

Managing FileVault in macOS Catalina





Frederick Abeloos

Enterprise Support Engineer II

JAMF

JNUC2020

VIRTUAL CONFERENCE



2020

JNUC

VIRTUAL

CONFERENCE

2020



Frederick Abeloos

Enterprise Support Engineer II

JAMF



TRAVELLING TECH GUY

macOS and iOS management with a twist of Jamf (less travel, a lot more tech)

2020



JNUC

VIRTUAL

CONFERENCE

20
02

Managing FileVault in macOS Catalina

Presentation agenda:

Terminology

SecureToken Flows

Remotely enforcing FileVault

Recovery Keys

Troubleshooting and fixes

20
02

JNUC

VIRTUAL

CONFERENCE

20
02

Terminology

FileVault

SecureToken

BootstrapToken

“Managed Administrator”

Deferred enablement

Recovery Keys

20
02





FileVault

Introduced in Mac OS X 10.3 Panther

Initially only the user's home folder

FileVault 2 introduced in Mac OS X 10.7 Lion

Full startup disk encryption

Further changes:

Mac OS X 10.13 High Sierra: SecureToken

Mac OS X 10.15 Catalina: BootstrapToken





SecureToken

Wrapped version of a Key Encryption Key (KEK) protected by a user's password.

Basically an attribute linked to a user's account to allow it to interact with FileVault

FileVault enabled user = SecureToken enabled user





BootstrapToken

Introduced in macOS Catalina to facilitate the management of FileVault and FileVault enabled users (SecureToken users)

Mainly due to the need of most MacAdmins to have a local administrator with SecureToken, to be able to interact with FileVault when needed.

A special token, generated via MDM enrolment, adding the ability to automatically generate a SecureToken for the 'Managed Administrator' or Mobile Accounts





Managed Administrator

When using Automated MDM enrolment, and downgrading the end user to 'standard' privileges, or skipping user creation entirely, Apple MDM specifications require the creation of an Admin account via MDM.

= 'The Managed Admin'

!= 'The Jamf Management Account'

“Administrator account created by MDM during Automated MDM enrolment (DEP)”



Managed Administrator

Computers : PreStage Enrollments
< Standard

Options
Scope
MANAGED ADMINISTRATOR

General
Account Settings >
Configuration Profiles 0 Profiles
User and Location
Purchasing
Attachments 0 Attachments
Certificates
Enrollment Packages 0 Packages

Account Settings

☒ Create a local administrator account before the Setup Assistant
Local administrator account to create before the Setup Assistant for computers enrolled with this PreStage enrollment

Username
jamfadmin

Password
.....

Verify Password
.....

☐ Hide managed administrator account in Users & Groups

Local User Account Type

Type of user account to create during enrollment

☐ Administrator Account
Make the user an administrator for the computer

☒ Standard Account
Make the user a standard user on the computer

☐ Skip Account Creation
The user will not create a local user account

☐ Pre-fill primary account information

JNUC

VIRTUAL

CONFERENCE

2020



Jamf Management Account

jamf | PRO

Full Jamf Pro

ComputersDevicesUsers

VERSION
10.23.0-t1595614145

MANAGED
Computers: 1
Mobile Devices: 2

UNMANAGED
Computers: 0
Mobile Devices: 0

Settings : Global Management

← User-Initiated Enrollment

GeneralMessagingPlatformsAccess

macOSiOS

☒ Enable user-initiated enrollment for computers
Allow users to enroll computers by going to <https://jamf.mycompany.com:8443/enroll>

Management Account

Account to use for managing computers enrolled by user-initiated enrollment

Username
jamfadmin

Method For Setting Password
Method to use for setting the management account password. If randomly generating passwords, a unique password is created for each computer.
Specify password
⚠ For maximum security, it is recommended that you choose the "Randomly generate new password" option.

Password
.....

Verify Password
.....

☒ Create management account
Create the management account during enrollment if it does not already exist

☒ Hide management account
Hide the management account from users



2020



Deferred enablement

When remotely enabling / enforcing FileVault

Jamf Pro Policy

MDM Configuration Profile

Enabling FileVault (~ SecureToken) requires authentication
(password)

“Delayed enablement” => to allow authentication





Recovery keys

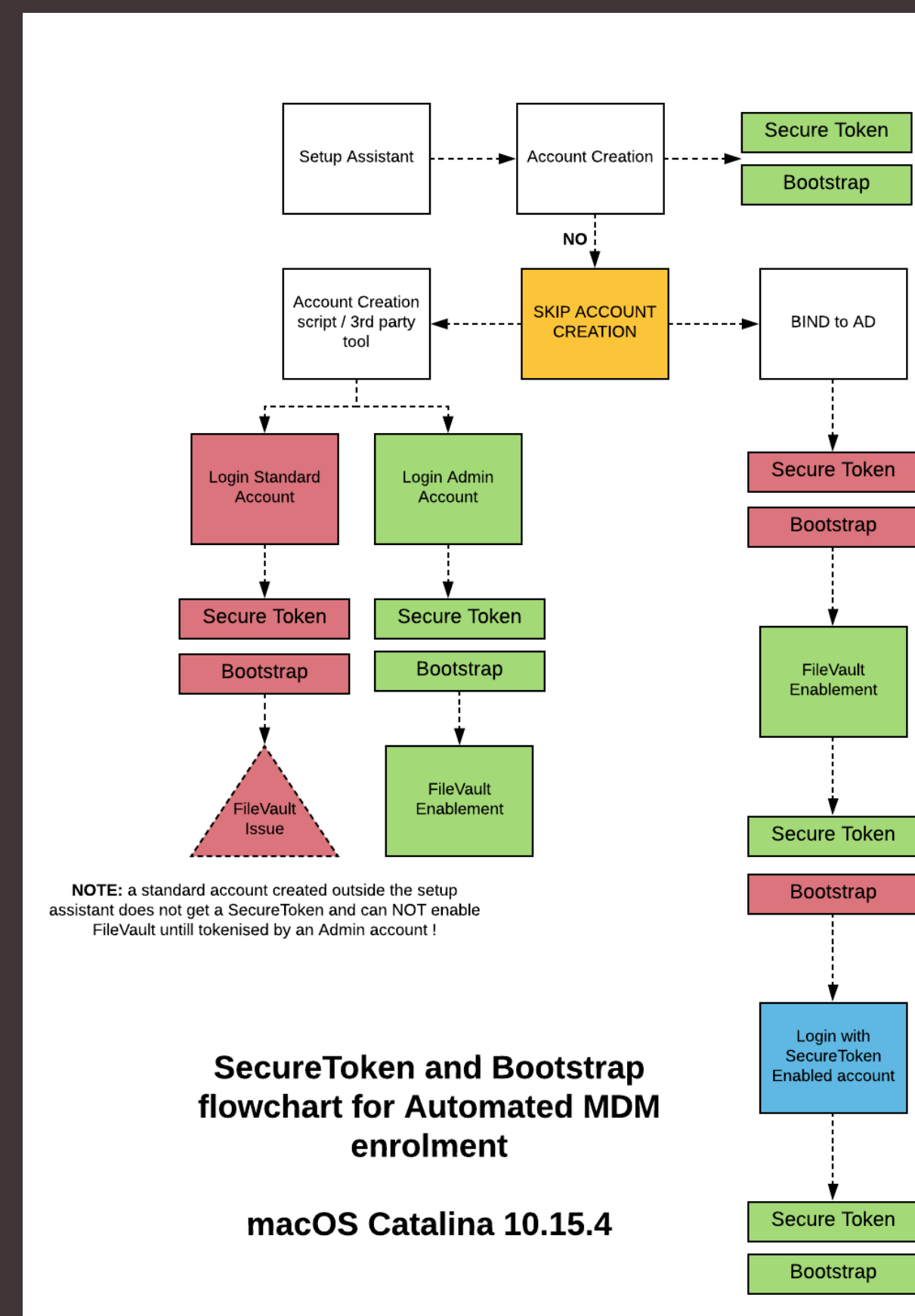
- iCloud recovery for FileVault (Apple ID)
- Personal Recovery Key
 - PseudoRandom (120 Bit) code
 - Automatically generated
 - XXXX-XXXX-XXXX-XXXX-XXXX-XXXX
- Institutional Recovery Key
 - Keychain
 - Public Key (certificate)
 - Private Key



SecureToken Flows

User Initiated Enrolment

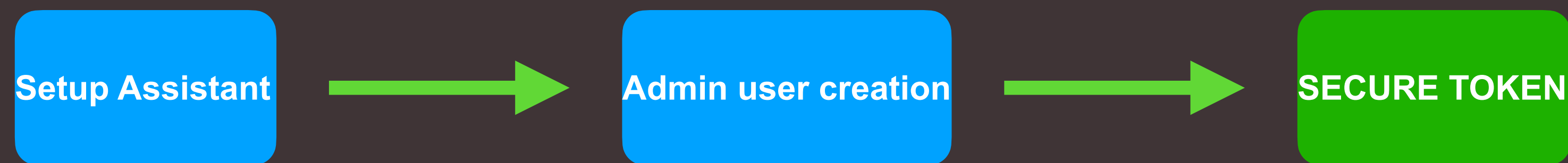
Automated MDM Enrolment





User Initiated Enrolment

No MDM involved during initial setup



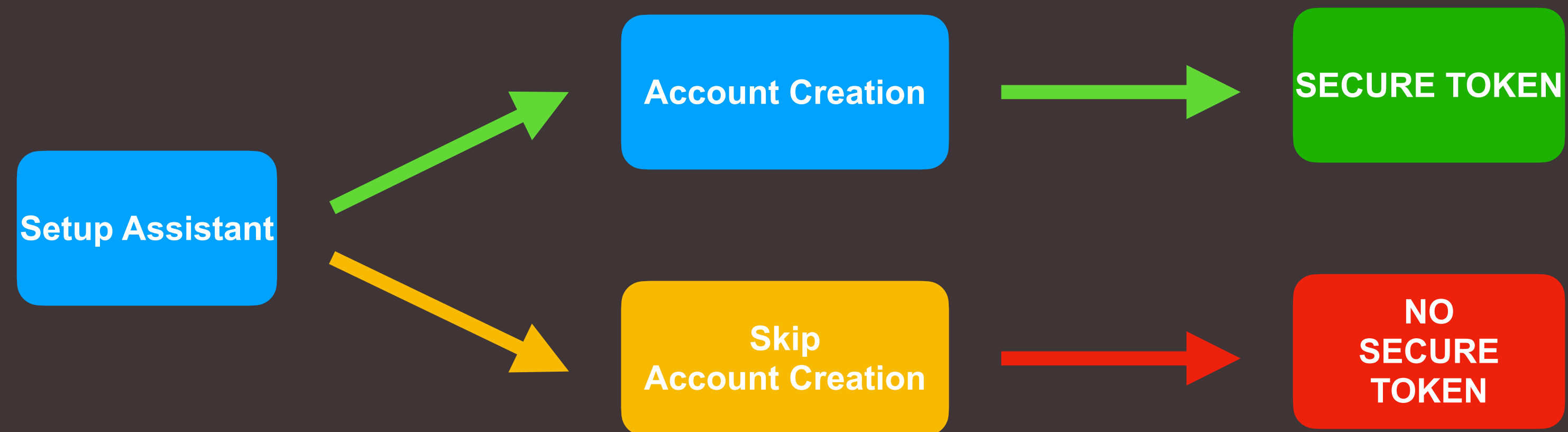
UIE enrolment has NO impact or influence on SecureToken
Jamf Pro Management Account does NOT get a SecureToken



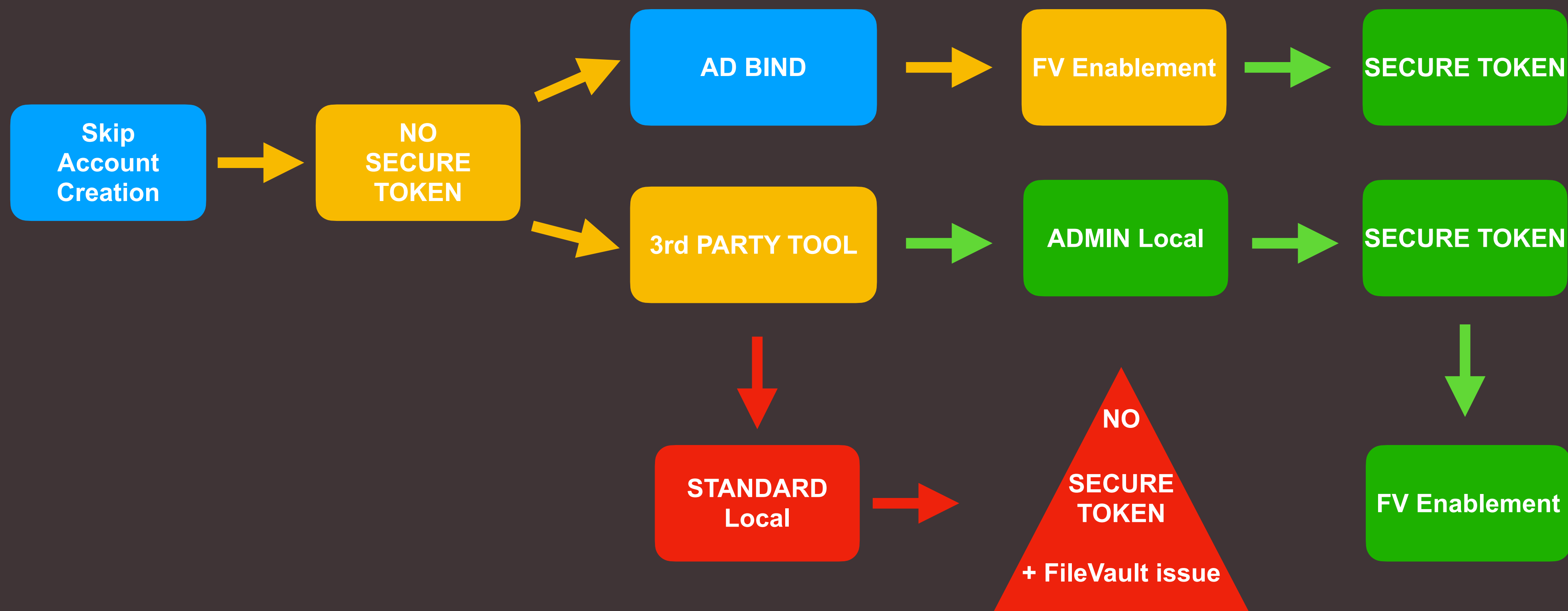
Automated MDM Enrolment

Account Creation

Skip account creation



Skip Account Creation



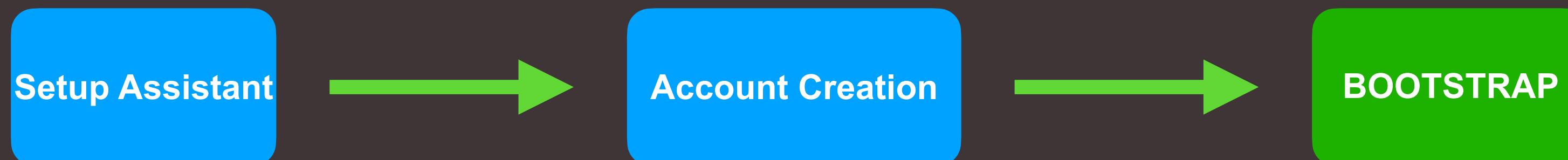


BootstrapToken

Apple Business / School Manager

“Managed Administrator” / Mobile Accounts

=> Automated MDM Enrolment



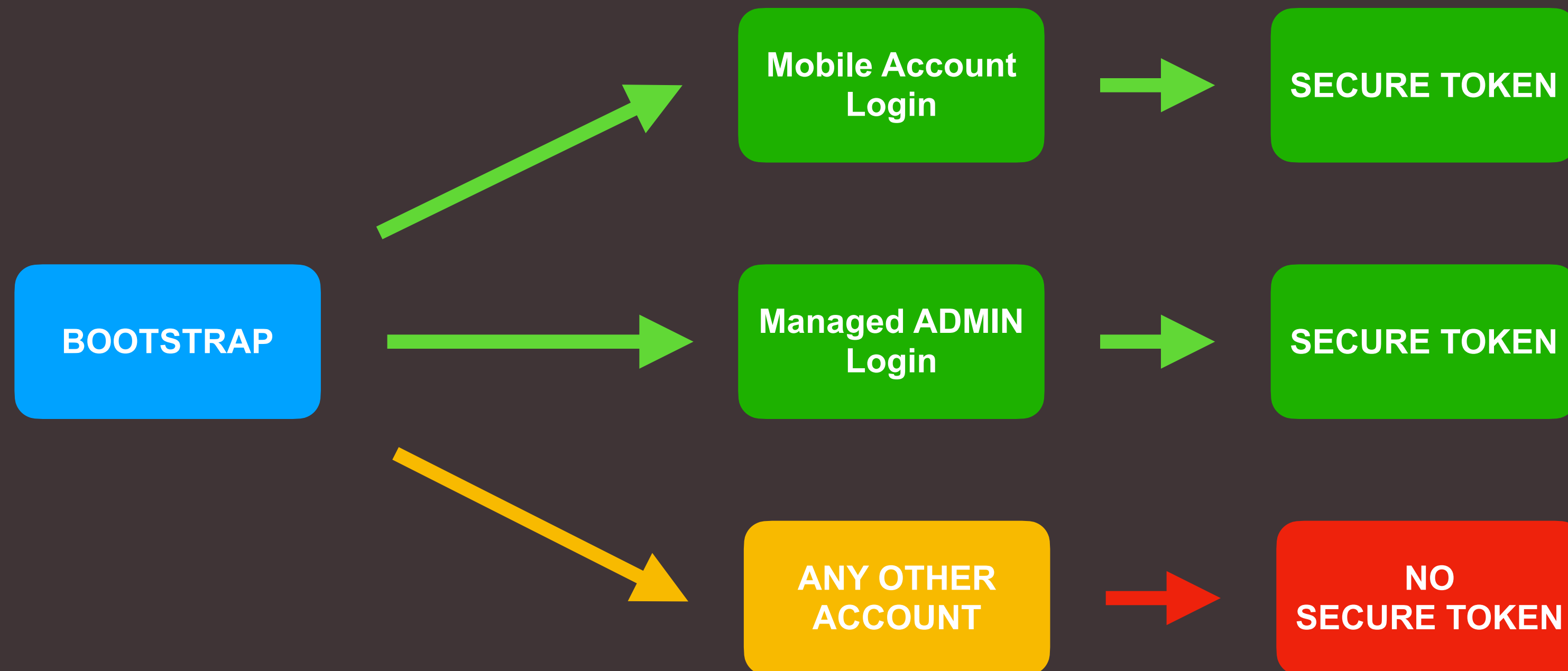


Automated MDM with skip account creation

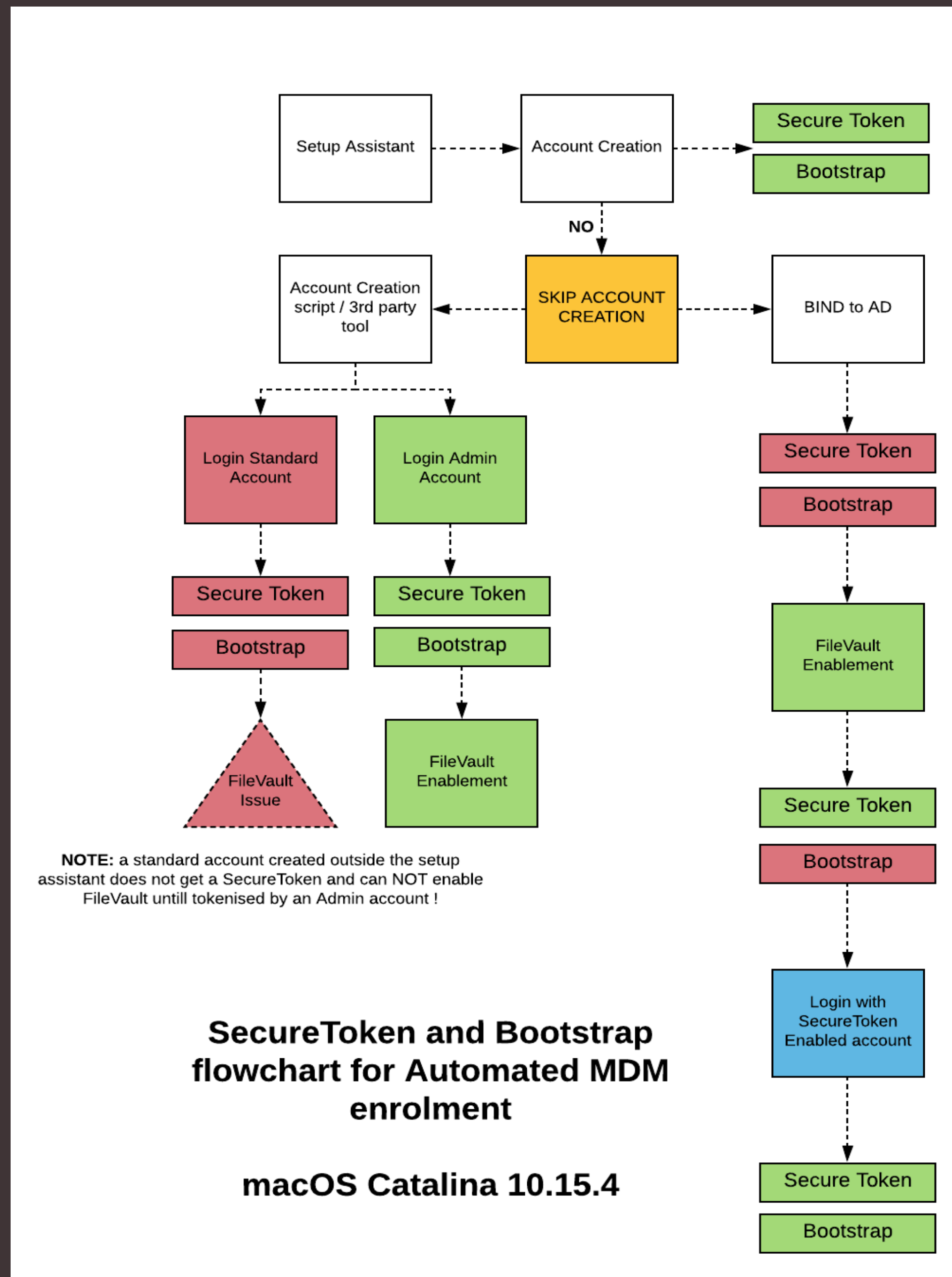




SecureToken generation via Bootstrap



Overview



JNUC

VIRTUAL

CONFERENCE

20
02

Remotely enabling/enforcing FileVault

Configuration profile

Jamf Pro Policy

Jamf Connect Login



20
02

Configuration profile (High Sierra and Later)

Computers : Configuration Profiles

← FileVault

FV Enabled @ Logout

Options

Scope

☐ Show in Jamf Pro Dashboard

General

Security and Privacy
1 payload configured

Security & Privacy

General

FileVault

Firewall

Privacy

☒ Require FileVault 2
If not already enabled, FileVault 2 will be enabled at the next logout

☐ Use institutional recovery key
Enables access to the FileVault 2-encrypted drive using an institutional recovery keychain

☒ Create individual recovery key
Create an individual recovery key. To store the individual recovery key in Jamf Pro, you must also configure the FileVault Recovery Key Redirection payload

☐ Require user to unlock FileVault 2 after hibernation
The user will be required to unlock FileVault 2 when the computer awakes from hibernation

☒ Enable Escrow Personal Recovery Key (macOS 10.13 or later)
When enabled, the device will encrypt the personal recovery key with the provided certificate and report it to Jamf Pro. The encrypted key can be downloaded from the computer's Inventory tab.

Escrow Location Description
Short description of where the personal recovery key will be escrowed. This message will be presented to the user when enabling FileVault.

PRK will be stored in Jamf Pro



Configuration profile (pre - High Sierra)

2020

Computers : Configuration Profiles

← FileVault

Options Scope ☐ Show in Jamf Pro Dashboard

General

Certificate
Payloads configured: 2

Security and Privacy
1 payload configured

FileVault Recovery Key
Redirection
1 payload configured

FileVault Recovery Key Redirection

Recovery Key Redirection Method to use for specifying the URL to which the recovery keys should be sent

Automatically redirect recovery keys to the Jamf Pro server ▼

2020



Jamf Pro Policy



Settings : Computer Management > Disk Encryption Configurations

← **INST**

Display Name Display name for the disk encryption configuration

FileVault

Recovery Key Type Recovery key to use for the disk encryption configuration

- Individual
- ✓ Institutional
- Individual And Institutional

Institutional Recovery Key Recovery key file for the institutional recovery key (.p12, .cer, or .pem)

OID.2.5.4.13=Fredericks-MacBook-Pro.local, CN=FileVault Recovery Key

Upload Institutional Recovery Key

Enabled FileVault 2 User User to enable for FileVault 2

Current or Next User ▼

Jamf Pro Policy

Computers : Policies

← FileVault

Options Scope Self Service User Interaction

 General

 Disk Encryption
IND >

 Restart Options
Configured

Disk Encryption

Action Action to take on computers

Apply Disk Encryption Configuration ▼

Disk Encryption Configuration Disk encryption configuration to use to enable FileVault 2

IND ▼

Require FileVault 2 Require users to enable FileVault 2 based on one of the following events

At next login ▼

Jamf Connect Login

Key	Description	Example
EnableFDE	Enable FileVault If set to true, FileVault will be enabled for the first user that logs in to a computer.	<pre><key>EnableFDE</key> <false/></pre>
EnableFDERecoveryKey	Save FileVault Recovery Key If set to true, Jamf Connect will store the FileVault recovery key to /var/db/NoMADFDE unless otherwise specified.	<pre><key>EnableFDERecoveryKey</key> <false/></pre>
EnableFDERecoveryKeyPath	Set Recovery Key Filepath Specifies a custom file path for the FileVault recovery key	<pre><key>EnableFDERecoveryKeyPath</key> <string>/usr/local/filevault</string></pre>
LAPSUser	LAPS User An existing local administrator account, of which Jamf Connect can change the password to the personal recovery key. This setting is only used by Jamf Connect to help enable FileVault on standard accounts on macOS 10.15 or later.	<pre><key>LAPSUser</key> <string>AdminUser</string></pre>



Jamf Connect Login

- Local Admin Password Solution (LAPS)

```
<key>LAPSUser</key>  
<string>AdminUser</string>
```

Watch out with Passcode policies in Configuration Profiles!

(Standard Account creation only)

Jamf Connect Login

- Local Admin Password Solution (LAPS)

```
<dict>
  <key>SystemPolicyAllFiles</key>
  <array>
    <dict>
      <key>Allowed</key>
      <true/>
      <key>CodeRequirement</key>
      <string>identifier "com.apple.authorizationhost" and anchor apple</string>
      <key>Comment</key>
      <string></string>
      <key>Identifier</key>
      <string>com.apple.authorizationhost</string>
      <key>IdentifierType</key>
      <string>bundleID</string>
      <key>StaticCode</key>
      <false/>
    </dict>
  </array>
</dict>
```

JNUC

Recovery Keys

VIRTUAL

Personal Recovery Key

Institutional Recovery Key

CONFERENCE

20
02

20
02



Personal Recovery Key

Computers

← MacBook Air

Inventory

Management

History

General

MacBook Air

Hardware

MacBook Air (11-inch Early 2015)

Operating System

Mac OS X 10.15.3

User and Location

adm_user@travellingtechguy.dev

Security

Purchasing

Storage

1 Drive

Extension Attributes

Disk Encryption

Encrypted

Applications

54 Applications

Disk Encryption

Name: Macintosh HD (Boot Partition)

Last Inventory Update: Less than a minute ago

FileVault 2 Partition Encryption State: Encrypted

Individual Recovery Key Validation: Valid

Individual Recovery Key: QKW7-JTWM-A774-QPQD-GEX9-AKW9

Device Recovery Key: C02S80M1GFWK

Institutional Recovery Key Status: Not Present

Disk Encryption Configuration:

FileVault 2 Enabled Users: jamfadmin, test

History

Autorun Data

Delete

2020

© copyright 2002-2020 Jamf



Institutional Recovery Key

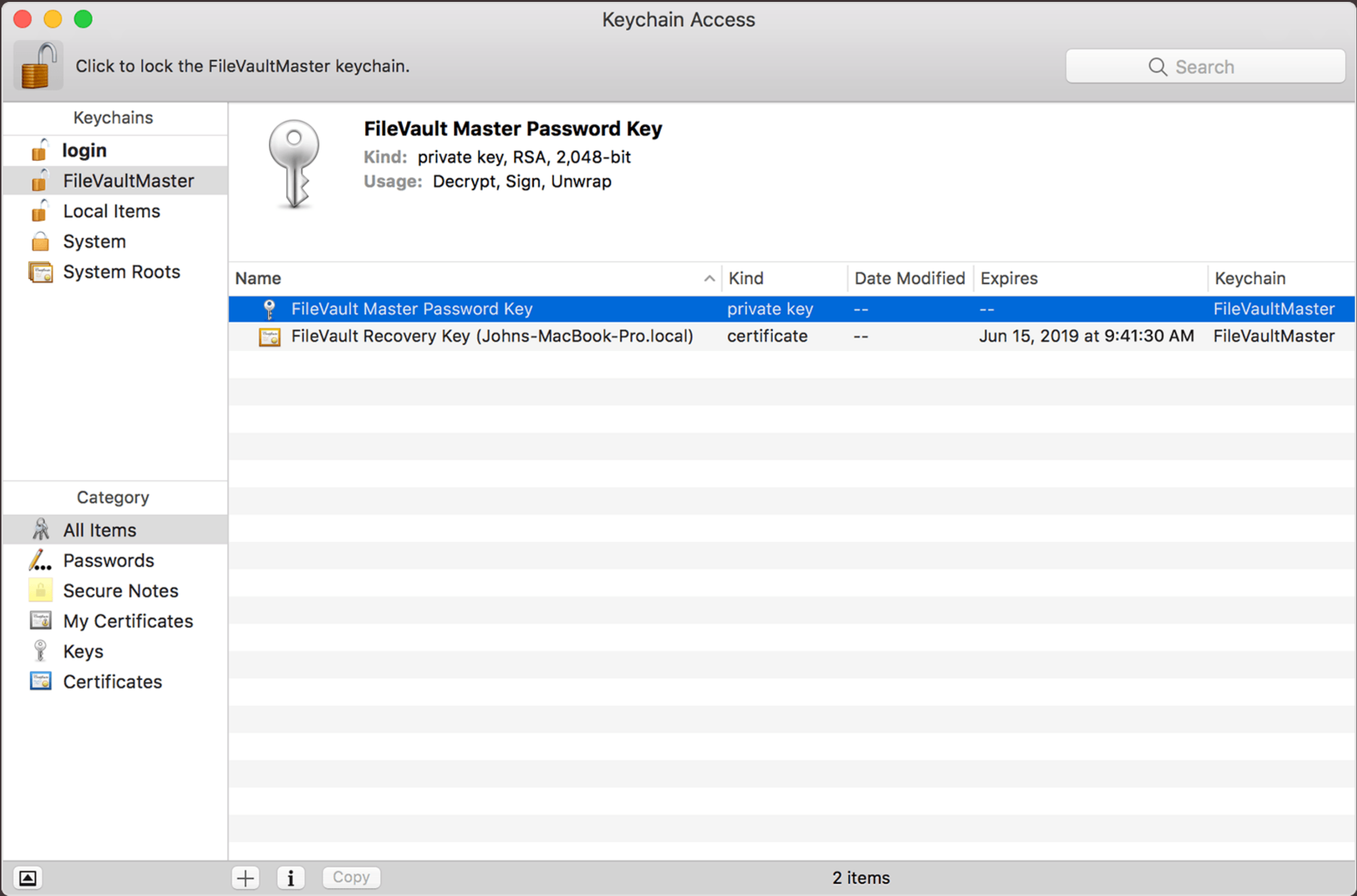
```
security create-filevaultmaster-keychain ~/Desktop/FileVaultMaster.keychain
```

You can export the recovery key with or without the private key. Exporting with the private key allows you to store it in Jamf Pro. If you export without the private key, you must store it in a secure location so you can access it when needed.

You **cannot** use an institutional recovery key with a private key to activate FileVault Disk Encryption using a configuration profile in Jamf Pro. You must create and deploy the disk encryption configuration using a policy in Jamf Pro.



Institutional Recovery Key



Upload Institutional Recovery Key

Settings : Computer Management > Disk Encryption Configurations

← **INST**

Display Name Display name for the disk encryption configuration

FileVault

Recovery Key Type Recovery key to use for the disk encryption configuration

- Individual
- ✓ Institutional
- Individual And Institutional

Institutional Recovery Key Recovery key file for the institutional recovery key (.p12, .cer, or .pem)

OID.2.5.4.13=Fredericks-MacBook-Pro.local, CN=FileVault Recovery Key

Upload Institutional Recovery Key

Enabled FileVault 2 User User to enable for FileVault 2

Current or Next User ▼



Troubleshooting & Fixes

Identifying SecureToken holders

Deferred enablement related issues

Validating Recovery Key

Renewing Recovery Keys

Validating / Enabling Bootstrap

Scripting Secure Token





Identifying SecureToken holders

```
diskutil apfs listusers /
```

```
(diskutil apfs listcryptousers /)
```

```
Cryptographic users for disk1s5 (4 found)
|
+-- FB756838-82AC-4C28-8FA0-40FB5E7D5D3F
|   Type: Local Open Directory User
|
+-- EBC6C064-0000-11AA-AA11-00306543ECAC
|   Type: Personal Recovery User
|
+-- C22BDCD3-11DE-422F-9C4C-65D3332605C3
|   Type: Local Open Directory User
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
|   Type: MDM Bootstrap Token External Key
```



Identifying SecureToken holders

```
sudo fdesetup list -extended
```

```
ESCROW  UUID                                TYPE  USER
        FB756838-82AC-4C28-8FA0-40FB5E7D5D3F      OS User frederick.abeloos
        EBC6C064-0000-11AA-AA11-00306543ECAC      Personal Recovery Record
        C22BDCD3-11DE-422F-9C4C-65D3332605C3      OS User ttg
        2457711A-523C-4604-B75A-F48A571D5036      Bootstrap Token
```





Identifying SecureToken holders

```
sysadminctl -adminUser <username> -adminPassword  
<password> -secureTokenStatus ttg
```

```
2020-08-03 23:46:41.454 sysadminctl[20009:609662] Secure  
token is ENABLED for user Travelling Techguy
```

Deferred enablement related issues

fdsetup status

FileVault is ON/OFF

“Deferred enablement appears to be active for user ‘username’”

Deferred enablement related issues

Unscope FileVault Config Profile / Policy

```
sudo fdsetup disable
```

+REBOOT

Validating Recovery Key

```
fdsetup haspersonalrecoverykey
```

```
fdsetup hasinstitutionalrecoverykey
```

```
sudo fdsetup validaterecovery
```

Renewing Recovery Key

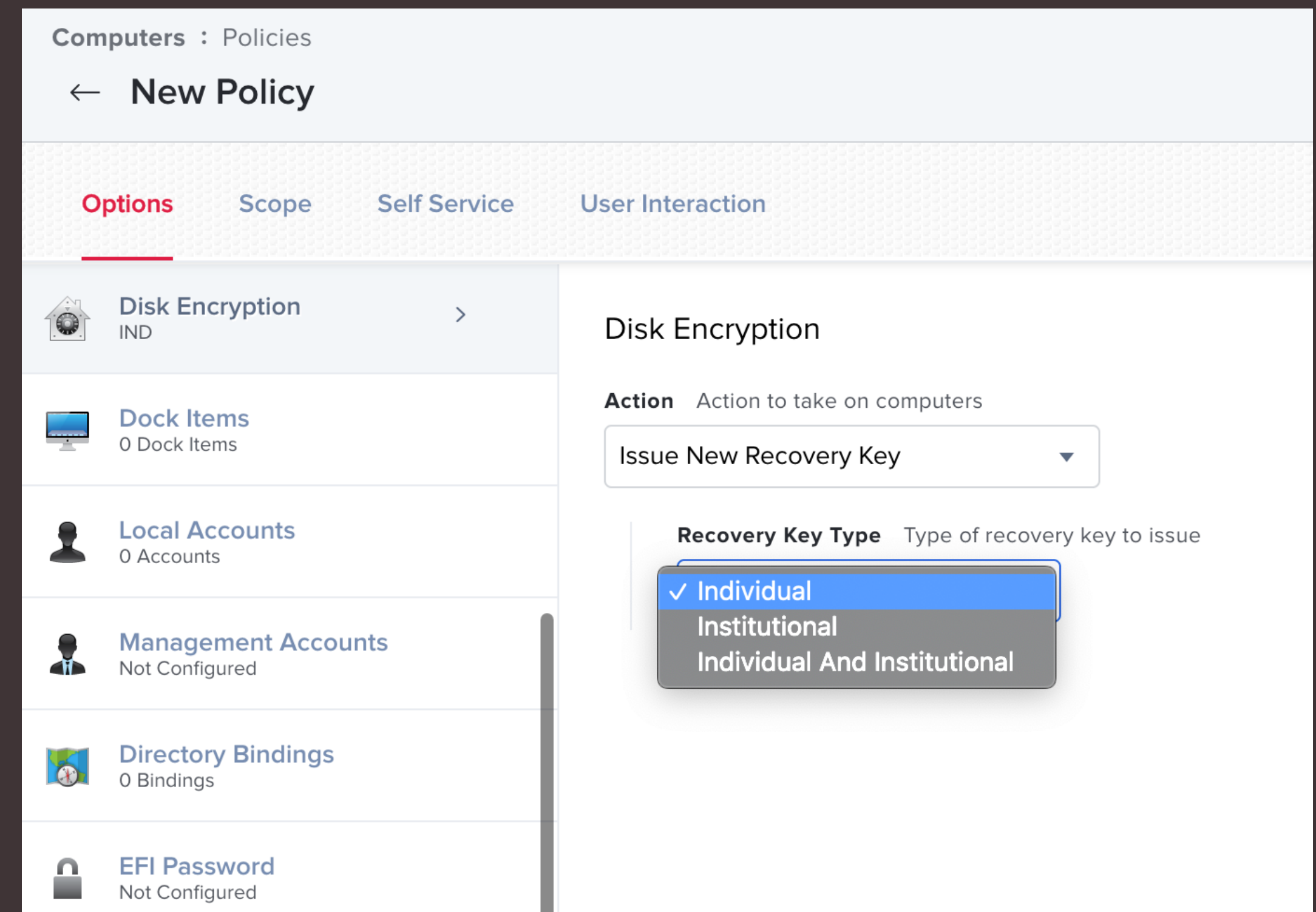
macOS 10.14 or later

A “Recovery HD” partition

FileVault activated

One of the following two conditions met:

- The management account with a SecureToken
- An existing, valid individual recovery key (Personal Recovery Key only)



Renewing Personal Recovery Key

```
fdsetup changerecovery -personal
```

(script)

! Make sure to have escrow in place !

JNUC

VIRTUAL

CONFERENCE

20
02

Renewing Institutional Recovery Key

```
fdsetup changerecovery -institutional -keychain  
-certificate /path/to/filename.cer
```

20
02





Validating / Enabling Bootstrap

```
sudo profiles status -type bootstraptoken
```

Profiles: Bootstrap Token supported on Server YES/NO

Profiles: Bootstrap Token escrowed to Server YES/NO

Validating / Enabling Bootstrap

```
sudo profiles install -type bootstraptoken
```

```
sudo profiles remove -type bootstraptoken
```





Scripting SecureToken

```
sysadminctl -adminUser $addAdminUser  
-adminPassword $addAdminUserPassword  
-secureTokenOn $userName -password $userPass
```

Both username/password of a SecureToken-enabled ADMIN and the targeted username are required!



Anticipated changes in future macOS versions

To be confirmed



JNUC

VIRTUAL

CONFERENCE

2020

JNUC

Ressources

VIRTUAL

CONFERENCE

20
20

jamf.it/FVJNUC2020

20
20



Thank you for listening!

Give us feedback by completing the
survey using the widget below

JNUC2020
VIRTUAL CONFERENCE



20
20