Randomize your Local Administrator Passwords

Who am I?

Joshua D. Miller

@JMiller

https://github.com/joshua-d-miller

https://joshua-d-miller.com

What is macOSLAPS?

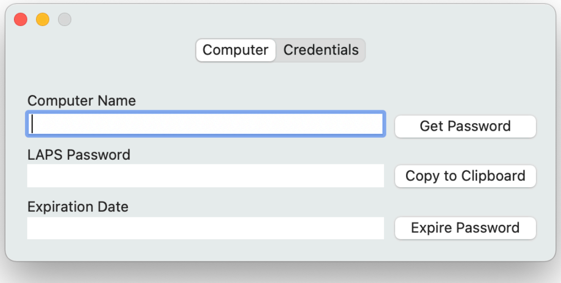
- LAPS - Local Administrator Password Solution
- A Swift binary that performs password rotation of a specified administrator account
- Customizable (Can be used with an MDM)
- Easy to use
- Open Source

Why use macOSLAPS?

- Local Admin Account Rotation that is unique to each system
- Easy to look up the password in AD or MDM
- Give your user the password for a limited amount of time
- Be as simple or as complex in your password as you’d like
- Have a user to maintain secureToken
- Universal

Retrieving LAPS Passwords

- LAPS for macOS utility will allow an Active Directory bound machine to retrieve passwords for macOS and Windows clients
  - Expire a Password immediately
  - Set a custom expiration
  - Saving privileged credentials to keychain
  - Great readable password font
  - Universal



Configuring macOSLAPS

- Install the PKG
- Configure the PLIST
- Run the Binary

Install the PKG

- The PKG installer can be downloaded from https://github.com/joshua-d-miller/macOSLAPS/releases
- Use your favorite deployment service to install the pkg

Configure the PLIST

- macOSLAPS will read it's configuration from the following locations:
  - /Library/Preferences/edu.psu.macOSLAPS
  - /Library/Managed Preferences/edu.psu.macOSLAPS <— **MDM**
- If neither of these exist then the default values will be used and the binary will most likely fail

Configure the PLIST (Without an MDM)

- Use the *defaults* command to write to the PLIST
- Examples:
  - defaults write /Library/Preferences/edu.psu.macOSLAPS LocalAdminAccount youradminhere
  - defaults write /Library/Preferences/edu.psu.macOSLAPS DaysTillExpiration -int 25

Configure the PLIST (MDM)

- The PLIST can be uploaded to jamf Pro or your MDM of choice
- jamf Pro Schema: https://github.com/Jamf-Custom-Profile-Schemas/joshua-d-miller-schemas/blob/master/edu.psu.macoslaps.json
- Keys required - LocalAdminAccount
- Default Values

Account	Password Length	Expire in	Characters Removed	Keychain Removal	Method
admin	12 Characters	60 Days	'	Yes	Active Directory

Customizing macOSLAPS

LocalAdminAccount	Shortname for the account we want to rotate
DaysTillExpiration	How many days to wait until expiring the password
PasswordLength	How long the generated password will be
RemoveKeyChain	Removes the local administrator's keychain
RemovePassChars	Exclude specific characters from being used in the password
ExclusionSets	Exclude an entire character set

Accounting for secureToken

- In macOS 10.13 and above with the introduction to APFS users that can administer or unlock the device via FileVault will be given an additional tag on their account called a secureToken
- We must know the current Password in order to change an account's password that has a secureToken
- FirstPass
  - Enter a string value that is a "burner" password that will be used to perform the first password change in macOSLAPS
  - Subsequent password changes will rely on access to a keychain item in System Keychain called macOSLAPS

What if I have Read Only Domain Controllers?

- PreferredDC
  - Allows us to specify a specific domain controller that we know is writable to ensure password change. (FQDN required)

Sending the password to MDM

- Method
  - **AD** - Keeps sending the password Active Directory
  - **Local** - Password is only kept locally so that MDMs can pick up the password and expiration date

Sending the Password to MDM (Continued)

- To retrieve the password for MDM a script can be called that runs the following
  - */usr/local/laps/macOSLAPS -getPassword*
- Password and expiration date are saved in the folder /var/root/Library/Application Support. Two files are created called
  - macOSLAPS-password
  - macOSLAPS-expiration
- MDM agents can read the contents of these files and report results back
- Files are deleted the next time macOSLAPS runs via the LaunchAgent or manually

Password Grouping

- New feature to allow the passwords to appear similar to Safari type passwords

PasswordGrouping	Define the number of characters you would like to be in each group
PasswordSeparator	Define the separator you would like to use (Default -)

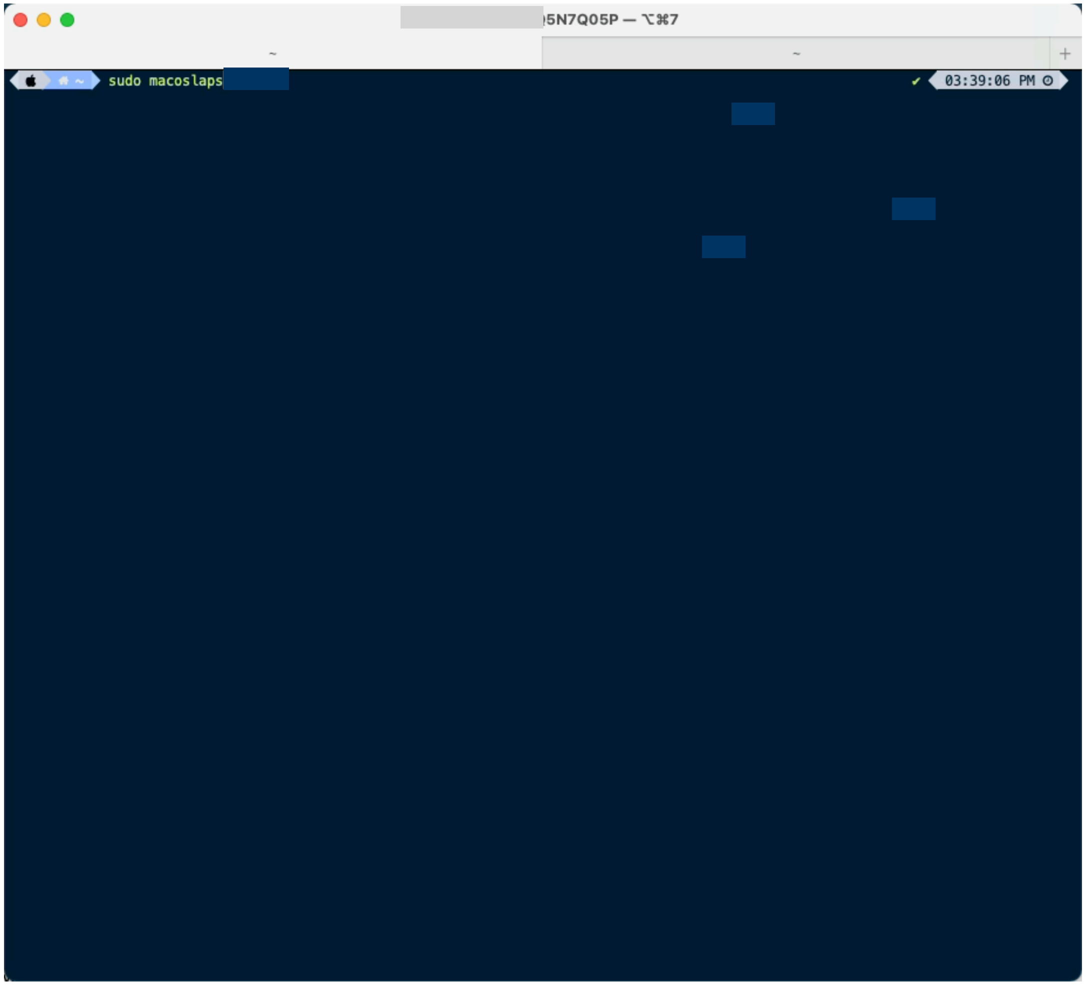
- Example - *les3-#81n-@imd*
  - PasswordLength is 12
  - PasswordGrouping is 4
  - PasswordSeparator is -

Run the Binary

- By default if installed using the PKG installer macOSLAPS will run every 90 minutes
- Can be invoked manually using */usr/local/laps/macOSLAPS*
  - Must be run as root
- Can be called via a script using the above method
- Reset the password and disregard the expiration date
  - */usr/local/laps/macOSLAPS -resetPassword*
- *Get the version*
  - */usr/local/laps/macOSLAPS -version* (Will not perform password check)

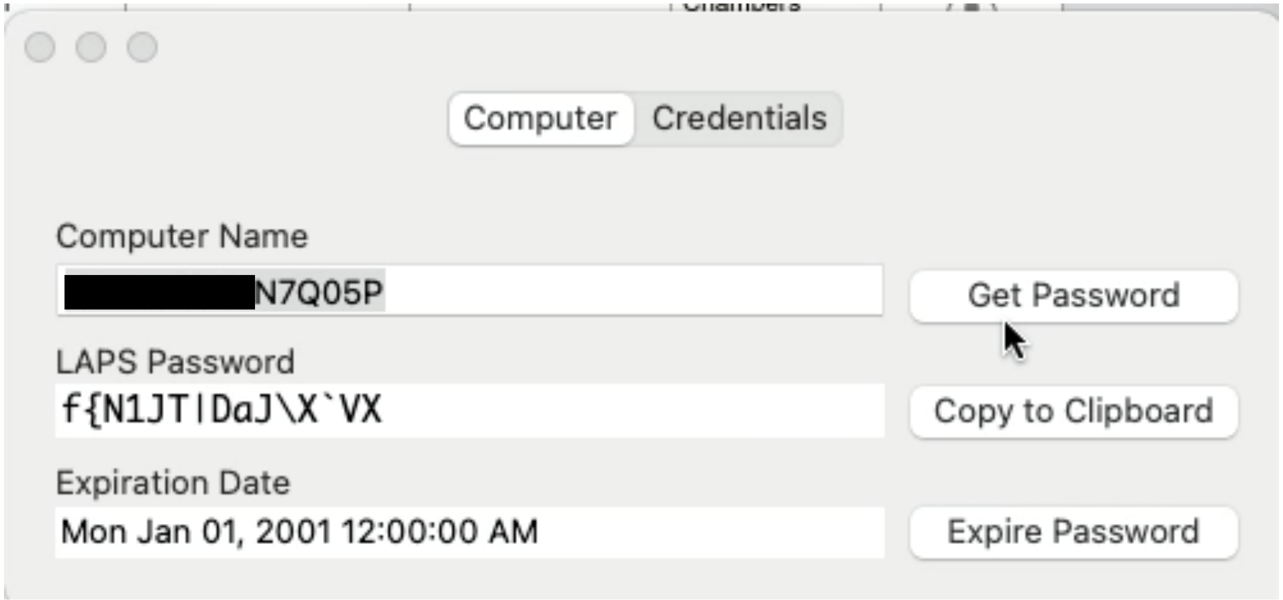
Bug Fixes

- Error checking improved for AD Method
    - If the password change fails to write to Active Directory, the binary will log this and revert to the previous password before exiting
- ISODate Formatting
    - Will allow the date to be formatted correctly locally and internationally



```
 ~  sudo macoslaps[redacted]                                          ✔  03:39:06 PM 
                                              [redacted]

                                                                [redacted]
                                            [redacted]
```



Computer Name

[redacted]N7Q05P

LAPS Password

f{N1JT|DaJ\X`VX

Expiration Date

Mon Jan 01, 2001 12:00:00 AM

Thank you
Questions?

macOSLAPS	https://tinyurl.com/374rxahj
LAPS-for-macOS	https://tinyurl.com/8a32zb8s
jamf Pro Schema	https://tinyurl.com/j9cv4e8
jamf Pro Extension Attribute	https://tinyurl.com/mazmtt87