start with "admin" followed by zero or more digits.
The evaluation of the listed accounts and groups is terminated when the first match applies.
The accounts promoted or demoted are limited to those for which a password is defined.
To enhance privacy, the list may be encrypted.
RSA encryption : use the script "mcs_rsa_engine" to generate the full value including the "RSA-" prefix.

EXTERNAL_MODULES	Dictionary	LIST — Array -- Item 0 — Dictionary -- -- TYPE — String — script -- -- DISPLAYNAME — String — Script A -- -- ICON — String — script_a_icon.png -- -- FILENAME — String — script_a.sh -- -- PARAMETERS — String — -a 10 -- -- TIMEOUT — Integer — 10 -- -- SIGNATURE — String — encoded_signed_script_hash (auto-generated)

List of external modules executed during the workflow.
TYPE : set to "script"
DISPLAYNAME : the name displayed for the script in the stages list
ICON : the icon embedded in the mCS-Content which is displayed for the script in the stages list
FILENAME : the name of the script embedded in the mCS-Content which is executed
PARAMETERS : the parameters (options and arguments) passed to the script upon execution
PREFER_PRIVILEGED_HELPER : set to "true" to delegate the execution of the script to the mCS Privileged Helper
TIMEOUT : the maximum wait time in seconds before waiting is interrupted
A template for an external module is available : mCS-Toolkit > mcs_library > placeholder.sh
Scripts are automatically hashed, and the hashes are signed during the conversion of an mCS configuration file into a Custom configuration profile. Signatures are stored in the SIGNATURE key of each dictionary.
When the script terminates with a zero exit code, the Flight Recorder reports the display name and the string that the script sends to standard output, which is enclosed within tags of any name, following the structure <tag>string</tag> (e.g. <result>Printer management privileges granted</result>).
When the script terminates with a non-zero exit code, the Flight Recorder reports the display name and the exit code.
When the script terminates due to tampering detection, the Flight Recorder reports the display name along with the message "Unverified signature".
When the script terminates due to a timeout, the Flight Recorder reports the display name along with the message "Timeout exceeded".
When script execution is delegated to the Privileged Helper, its signature is verified before invocation. If the script is not executed due to tampering detection, the Flight Recorder reports the script display name along with the message "Unverified Privileged Helper".