WHATS NEW IN MACOSLAPS

MACADMINS 2021 CAMPFIRE SESSIONS

WHO AM I?

Joshua D. Miller

@JMiller

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

https://joshua-d-miller.com

WHAT IS MACOSLAPS?

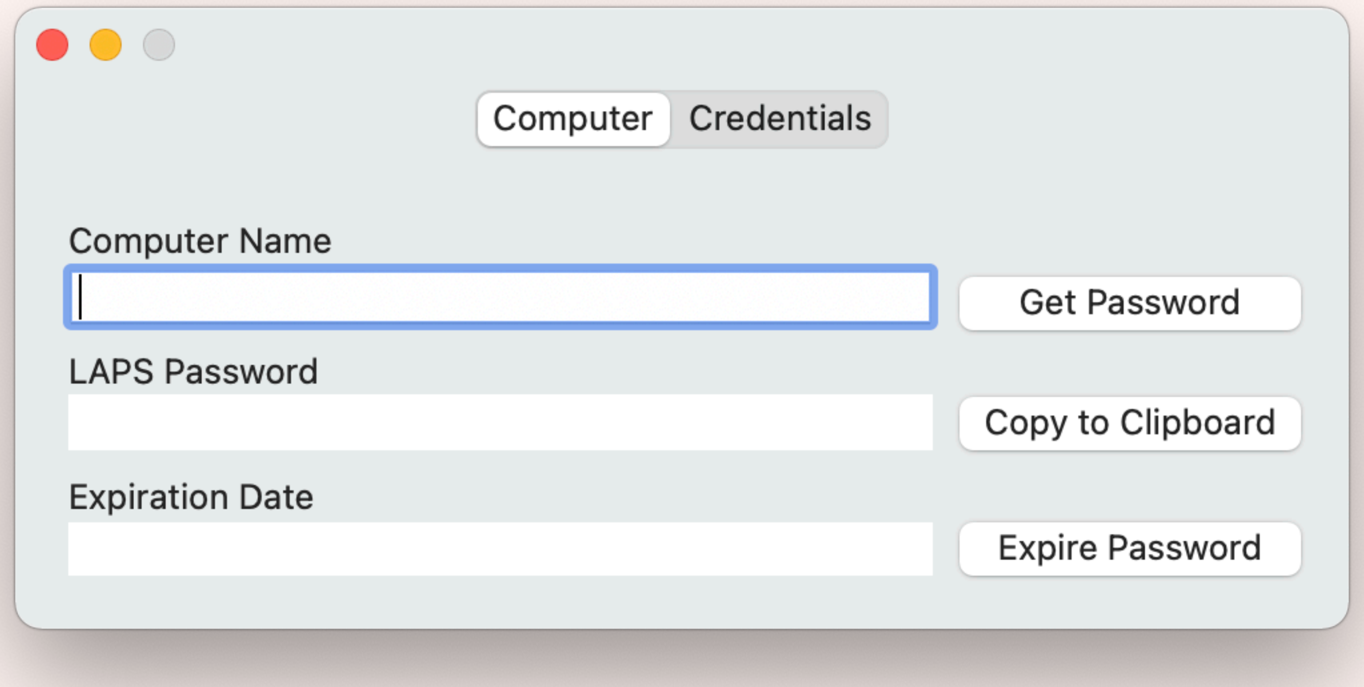
- LAPS - Local Administrator Password Solution
- A Swift binary that performs password rotation of a specified administrator account
- Customizable (Can be used with an MDM)
- Easy to use
- Open Source

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

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 you will need to specify**
    - **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
- Enter the FirstPass key
  - 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**
  - If you'd like to continue using Active Directory the default option for this is AD or you can set it to AD to be sure. If you would like to use the local method then you would set this key to Local
- The password is only recorded in the keychain item

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 following locations
  - */var/root/Library/Application Support/macOSLAPS-password*
  - */var/root/Library/Application Support/macOSLAPS-expiration*
- MDM agents (jamf Binary / WorkspaceOne cli) could read the contents of these files and report them to the MDM
- Files are deleted the next time macOSLAPS runs via the LaunchAgent or manually

PASSWORD GROUPING

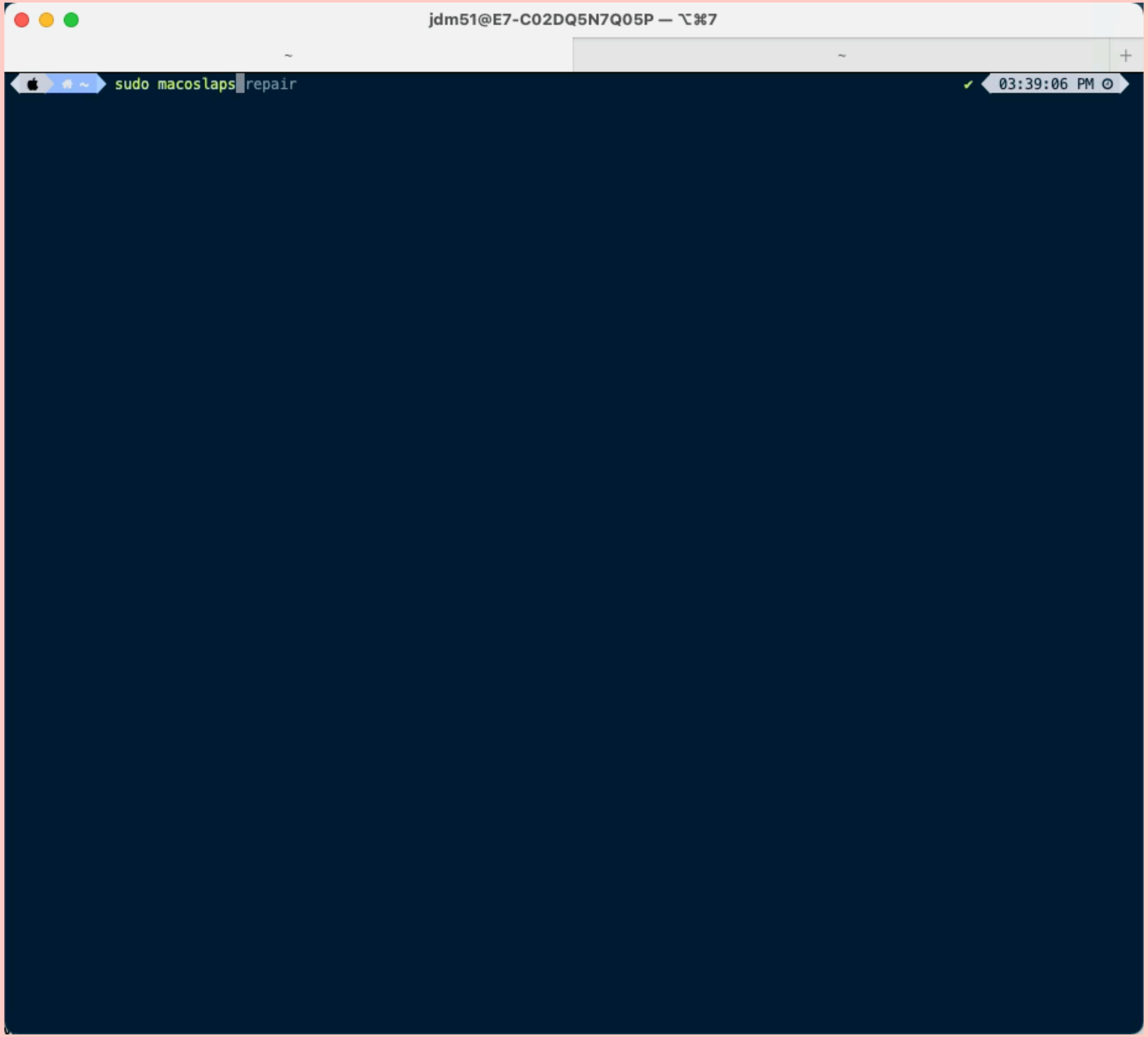
- New feature implemented by Per Olofsson (@magervalp) to allow the passwords to appear similar to Safari type passwords
- PasswordGrouping
  - Define the number of characters you would like to be in each group
- PasswordSeparator
  - Define the separator you would like to use (Default -)
- Example (With PasswordLength set to 12, PasswordGrouping set to 4 and PasswordSeparator set to -
  - les3-#81n-@imd

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)

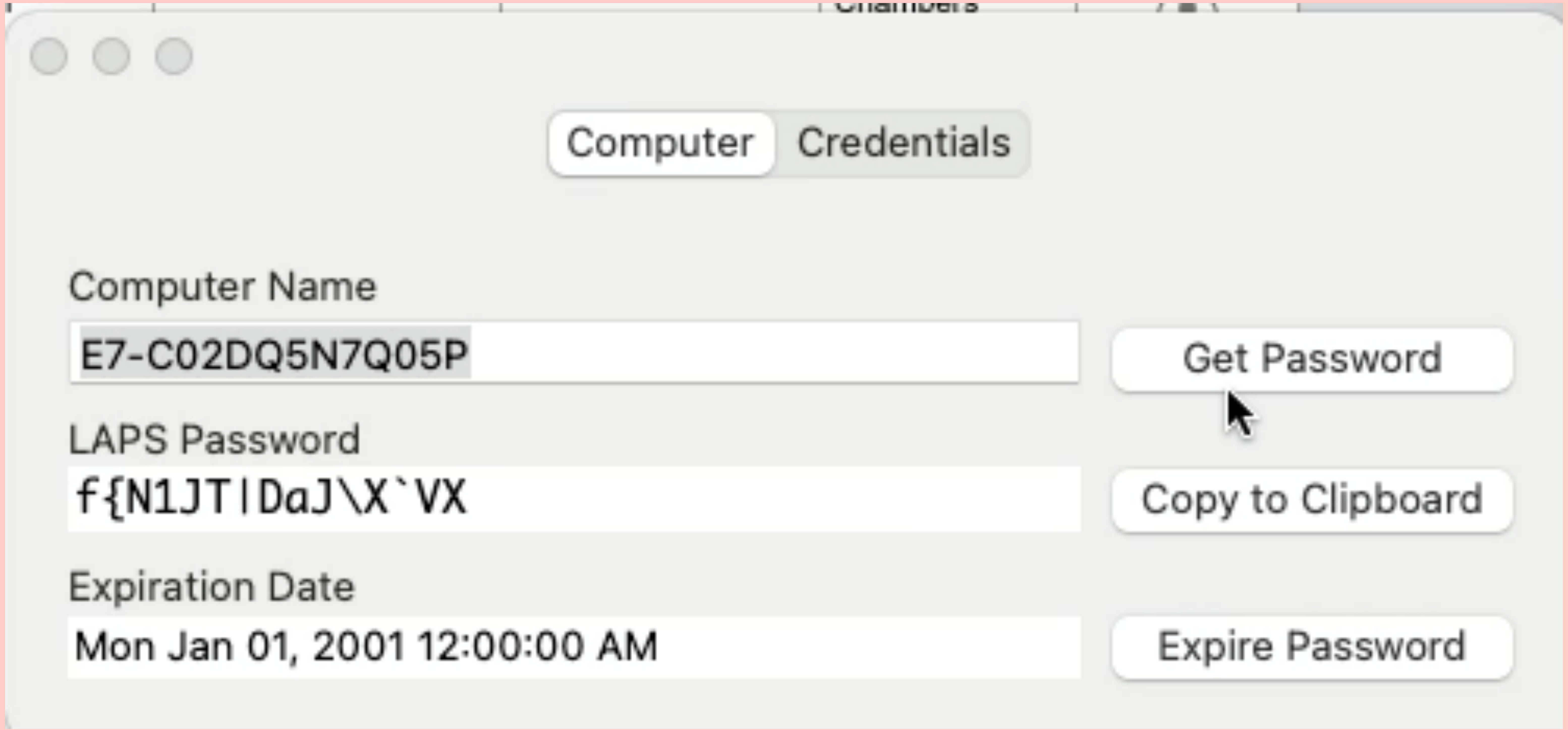
BUG FIXES

- 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
  - Thanks to Per Olofsson (@magervalp) on his insight and shared code to allow the date to work properly internationally
- Certificate Rotation
  - A secondary binary is deployed with macOSLAPS called macOSLAPS-repair to allow rotation of the Developer ID certificate if needed to maintain access to the keychain item
  - Major thanks to Joel Rennich (@mactroll) and Mike Lynn (@frogor)



```
 ~ sudo macoslaps repair                                              ✔ 03:39:06 PM
```

LAPS FOR MACOS DEMO



Computer Name

E7-C02DQ5N7Q05P

LAPS Password

f{N1JT|DaJ\X`VX

Expiration Date

Mon Jan 01, 2001 12:00:00 AM

THANK YOU

macOSLAPS (Set the Password): https://github.com/joshua-d-miller/macOSLAPS
LAPS-for-macOS (Get the Password): https://github.com/joshua-d-miller/LAPS-for-macOS
macOSLAPS Jamf Schema: https://github.com/Jamf-Custom-Profile-Schemas/joshua-d-miller-schemas/blob/master/edu.psu.macoslaps.json