

LAPS

The Kandji way

trams | econocom

- + CISO @ Trams|Econocom
- + github.com/ons-mart
- + linkedin.com/in/martijngregoire
- + martijn.gregoire@trams.co.uk

trams | econocom



Martijn Gregoire

LAPS: Who, What & Why

trams | econocom

Requirements

- No clear text credentials
- Rotate password after use
- Auto rotate at set interval
- Retrieval should work when device is offline

My Solution

Create user accounts

Create Administrator or Standard user accounts if they do not already exist.

Warning:

Kandji will only create a user account if it does not already exist. Updating a user password in this Parameter will not update a password for an existing local user.

macOS 10.13+

NIST

Account #1

Full name

Trams Administrator

Short name (Account name)

tramsadmin

Password

.....

Path to home folder

/private/var

User type

Administrator

Demote user accounts to Standard

Demotes local accounts to Standard users. At least one administrator user account must excluded from the demotion process.

Warning:

Please thoroughly test and understand user demotion before deploying to end users. Kandji will prompt for a restart when users are demoted to Standard.

Dependency:

Create user accounts

macOS 10.13+

NIST

Excluded administrator short names (account names)

tramsadmin

+ Add Exclusion

My Solution

>_

Admin Password Rotation

...

Active

Custom Script

Run any type of script supported by macOS. Choose to run once per device or continuously, and add an optional remediation script that can be run when needed. If you do not specify a shell or interpreter, scripts will run in shell (/bin/sh).

Publisher:

Kandji, Inc.

Device families:

Mac

OS requirement:

macOS 10.11+

⚠

WARNING: This is a very powerful feature. All scripts run as root. Test your scripts extensively before deploying to production machines.

Audit Script

⚠ A script's reported status depends on the exit code. An exit code of 0 means the item will pass, otherwise an alert will be triggered.

1

#!/bin/bash

2

3

#####

4

#

5

#

6

#

7

#

8

Hide details in Kandji

9

#

10

#

11

#

12

#

13

#

14

#####

Remediation Script

⚠ Remediation scripts are executed only when audit scripts fail, which is determined if a script's exit code is anything but 0. Upon success of a remediation script, a status of "remediated" will be shown. Should the script fail, an alert will be triggered and enforcement will stop until the Library Item is flushed.

1

#!/bin/bash

2

3

#####

4

#

5

#

6

#

7

#

8

Hide details in Kandji

9

#

10

#

11

#

12

#

13

#

14

#####

Audit

- No note found
- Incorrect epoch
- Epoch in the past

```
#!/bin/bash

#####
#
#
#
# Hide details in Kandji
#
#
#
#####

APIkey="<KANDJI API Key>"
URL="<KANDJI API URL>"

### get device_id
serialnumber=$(system_profiler SPHardwareDataType | awk '/Serial Number/{print $4}')
deviceid=$(curl -sk GET "$URL/api/v1/devices?serial_number=$serialnumber" --header "Authorization: Bearer $APIkey" | grep -o "device_id":
*"[""]*" | awk -F "' ' '{print$4}'")

#loop through device notes for encrypted details
jsonoutput=$(curl -sk GET "$URL/api/v1/devices/$deviceid/notes" --header "Authorization: Bearer $APIkey")
index=$(plutil -extract "notes" raw - <<< $jsonoutput)

if [[ ${index} == 0 ]]; then
    echo "No notes found"
    exit 1
fi

for ((i=0; i<$index; i++)); do
    content=$(plutil -extract "notes".$i."content" raw - <<< $jsonoutput)
    regex='^<p>key:.*<br>secret:.*<br>nr:.*</p>$'
    if [[ $content =~ ${regex} ]]; then
        renewepoch=$(echo $content | awk -F '<br>nr: ' '{print$2}' | awk -F '-' '{print$1}')
        break
    fi
done

#check if epoch is found and coreetly formatted
epochregex='^[0-9]{10}$'
if [[ ! ${renewepoch} =~ ${epochregex} ]]; then
    echo "Incorrect epoch"
    exit 1
fi

#get current epoch
current=$(date +%s)

#check if renew epoch is in the future
if [[ ${current} > ${renewepoch} ]]; then
    echo "admin password needs to be renewed"
    exit 1
fi

exit 0
```

Remediation

- Check for local admin
- Check note for password
- Verify current password
- Set new password
- Verify new password
- Create new note
- Report to Slack

```
#!/bin/bash

#####
#
#
#
# Hide details in Kandji
#
#
#
#####

APIkey="<KANDJI API Key>"
URL="<KANDJI API URL>"
Slack="<Slack Webhook>"
adminaccount="<Admin account>"
initialpassword="<Initial admin password>"
passwordlength=12
specialchar="true" #add special characters in password. true or false.
renewdays=30 #standard password rotation after x days

#### MAIN CODE ####

### get device_id
serialnumber=$(system_profiler SPHardwareDataType | awk '/Serial Number/{print $4}')
deviceid=$(curl -sk GET "$URL/api/v1/devices?serial_number=$serialnumber" --header "Authorization: Bearer $APIkey" | grep -o '"device_id": *"[^"]*"') | awk -F '"' '{print$4}')

### verify local account exists
```

trams | econocom



LAPS Notification APP 10:58 AM

Admin password rotated

Serial:
ZFJCC7M4MC

Next renewal:
27/10/2023

Device note in Kandji



LAPS- ZFJCC7M4MC

Model:	Virtual Machine	User:	Not assigned
Serial:	ZFJCC7M4MC	Asset tag:	Laps9999
OS:	13.6 (22G120)	Blueprint:	Kandji LAPS
Last Check-in:	7 minutes ago		


Status Activity Details Notes Applications

+ Create New Note


Martijn Gregoire Yesterday

key: U2FsdGVkX18E4o6uGPflja/OPI5z0Cnef8DwNz8xhns=
secret: FdYpCDI2zM5+CO
nr: 1698408118

Retrieve the password



LAPS



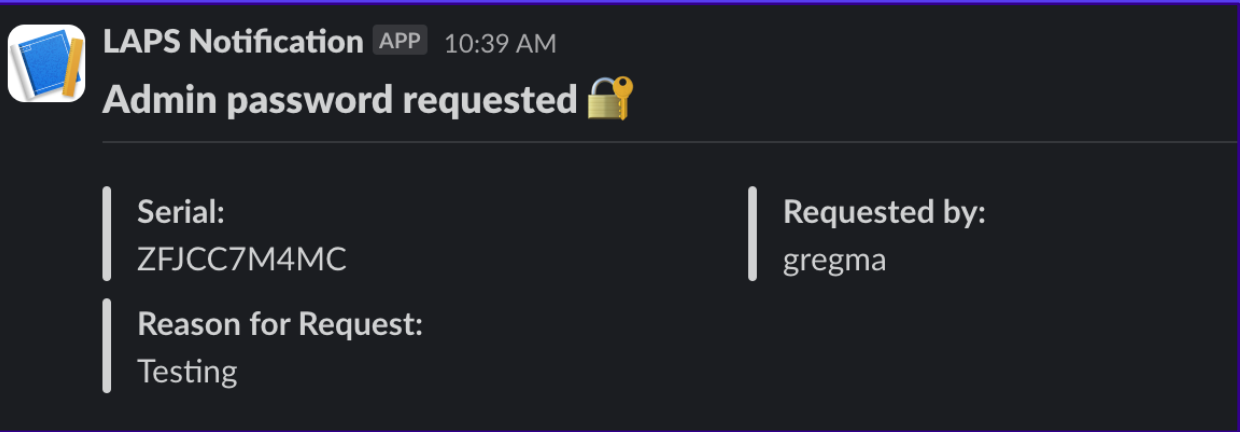
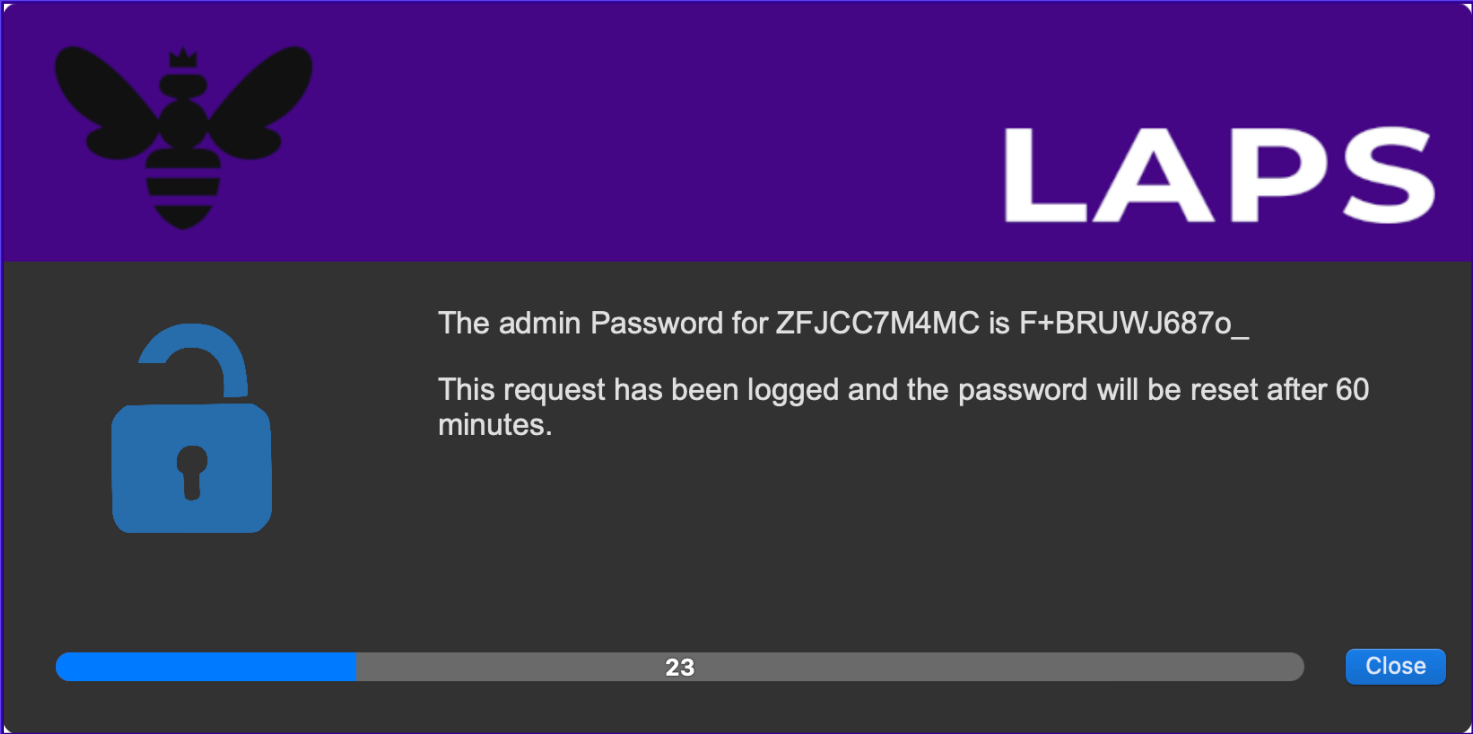
Please enter the serial of the device you wish to see the Admin password for. Please specify the reason why this password is required.

Serial *

Reason *

* Required Fields

Retrieve the password



What's next

trams | econocom

Thanks

trams | econocom