



# Escrow Buddy

A Tool for Escrowing Missing  
FileVault Recovery Keys



<https://tinyurl.com/JNUC23-EB>





# Elliot Jordan

Senior Client Systems Engineer • Netflix

<https://tinyurl.com/JNUC23-EB>



## Escrow Buddy Logs

Filtering the log data using "subsystem == "com.netflix.Escrow-Buddy""



```
Mon Jul 31 20:53:03 PDT 2023
{
  "httpStatus": 404,
  "errors": [
    {
      "code": "INVALID_ID",
      "description": "FileVault information for computer with
given id does not exist",
      "id": "18984",
      "field": null
    }
  ]
}
```



User Experience



## Escrow Buddy Logs

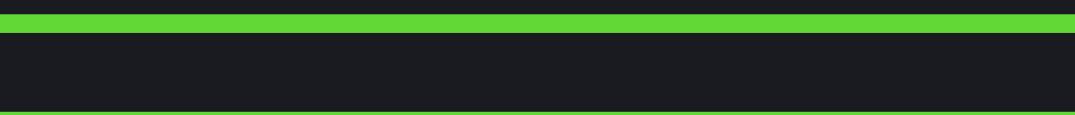
Filtering the log data using "subsystem == "com.netflix.Escrow-Buddy""



## Jamf FileVault Info

Mon Jul 31 20:53:03 PDT 2023

```
{  
  "httpStatus": 404,  
  "errors": [  
    {  
      "code": "INVALID_ID",  
      "description": "FileVault information for computer with  
given id does not exist",  
      "id": "18984",  
      "field": null  
    }  
  ]  
}
```



User Experience

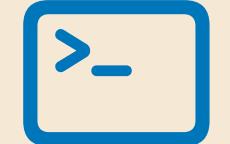
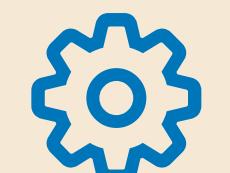


# Why are my FileVault recovery keys **missing**?

- กระเป๋า Migration from another MDM
- ⌚ Encrypted before enrollment
- ⚙️ Escrow profile misconfigured
- eraser Data loss or corruption



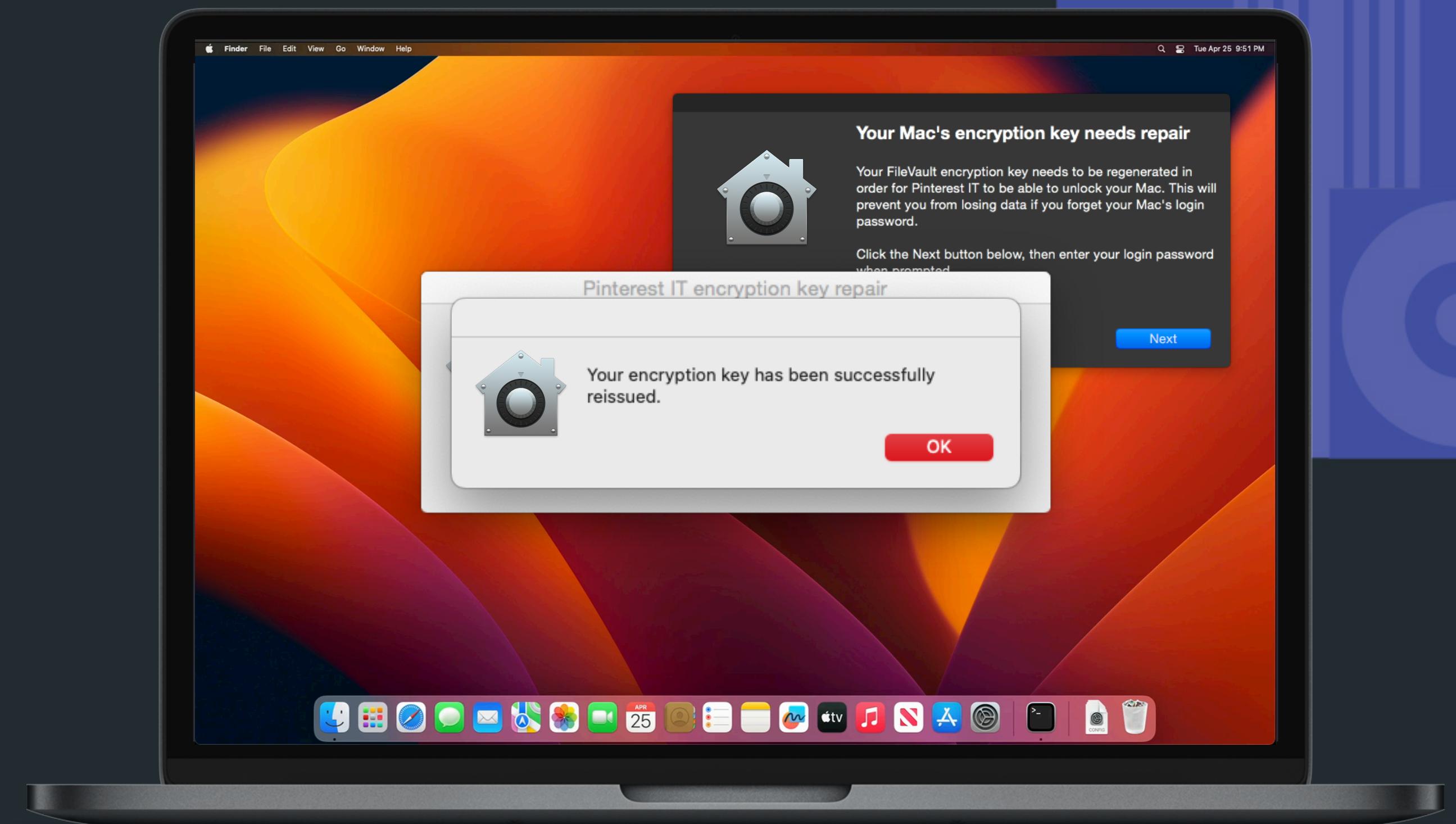
# How can I solve missing FileVault recovery keys?

-  Toggle FileVault off/on
-  Manually use `fdesetup`
-  Automate `fdesetup`



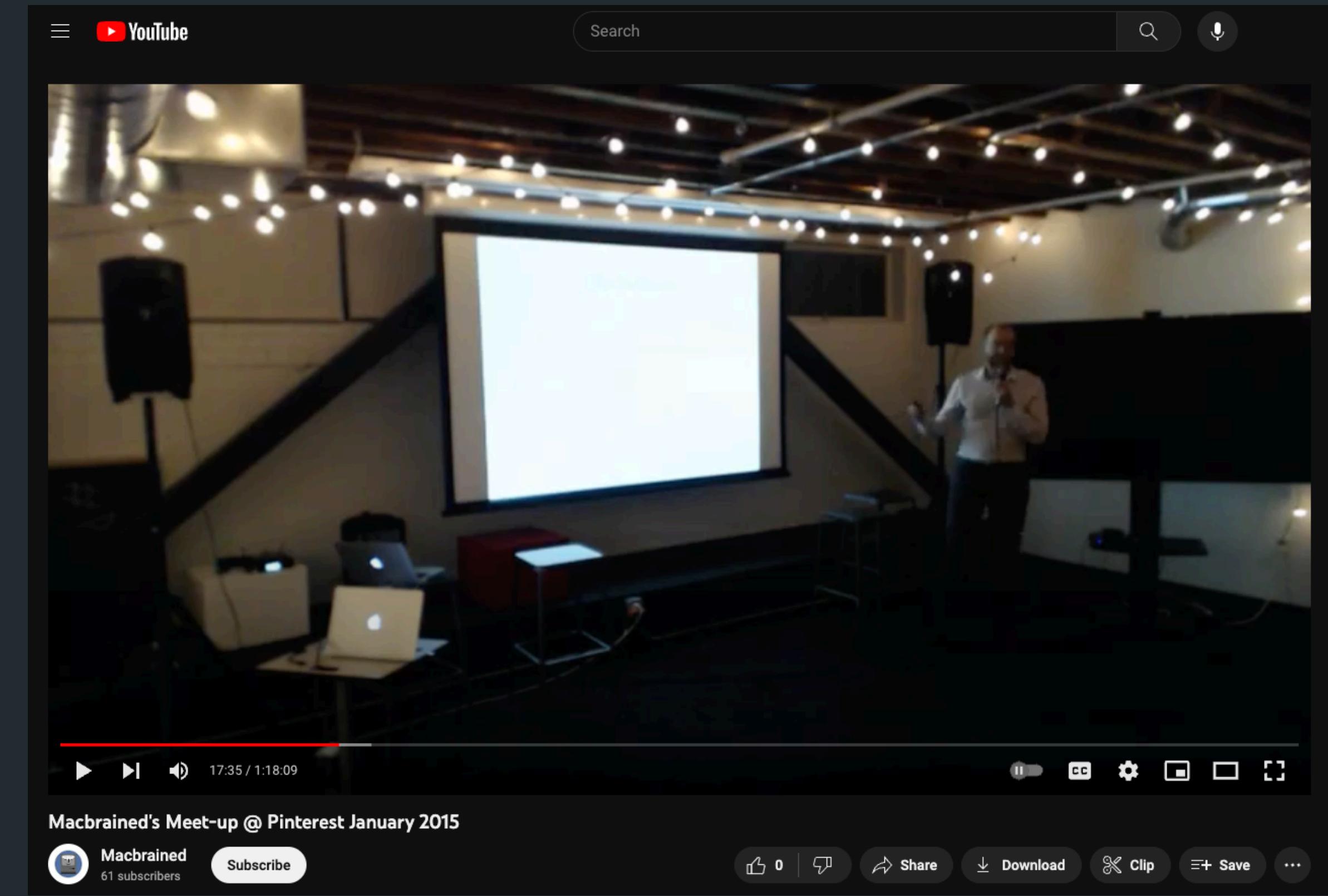
# The old way (stop doing this!)

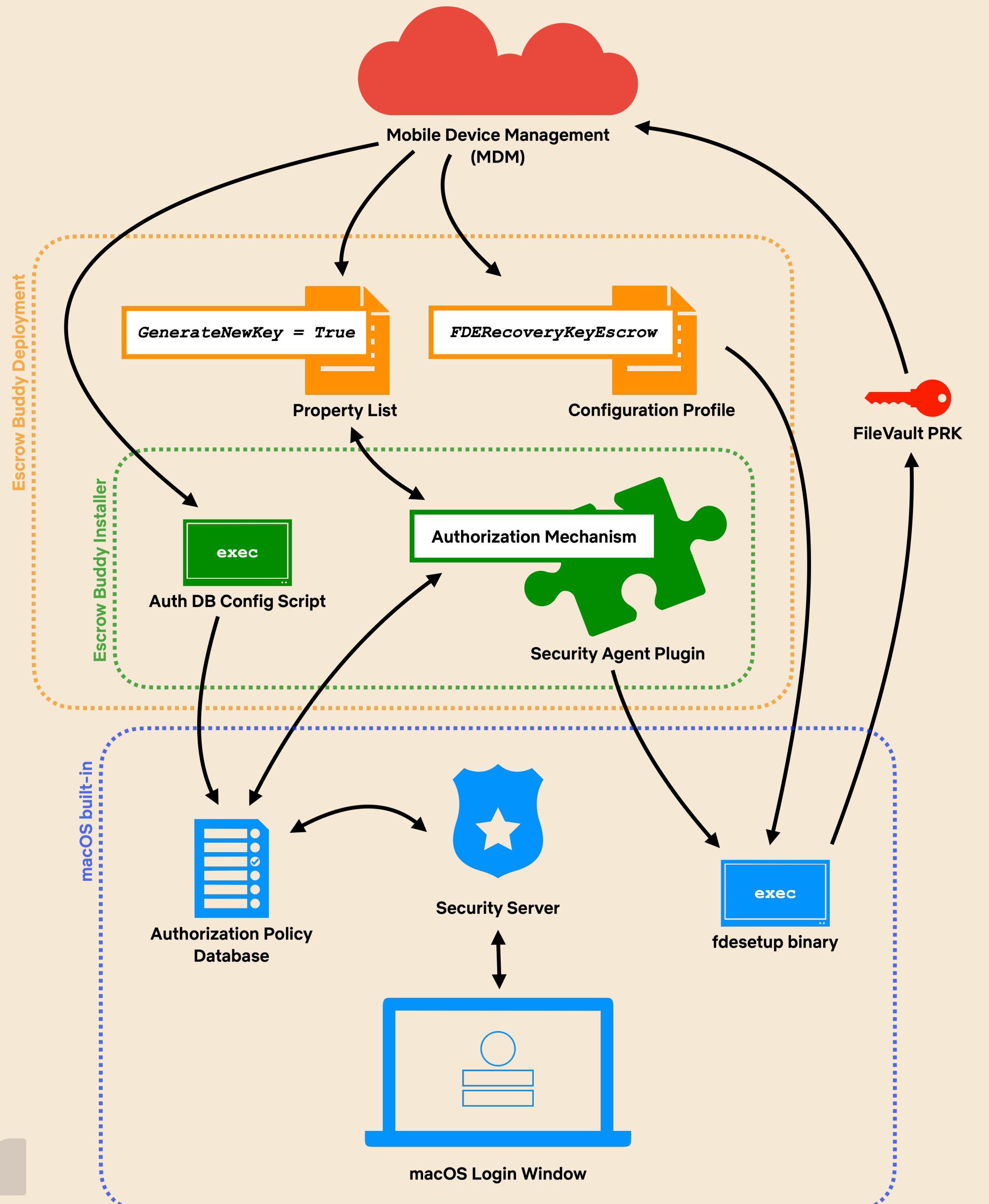
1. Make user aware
2. Prompt for password
3. Trigger **fdesetup**
4. Communicate result



<https://github.com/homebysix/jss-filevault-reissue>

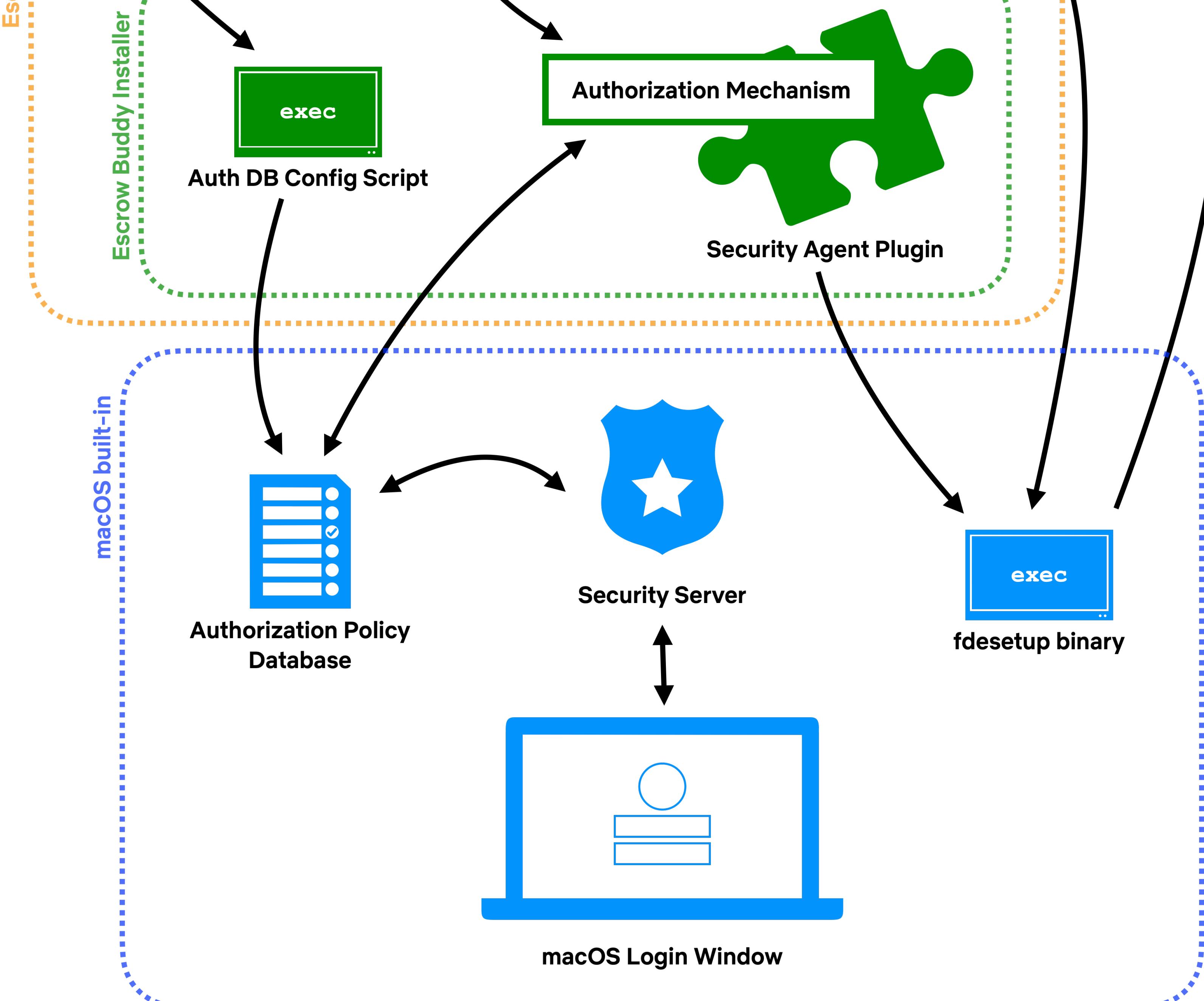
# The new way is better... (take it from the guy who popularized the old way)

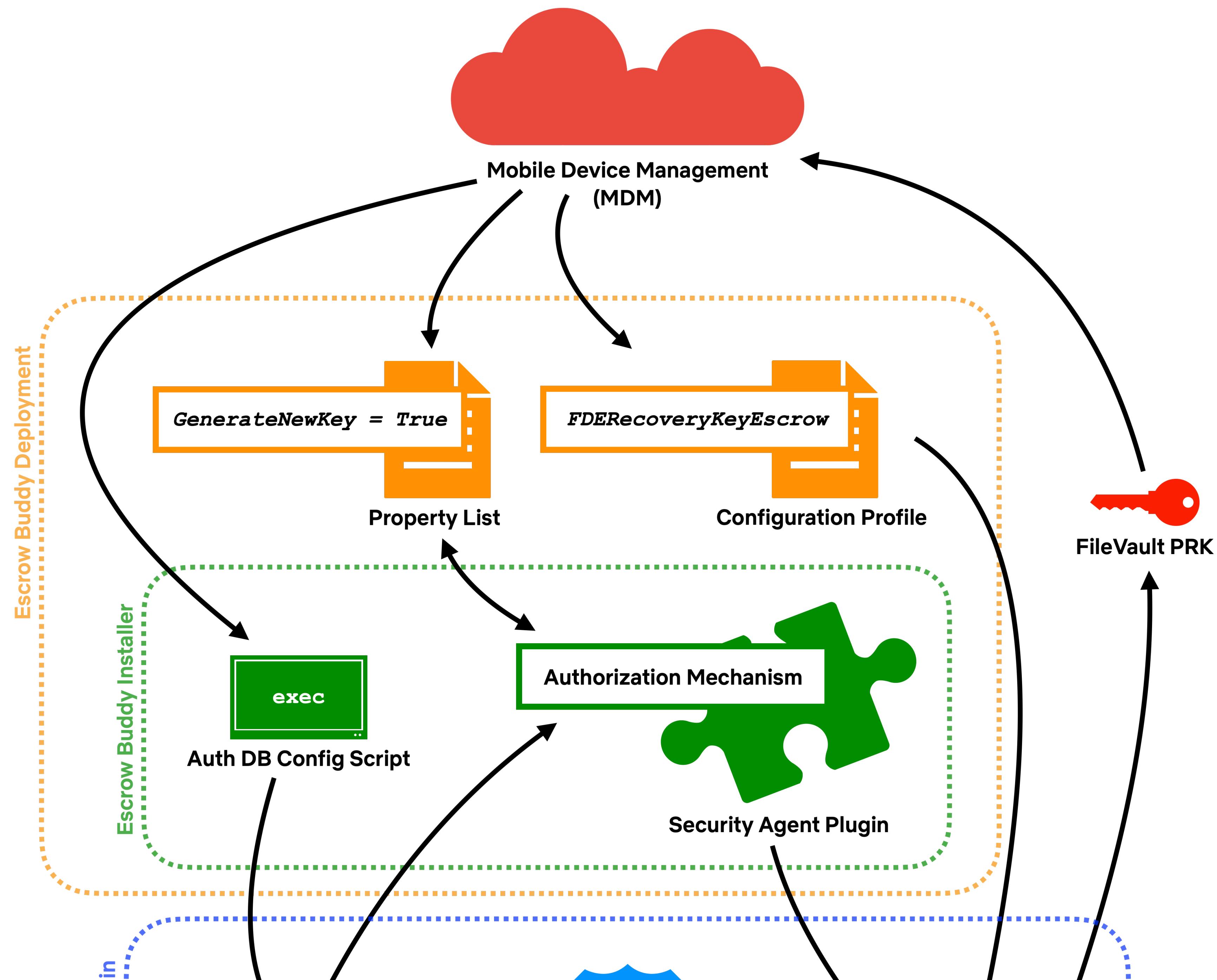




# The new way: authorization plugin

-  Leverages macOS login
-  Secure credential access
-  No additional prompts!





# Crypt did it first

***“Crypt is an authorization plugin that will enforce FileVault 2, and then submit it to an instance of Crypt Server.”***

(Lesser-known feature: standalone regeneration of FileVault keys upon login.)

<https://github.com/grahamgilbert/crypt/>

grahamgilbert / crypt Public

Code Issues 5 Pull requests Actions Projects Wiki Security Insights

crypt / README.md

grahamgilbert This too

Preview Code Blame 105 lines (63 loc) · 5.35 KB

## Crypt

**WARNING:** As this has the potential for stopping users from logging in, extensive testing should take place before production.

Crypt is an authorization plugin that will enforce FileVault 2, and then submit it to an instance of [Crypt Server](#). Crypt 11 and 12. For versions below 11.0, please use version 4.0.0. For versions below 10.12 please use version 2 and below.

Version 3.0.0 now supports 10.12 and above, previous macOS version support has been deprecated!

When using Crypt with macOS 10.15 and higher, you will also need to deploy a PPC TCC profile via user approved MDM. To enable FileVault. [An example can be found here](#).

## Features

- Uses native authorization plugin so FileVault enforcement cannot be skipped.
- Escrow is delayed until there is an active user, so FileVault can be enforced when the Mac is offline.
- Administrators can specify a series of username that should not have to enable FileVault (IT admin, for example).

## Configuration



# Escrow Buddy

makes it simple

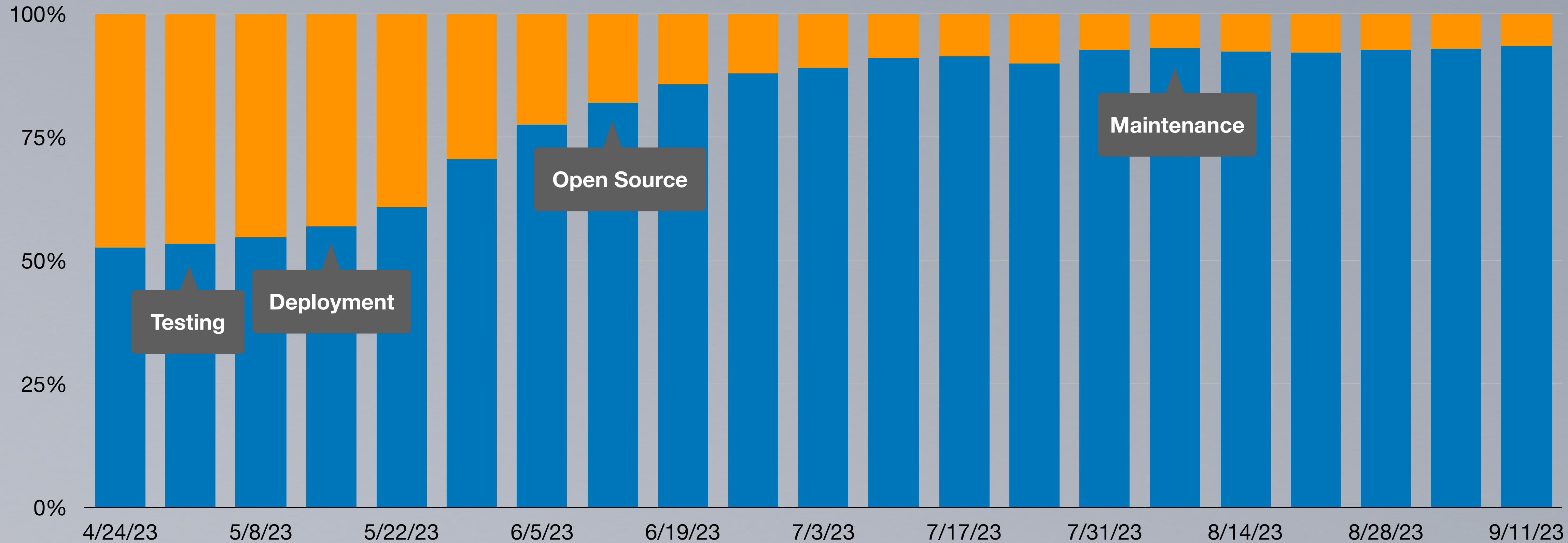
- ✓ Generates new FileVault keys upon login
- ✓ Checks for FDERecoveryEscrow payload
- ✓ Nothing else

<https://github.com/macadmins/escrow-buddy/>



# FileVault Recovery Key Validity

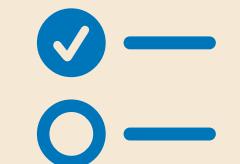
Invalid  
Valid



## Our Success Story



# Basic deployment with Jamf

-  **Package:** Escrow Buddy
-  **Smart Group:** FileVault PRK Missing or Invalid
-  **Policy:** Install and configure Escrow Buddy

**Wiki:** <https://github.com/macadmins/escrow-buddy/wiki/Jamf>

**HCS Guide:** <https://tinyurl.com/2systu46>



# Advanced workflow options

- ⚡ Separate installation/configuration
- ⟳ Recidivism detection
- 🔑 Automatic key rotation
- ❗ Logout notification

<https://github.com/macadmins/escrow-buddy/wiki/Jamf>



# Tips and troubleshooting

-  Reading logs
-  Testing with new macOS versions
-  Tracking success over time
-  Managing authorization database entries

<https://github.com/macadmins/escrow-buddy/wiki/>



# Escrow Buddy

## Usage Survey

When did you begin testing Escrow Buddy?

Date

mm/dd/yyyy

When did you deploy Escrow Buddy to your organization Macs?

Date

mm/dd/yyyy

How many total Macs does your organization manage?

-  Consider submitting our anonymous survey after you deploy
-  Collected data will help us prioritize potential future work

<https://tinyurl.com/eb-usage>



# Mac Admins Open Source

- █ Solving problems broadly
- █ Signed/notarized releases
- █ Community stewardship



<https://youtu.be/REyEYsgz5MI>



# Takeaways



- ☁ Check your FileVault key validity
- 🔑 Consider using Escrow Buddy to remediate
- 🚫 Stop prompting users for their passwords whenever possible

<https://tinyurl.com/JNUC23-EB>



# Thank you for listening!

<https://tinyurl.com/JNUC23-EB>

