Managing FileVault in macOS Catalina

© copyright 2002-2020 Jamf

Frederick Abeloos

Enterprise Support Engineer II

JAMF

JNUC2020

VIRTUAL CONFERENCE

© copyright 2002-2020 Jamf

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)

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Managing FileVault in macOS Catalina

Presentation agenda:

- Terminology
- SecureToken Flows
- Remotely enforcing FileVault
- Recovery Keys
- Troubleshooting and fixes

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Terminology

FileVault

SecureToken

BootstrapToken

“Managed Administrator”

Deferred enablement

Recovery Keys

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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 Aministrator’ or Mobile Accounts

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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)”

© copyright 2002-2020 Jamf

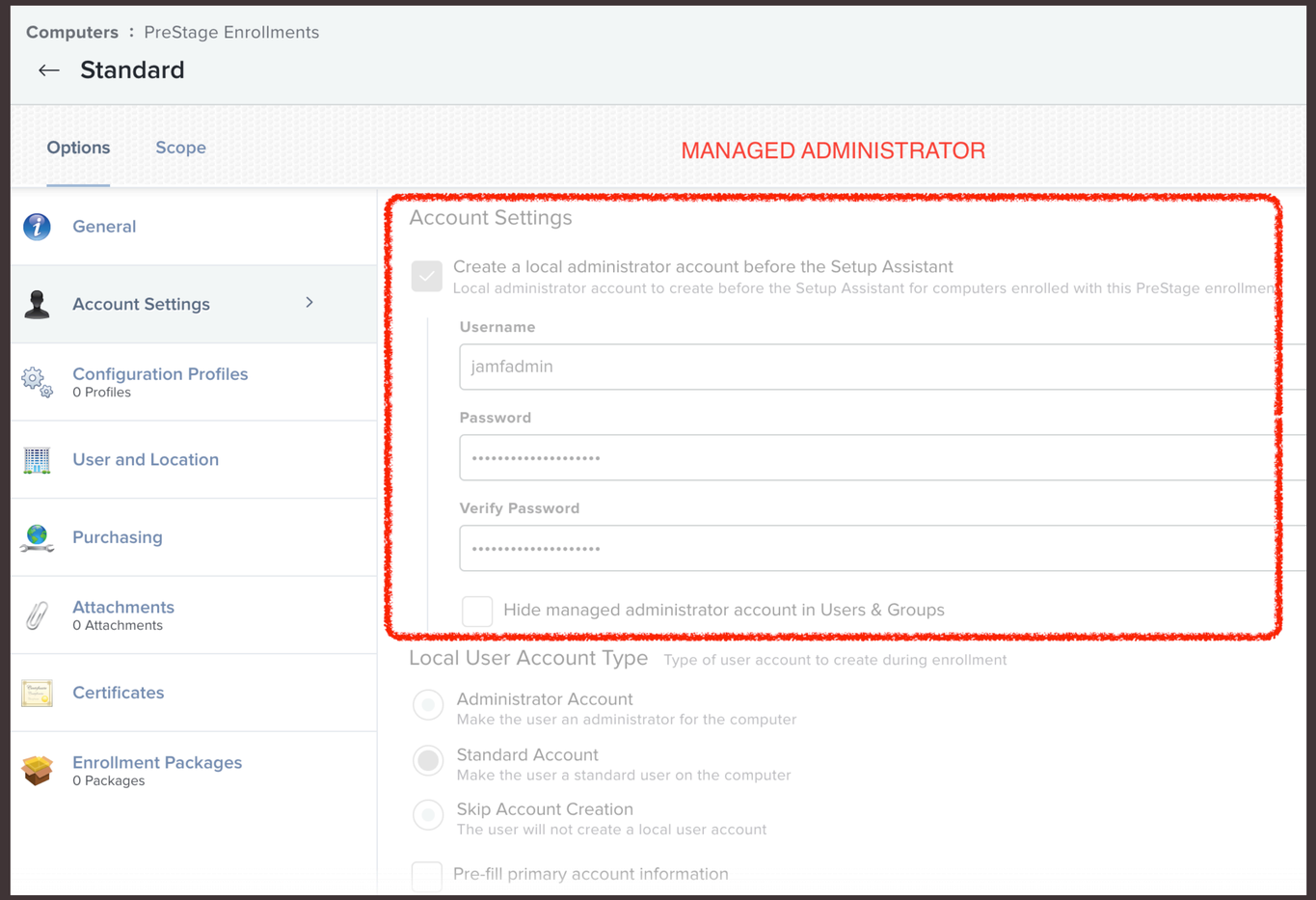
JNUC

VIRTUAL

CONFERENCE

2020

Managed Administrator



© copyright 2002-2020 Jamf

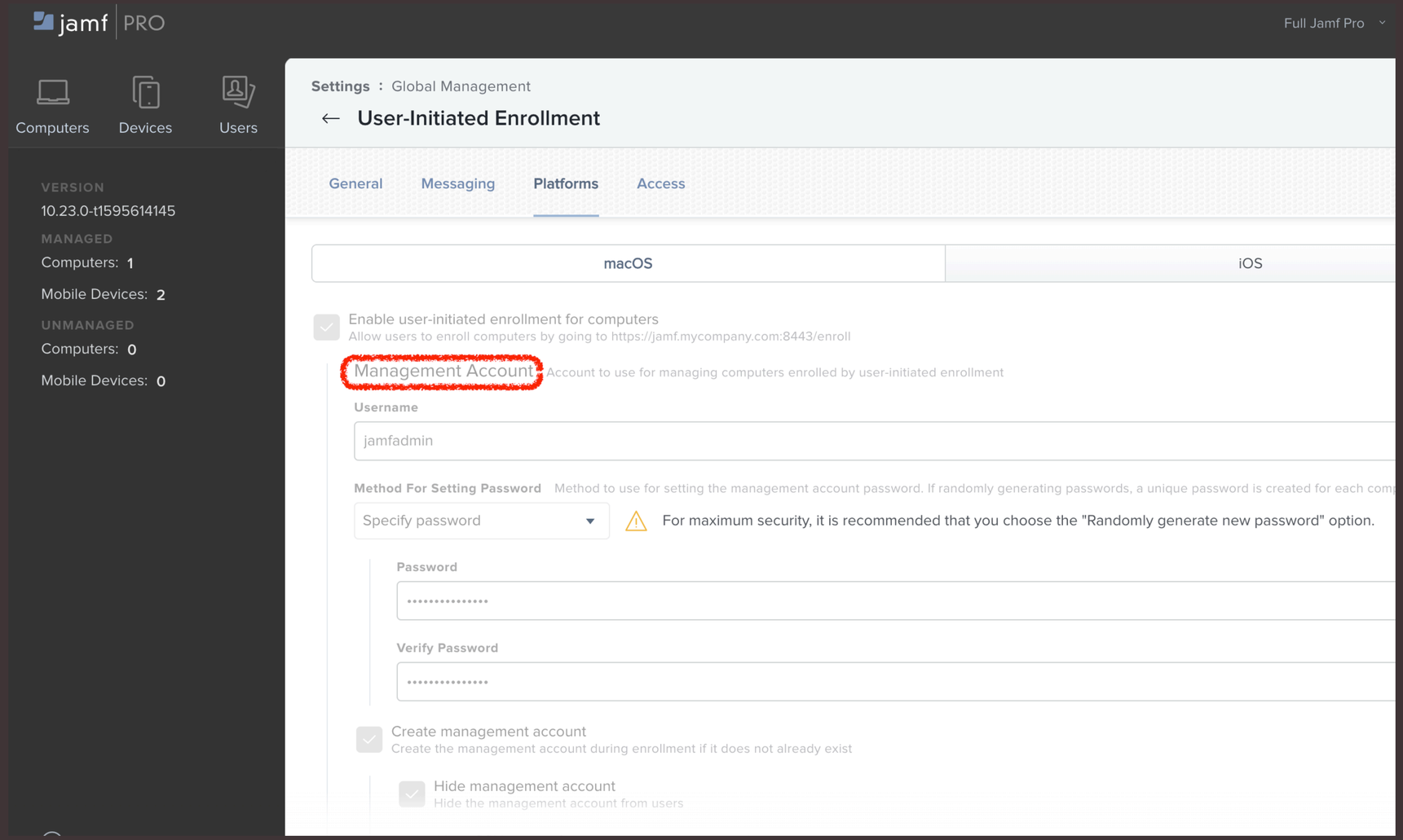
JNUC

VIRTUAL

CONFERENCE

2020

Jamf Management Account



© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Deferred enablement

When remotely enabling / enforcing FileVault

- Jamf Pro Policy
- MDM Configuration Profile

Enabling FileVault (~ SecureToken) requires authentication (password)

“Delayed enablement” => to allow authentication

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

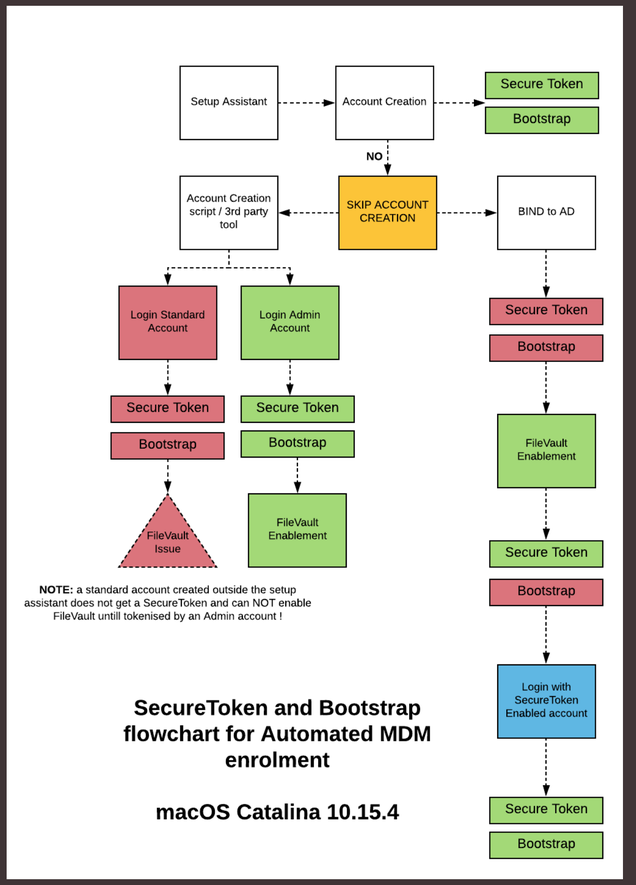
2020

jamf

SecureToken Flows

User Initiated Enrolment

Automated MDM Enrolment



2020

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

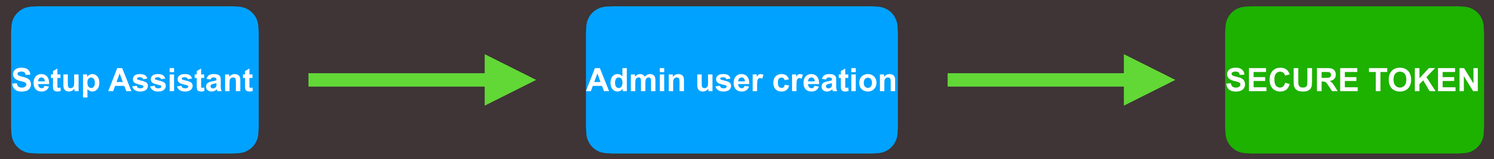
CONFERENCE

2020

jamf

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

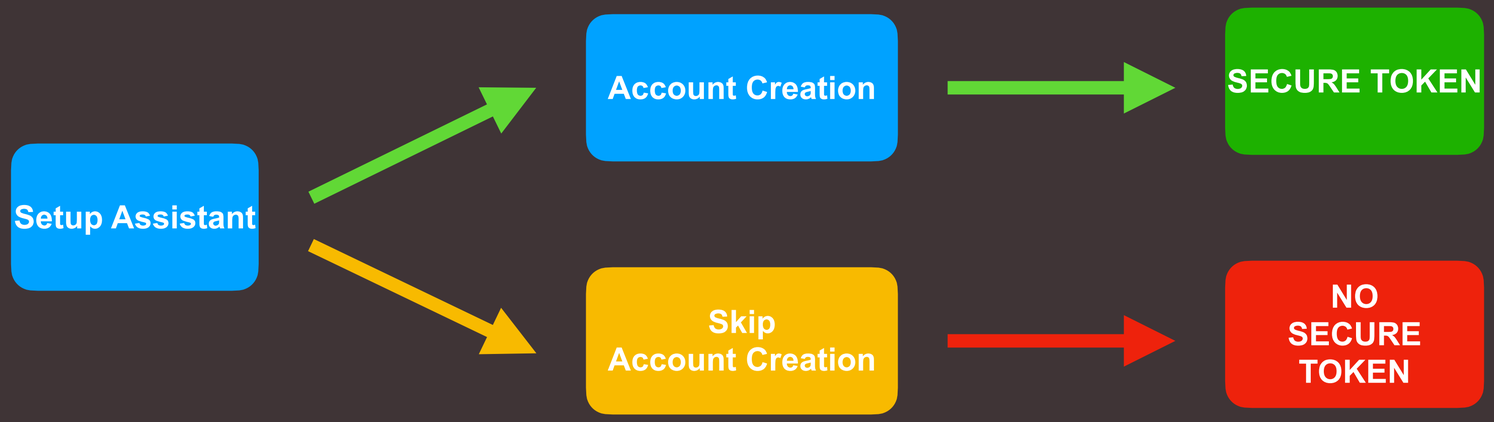
2020

jamf

Automated MDM Enrolment

Account Creation

Skip account creation



© copyright 2002-2020 Jamf

JNUC

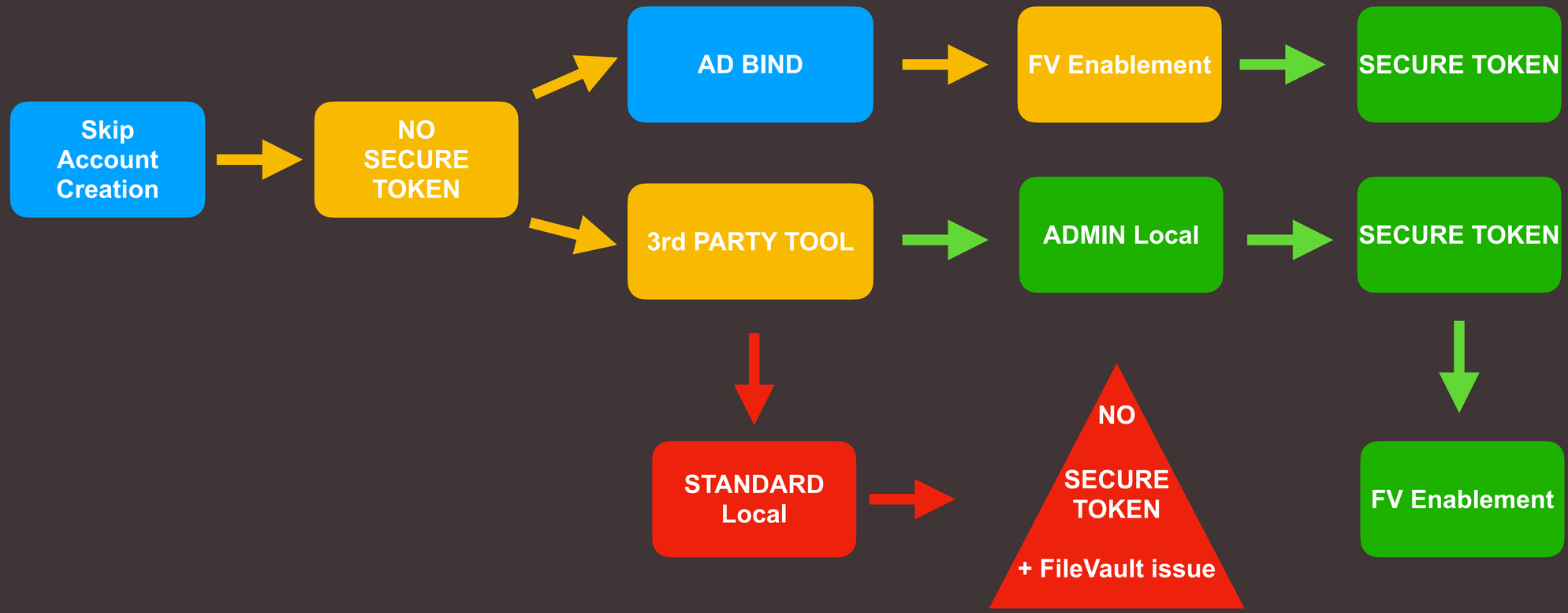
VIRTUAL

CONFERENCE

2020

jamf

Skip Account Creation



© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

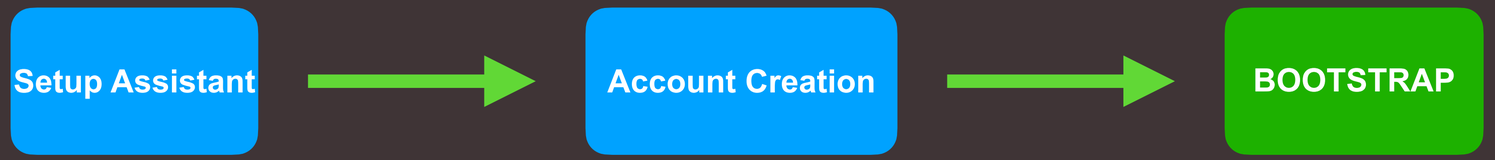
jamf

BootstrapToken

Apple Business / School Manager

“Managed Administrator” / Mobile Accounts

=> Automated MDM Enrolment



© copyright 2002-2020 Jamf

JNUC

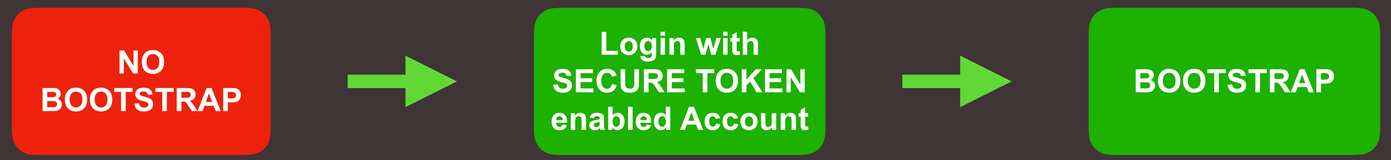
VIRTUAL

CONFERENCE

2020

jamf

Automated MDM with skip account creation



© copyright 2002-2020 Jamf

JNUC

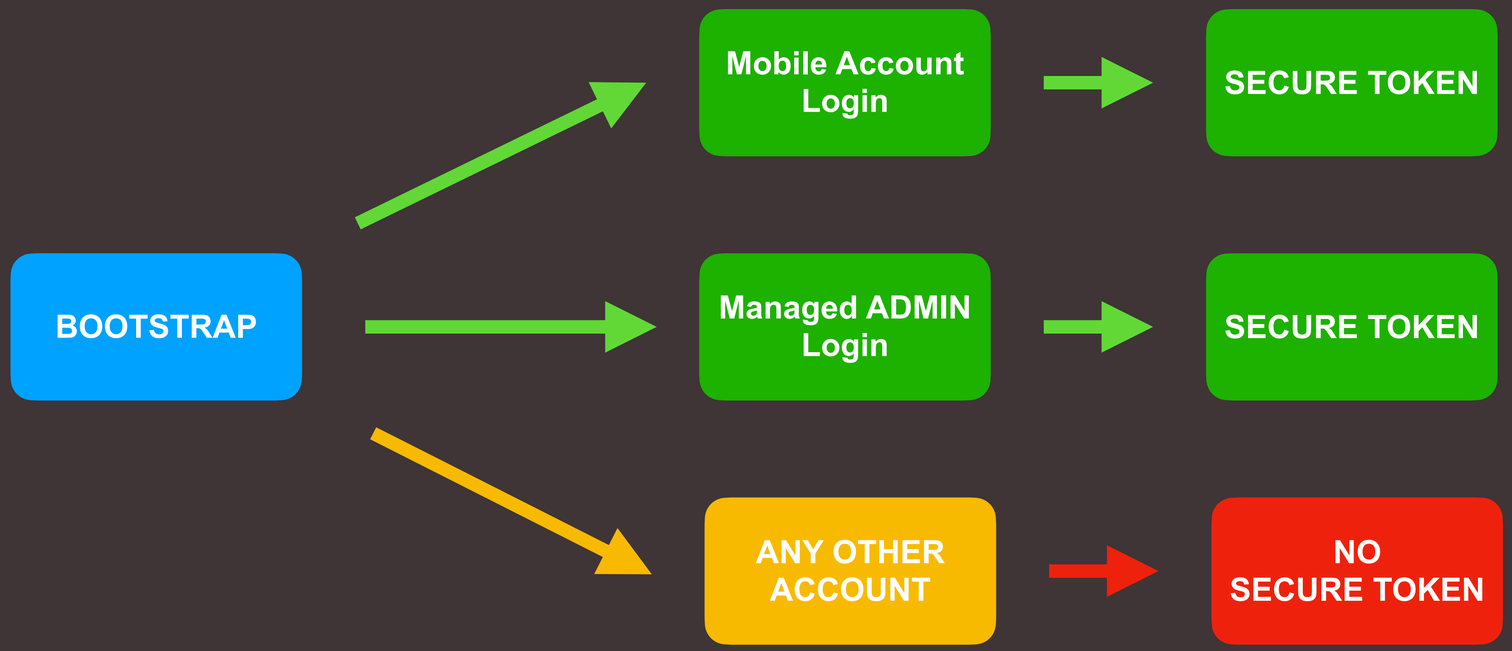
VIRTUAL

CONFERENCE

2020

jamf

SecureToken generation via Bootstrap



2020

© copyright 2002-2020 Jamf

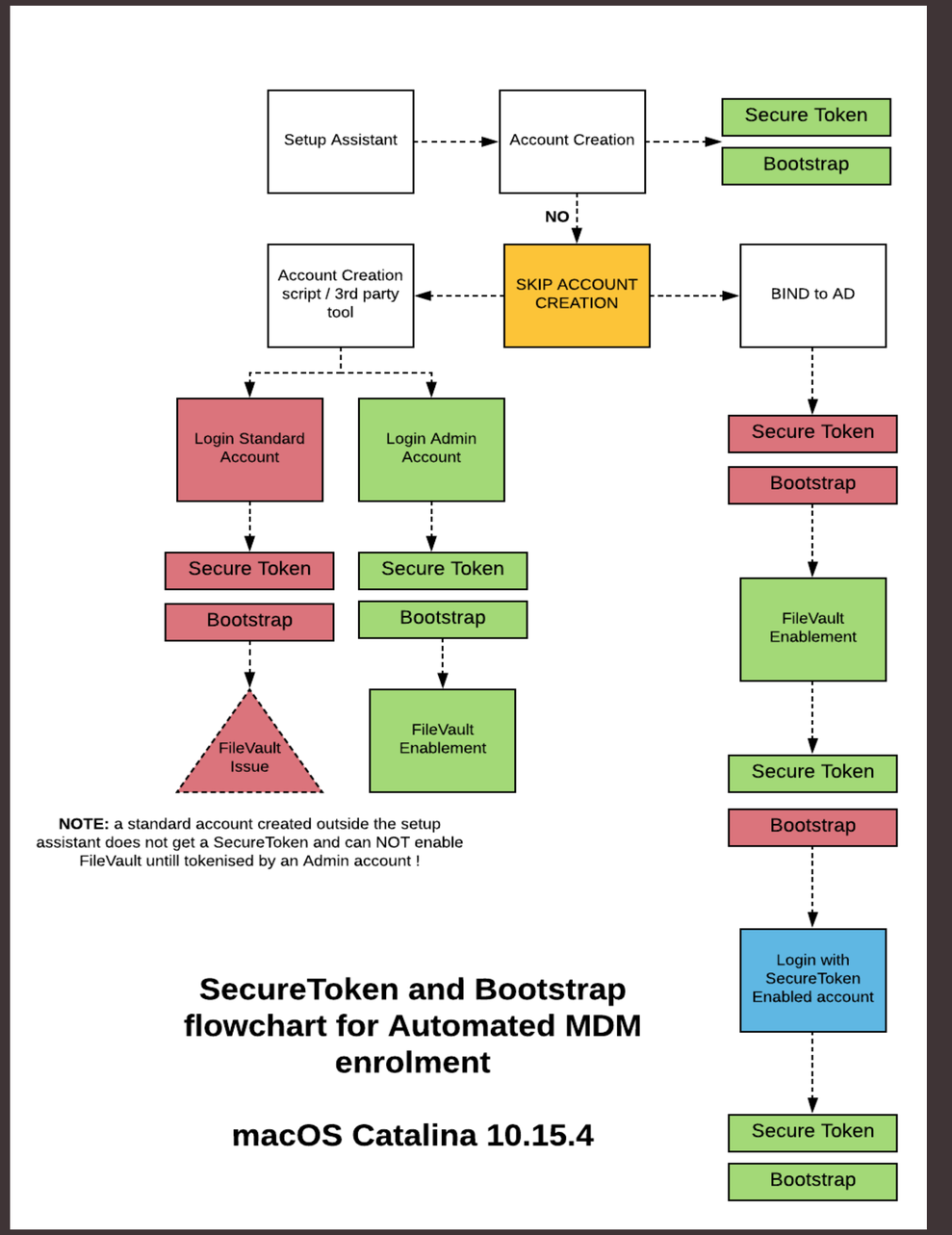
JNUC

VIRTUAL

CONFERENCE

2020

Overview



© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Remotely enabling/enforcing FileVault

Configuration profile

Jamf Pro Policy

Jamf Connect Login

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Configuration profile (High Sierra and Later)

© copyright 2002-2020 Jamf

JNUC

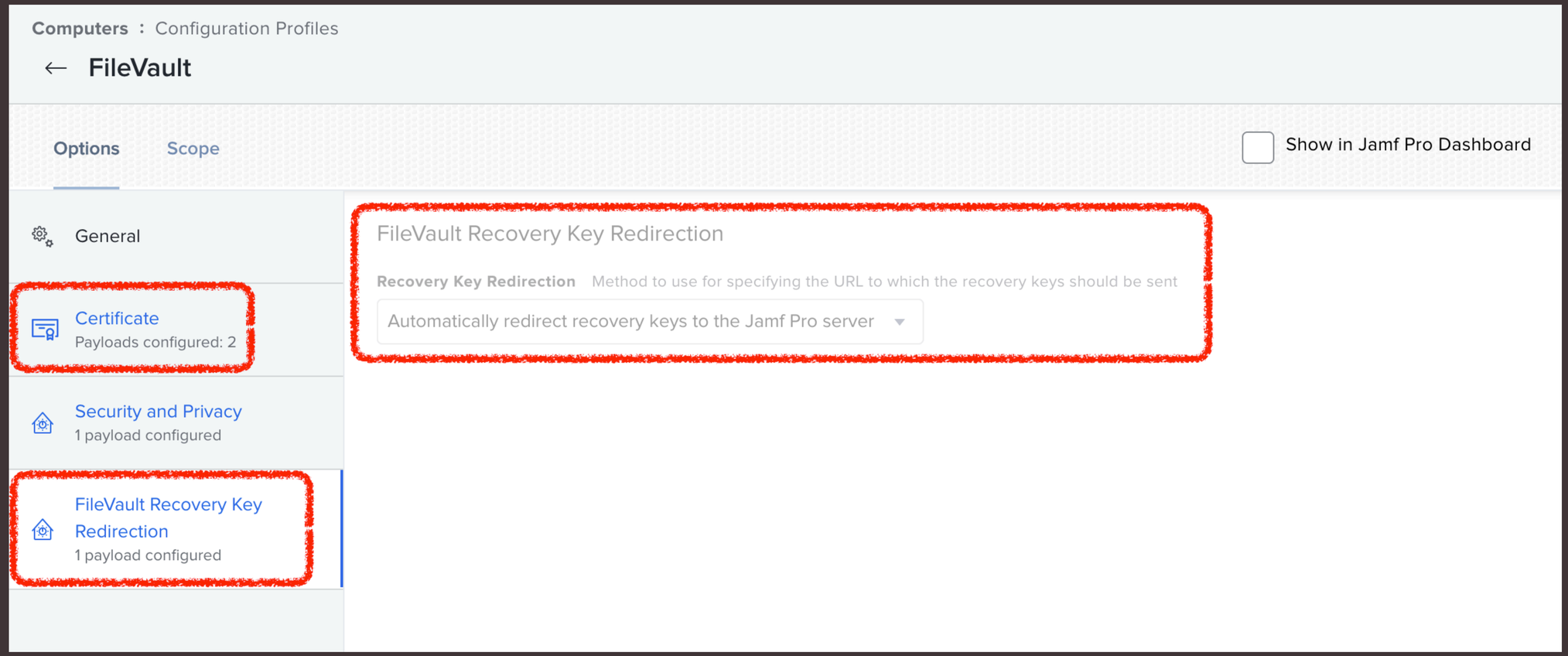
VIRTUAL

CONFERENCE

2020

jamf

Configuration profile (pre - High Sierra)



2020

© copyright 2002-2020 Jamf

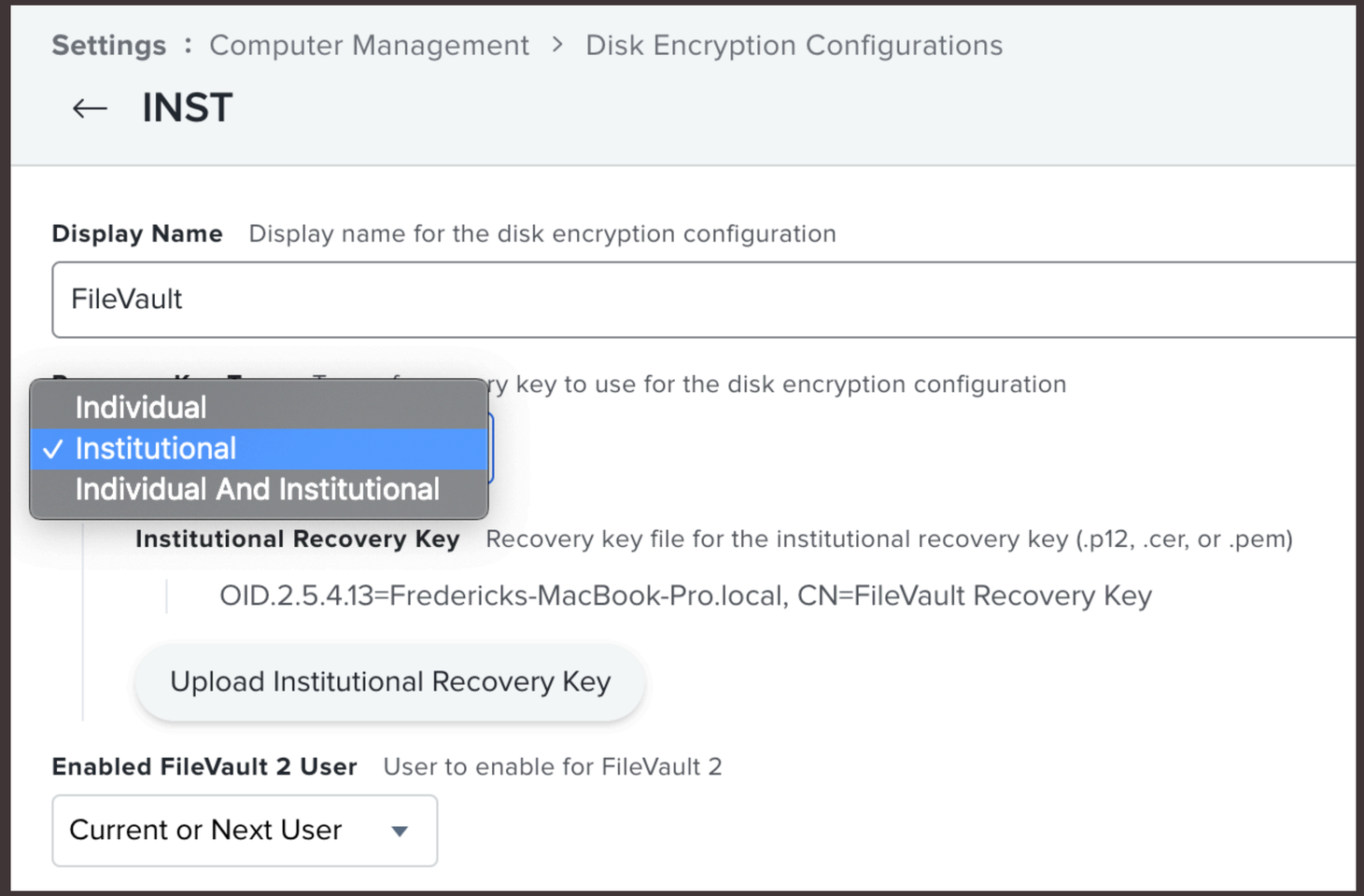
JNUC

VIRTUAL

CONFERENCE

2020

Jamf Pro Policy



© copyright 2002-2020 Jamf

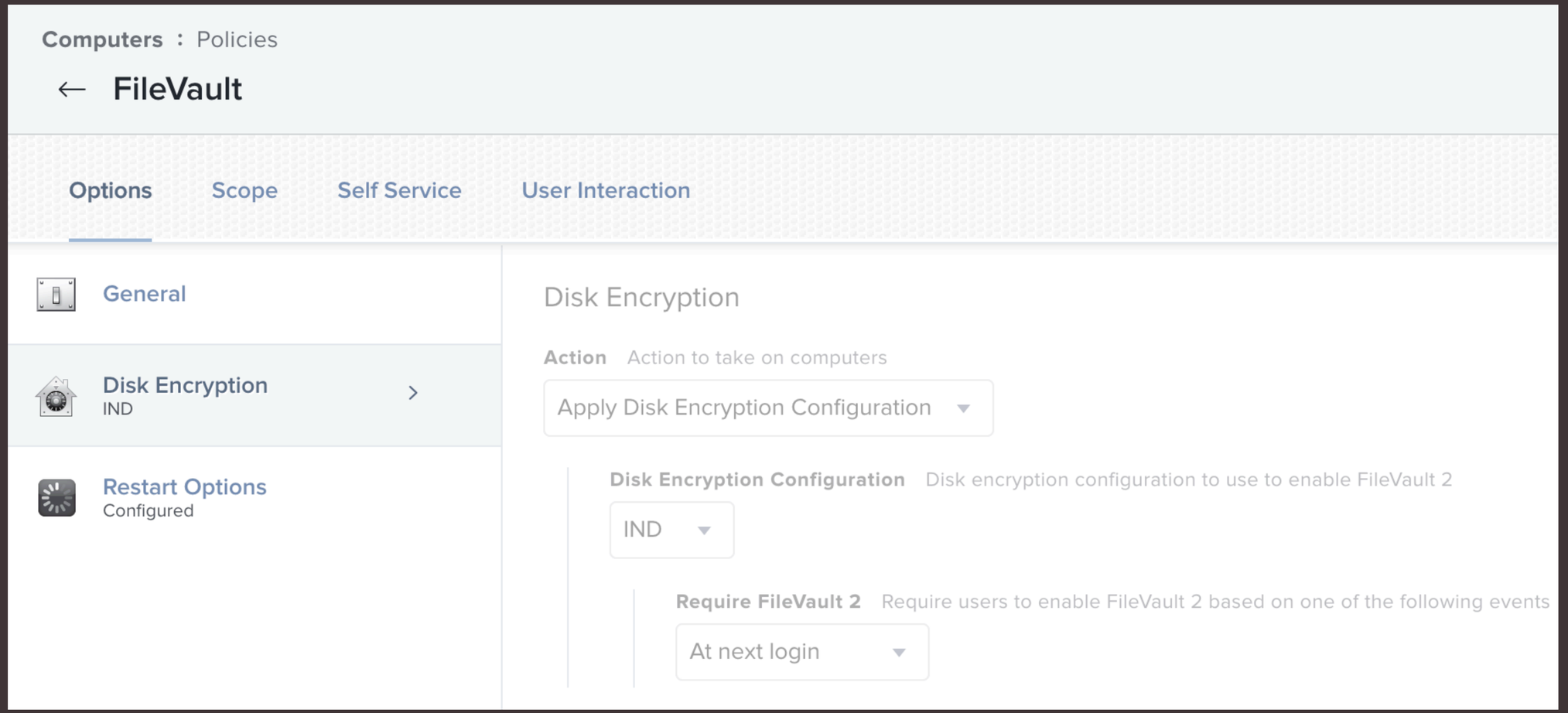
JNUC

VIRTUAL

CONFERENCE

2020

Jamf Pro Policy



© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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.
		`<key>EnableFDE</key>`
		
		`<false/>`

`EnableFDERecoveryKey`	**Save FileVault Recovery Key**
	
	If set to true, Jamf Connect will store the FileVault recovery key to `/var/db/NoMADFDE` unless otherwise specified.
		`<key>EnableFDERecoveryKey</key>`
		
		`<false/>`

`EnableFDERecoveryKeyPath`	**Set Recovery Key Filepath**
	
	Specifies a custom file path for the FileVault recovery key
		`<key>EnableFDERecoveryKeyPath</key>`
		
		`<string>/usr/local/filevault</string>`

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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)

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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>
```

2020

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Recovery Keys

Personal Recovery Key

Institutional Recovery Key

© copyright 2002-2020 Jamf

JNUC

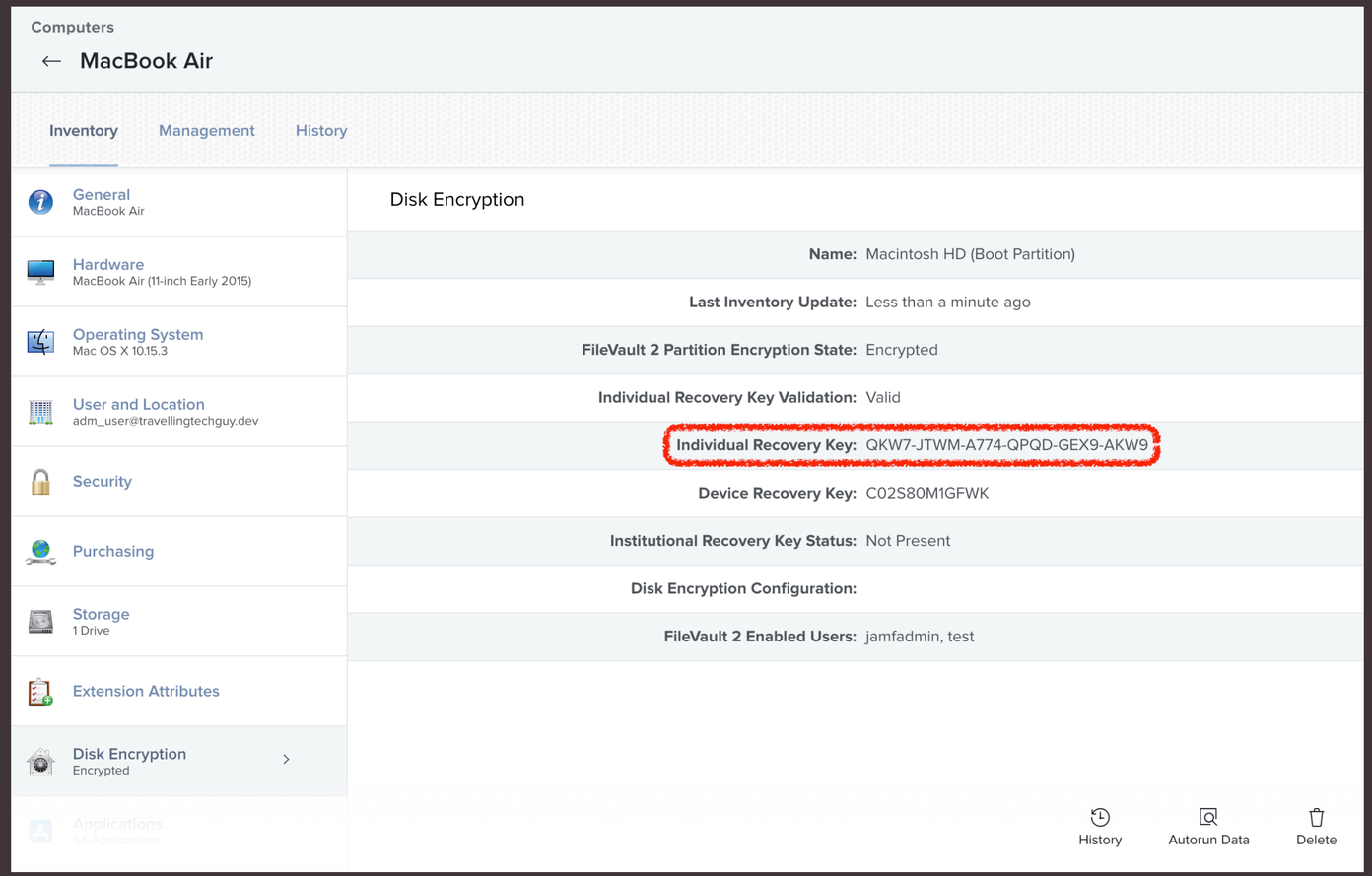
VIRTUAL

CONFERENCE

2020

jamf

Personal Recovery Key



© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

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.

© copyright 2002-2020 Jamf

JNUC

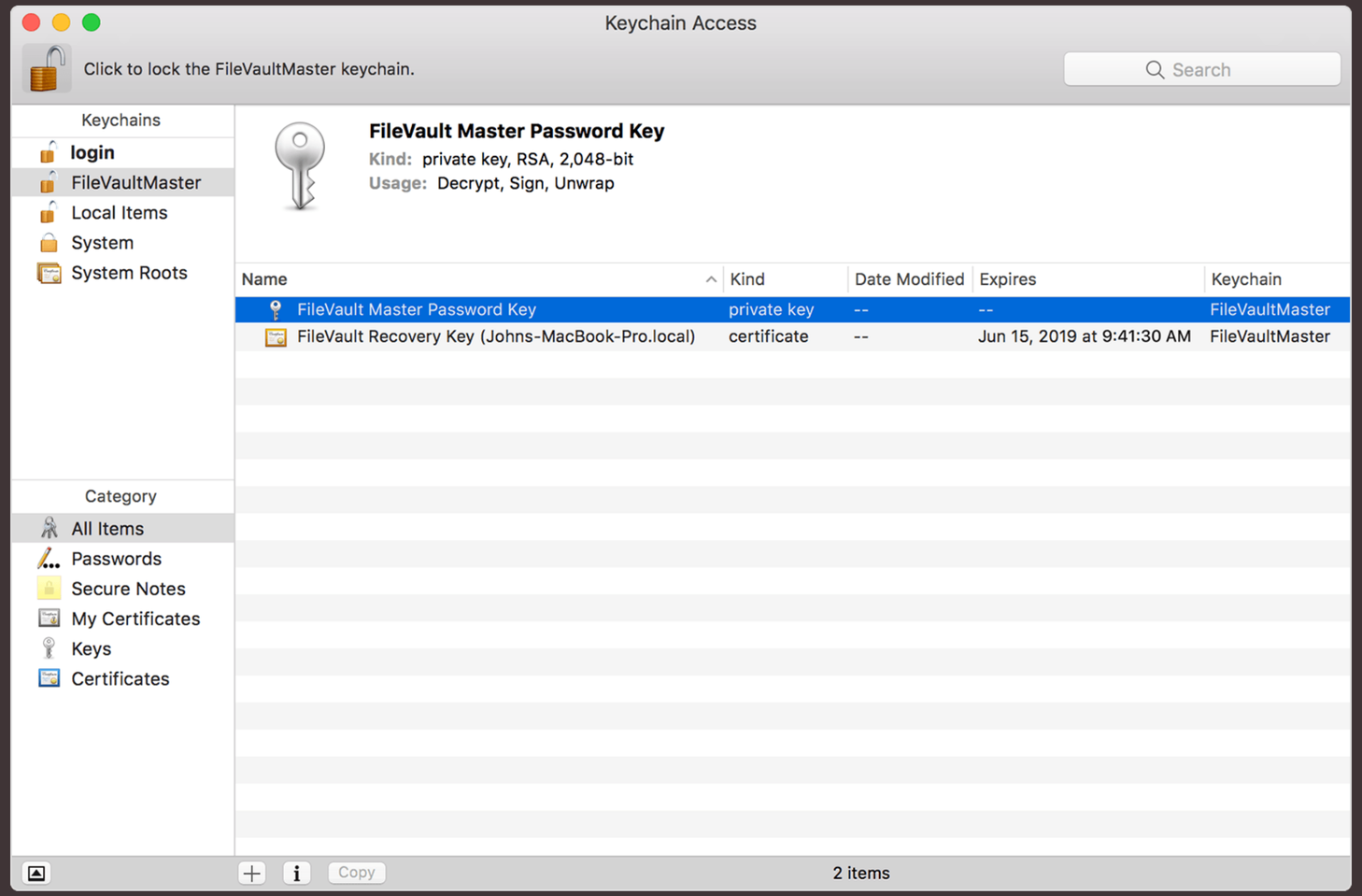
VIRTUAL

CONFERENCE

2020

jamf

Institutional Recovery Key



2020

© copyright 2002-2020 Jamf

JNUC

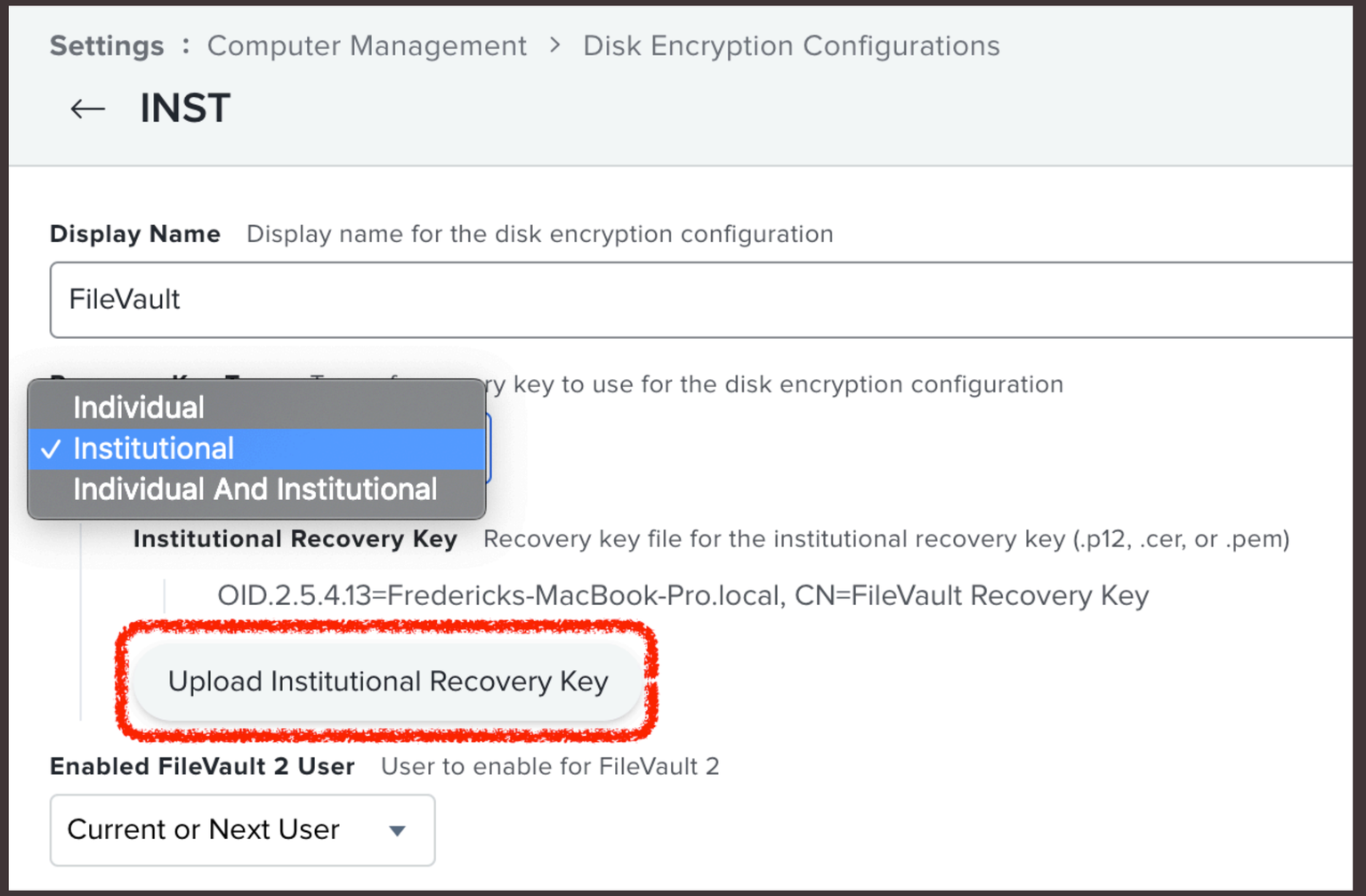
VIRTUAL

CONFERENCE

2020

jamf

Upload Institutional Recovery Key



© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Troubleshooting & Fixes

- Identifying SecureToken holders
- Deferred enablement related issues
- Validating Recovery Key
- Renewing Recovery Keys
- Validating / Enabling Bootstrap
- Scripting Secure Token

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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
```

2020

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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
```

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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
```

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Deferred enablement related issues

fdesetup status

FileVault is ON/OFF

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Deferred enablement related issues

Unscope FileVault Config Profile / Policy

sudo fdesetup disable

+REBOOT

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Validating Recovery Key

fdesetup haspersonalrecoverykey

fdesetup hasinstitutionalrecoverykey

sudo fdesetup validaterecovery

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Renewing Recovery Key

macOS 10.14 or later

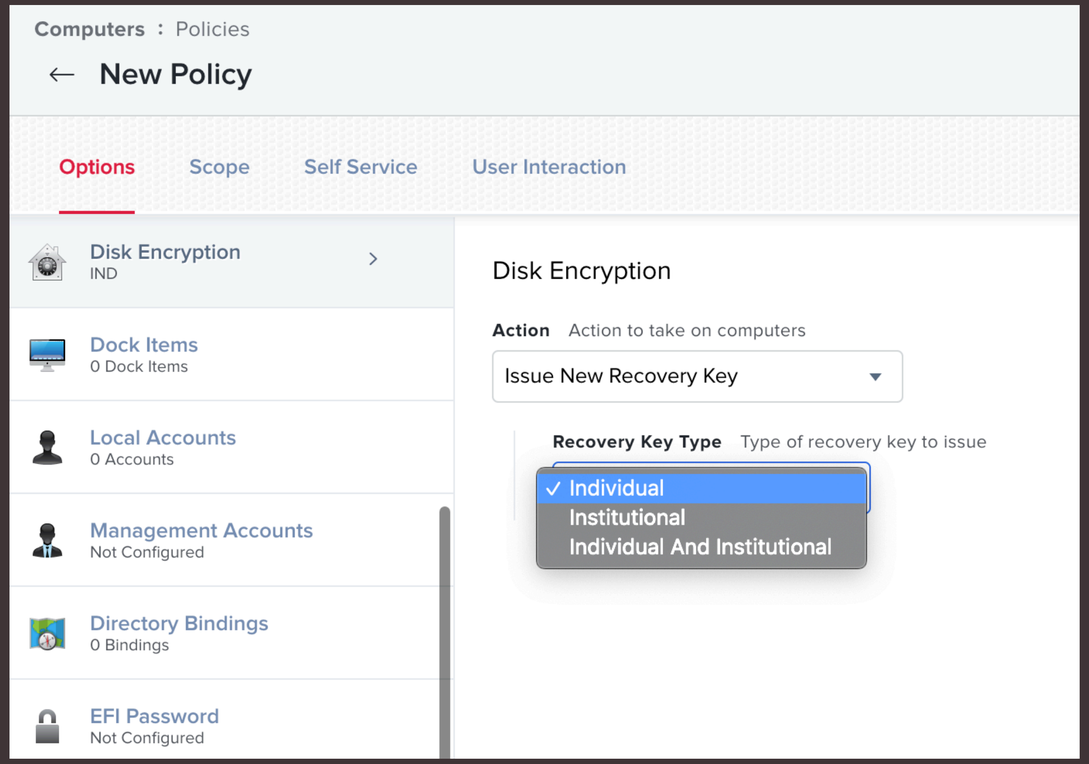
A “Recovery HD” partition

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)



2020

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Renewing Personal Recovery Key

fdesetup changerecovery -personal

(script)

! Make sure to have escrow in place !

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Renewing Institutional Recovery Key

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

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Validating / Enabling Bootstrap

sudo profiles status -type bootstraptoken

Profiles: Bootstrap Token supported on Server YES/NO

Profiles: Bootstrap Token escrowed to Server YES/NO

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Validating / Enabling Bootstrap

sudo profiles install -type bootstraptoken

sudo profiles remove -type bootstraptoken

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

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!

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Anticipated changes in future macOS versions

To be confirmed

© copyright 2002-2020 Jamf

JNUC

VIRTUAL

CONFERENCE

2020

jamf

Ressources

jamf.it/FVJNUC2020

© copyright 2002-2020 Jamf

Thank you for listening!

Give us feedback by completing the survey using the widget below

JNUC2020
VIRTUAL CONFERENCE

© copyright 2002-2020 Jamf