Pull Your Admin Up by the Bootstraps

Demystifying Secure and Bootstrap Tokens for Service Administrators, Enrollment Workflows, LAPS, FileVault, and more!

Jonathan Nelson
https://nverselab.com

CERTIFIED IT
Professional

jamf
MANAGEMENT
ENGINEER

jamf Certified EXPERT

jamf Certified Endpoint SECURITY ADMIN

github.com/nverselab/JNUC-2024

Secure Tokens

A Knowledge Transfer

github.com/nverselab/JNUC-2024

What is a Secure Token?

Technical:
A wrapped version of a Key Encryption Key (KEK) protected by the user's password.

Simplified:
A key that protects other keys.

Analogy:
A transponder chip inside your car key or fob that must be present to start or unlock your car along with the metal key.

Secure Tokens

A Knowledge Transfer

github.com/nverselab/JNUC-2024

What else do I need to know?

Where do I get a Secure Token?

- Account Creation during Setup Assistant
- Login Window as the first interactive login
- Enabled for FileVault by another Secure Token Administrator
- Login Window if the MDM has the Bootstrap Token

When is a Secure Token used?

- Authentication to enable or disable FileVault
- Unlock a FileVault encrypted volume
- Managing Software Updates
- Erase All Contents and Settings Command

Secure Tokens

A Knowledge Transfer

github.com/nverselab/JNUC-2024

What's the catch?

Stuff to be aware of:

- Secure Token enabled accounts must provide previous credentials to change the password or be deleted.
- The Jamf PreStage Admin account is changed with the SetAutoAdminPassword MDM Command for LAPS which will not change the FileVault Password.
- The Jamf Management Account is rotated using the Jamf Framework (Binary) and will also rotate it's FileVault Password.

Bootstrap Tokens

A Knowledge Transfer

github.com/nverselab/JNUC-2024

What is a Bootstrap Token?

Technical:
A token which enables an MDM to perform special actions that would otherwise require a Secure Token user.

Simplified:
The limited MDM equivalent of the Secure Token.

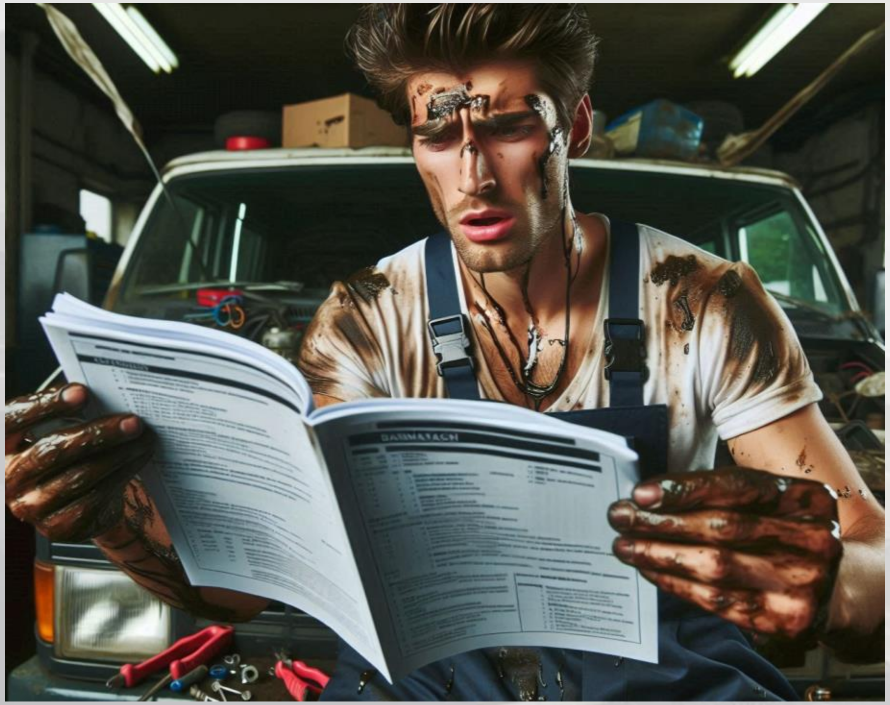
Analogy:
A special key you can provide to your mechanic or dealership to perform specific maintenance tasks.

Bootstrap Tokens

A Knowledge Transfer

github.com/nverselab/JNUC-2024

What else do I need to know?



When do I generate and escrow a Bootstrap Token?

- A Secure Token user logs in the first time after PreStage Enrollment
- During Setup Assistant Account Creation through PreStage (assuming Activation Lock is prevented)
- '/usr/bin/profiles install –type bootstraptoken' is run by a Secure Token enabled Administrator

When is a Bootstrap Token used?

- At the Login Window with MDM to provision new users a Secure Token
- Installing Kernel Extensions with MDM without modifying the Startup Security Settings
- Installing Updates via MDM Command

Volume Ownership

A Knowledge Transfer

You mean there's more?!

github.com/nverselab/JNUC-2024

What is a Volume Owner?

- A user with permissions to make specific changes to the system.
- Some tasks require both Volume Owner and Admin

Who gets Volume Owner permissions?

- The first user who setup the mac
  (the first Secure Token user)
- The Bootstrap Token itself
- Users given a Secure Token at the Login Window with MDM by the Bootstrap Token

When is Volume Ownership Used?

- Installing Software Updates
- Initiating the Erase All Contents and Settings command.
- Changing Startup Security Settings

github.com/nverselab/JNUC-2024

github.com/nverselab/JNUC-2024

Jamf Management Administrator (jamfManage)

- Managed Administrator for both PreStage and User-Initiated Enrollment workstations
- Required for workstation to be considered “Managed”
- LAPS enabled by default
- Can be given a Secure Token without breaking LAPS for Cryptographic (FileVault) Password rotation

github.com/nverselab/JNUC-2024

Jamf PreStage Administrator (jamfPreStage)

- Requires Jamf Management Account to be enabled
- Required when Account Creation needs to make users Standard or skipped entirely
- LAPS is not enabled by default, but will be in future versions of Jamf Pro
- Getting a Secure Token will break Cryptographic (FileVault) Password rotation with LAPS

Enrollment Workflows

"With Great Power Comes Great Tables" - Uncle Ben

github.com/nverselab/JNUC-2024

* indicates optional	LAPS Admins	Account Creation Types	First SecureToken User	FV Sync	Bootstrap Escrow	PRK Escrow	Remediations
Zero/Limited Touch Without PreStage Admin	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap* Setup Admin Cleanup*
Zero Touch With PreStage Admin	jamfManage jamfPreStage	Setup Assistant (Admin/Standard) Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	Assigned User Shared Account	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
Touch Required With PreStage Admin	jamfManage jamfPreStage	Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	jamfManage	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
			jamfPrestage	No			
User-Initiated Enrollment (BYOD-Style)	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	yes	Policy Script	Profile (Automatic) Policy Script (if enabled)	Bootstrap Escrow Script FV Wait for Bootstrap PRK Invalid - Reissue Script Setup Admin Cleanup*

Enrollment Workflows

"With Great Power Comes Great Tables" - Uncle Ben

github.com/nverselab/JNUC-2024

* indicates optional	LAPS Admins	Account Creation Types	First SecureToken User	FV Sync	Bootstrap Escrow	PRK Escrow	Remediations
Zero/Limited Touch Without PreStage Admin	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap* Setup Admin Cleanup*
Zero Touch With PreStage Admin	jamfManage jamfPreStage	Setup Assistant (Admin/Standard) Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	Assigned User Shared Account	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
Touch Required With PreStage Admin	jamfManage jamfPreStage	Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	jamfManage	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
			jamfPrestage	No			
User-Initiated Enrollment (BYOD-Style)	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	yes	Policy Script	Profile (Automatic) Policy Script (if enabled)	Bootstrap Escrow Script FV Wait for Bootstrap PRK Invalid - Reissue Script Setup Admin Cleanup*

Enrollment Workflows

“With Great Power Comes Great Tables” - Uncle Ben

github.com/nverselab/JNUC-2024

* indicates optional	LAPS Admins	Account Creation Types	First SecureToken User	FV Sync	Bootstrap Escrow	PRK Escrow	Remediations
Zero/Limited Touch Without PreStage Admin	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap* Setup Admin Cleanup*
Zero Touch With PreStage Admin	jamfManage jamfPreStage	Setup Assistant (Admin/Standard) Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	Assigned User Shared Account	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
Touch Required With PreStage Admin	jamfManage jamfPreStage	Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	jamfManage	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
			jamfPrestage	No			
User-Initiated Enrollment (BYOD-Style)	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	yes	Policy Script	Profile (Automatic) Policy Script (if enabled)	Bootstrap Escrow Script FV Wait for Bootstrap PRK Invalid - Reissue Script Setup Admin Cleanup*

Enrollment Workflows

"With Great Power Comes Great Tables" - Uncle Ben

github.com/nverselab/JNUC-2024

* indicates optional	LAPS Admins	Account Creation Types	First SecureToken User	FV Sync	Bootstrap Escrow	PRK Escrow	Remediations
Zero/Limited Touch Without PreStage Admin	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap* Setup Admin Cleanup*
Zero Touch With PreStage Admin	jamfManage jamfPreStage	Setup Assistant (Admin/Standard) Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	Assigned User Shared Account	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
Touch Required With PreStage Admin	jamfManage jamfPreStage	Directory Mobile (Admin/Standard) Jamf Connect (Admin/Standard) Policy Created Shared Account	jamfManage	Yes	Automatic	Profile (Automatic)	FV Wait for Bootstrap*
			jamfPrestage	No			
User-Initiated Enrollment (BYOD-Style)	jamfManage	Setup Assistant (Admin)	Assigned/Temp User (Admin)	yes	Policy Script	Profile (Automatic) Policy Script (if enabled)	Bootstrap Escrow Script FV Wait for Bootstrap PRK Invalid - Reissue Script Setup Admin Cleanup*

Remediation Workflows

“Apple is my sword. Jamf is my shield. Remediation workflows are my armor.” – Stephen Strange

github.com/nverselab/JNUC-2024

	Extension Attribute	Smart Group	Config Profile	Policy Payload
Wait for Bootstrap Escrow before FileVault		**Computers with Escrowed Bootstrap:** Boostrap Token Escrowed – is - Yes	Enable and Escrow FileVault with PRK	
Force Bootstrap Generation and Escrow		**Computers without Escrowed Bootstrap:** Bootstrap Token Allowed – is – Yes And - Bootstrap Token Escrowed – is – No		**Trigger:** Recurring Check-in **Script:** Jamf-EscrowBootstrap-StandardUser.sh **Maintenance:** Update Inventory
Validate and Reissue PRK when Invalid		**Computers with Invalid PRK:** Bootstrapt Token is Escrowed – is – Yes And – (FileVault 2 Status – is – All Partitions Encrypted Or – FileVault 2 Status – is – Boot Partitions Encrypted) And – FileVault Individual Key Validation – is - Invalid		**Trigger:** Recurring Check-in **Script:** reissueKey.sh **Maintenance:** Update Inventory
Clean up Setup User after another Secure Token Account is Detected	Jamf-ExtensionAttribute-SecureToken_Users.sh	Computers with setupUser and at least 1 other Account: Bootstrap Token Escrowed – is – Yes And – EA: Secure Token Users – is not – setupUser And – EA: Secure Token Users – like - setupUser		**Trigger:** Recurring Check-in **Local Accounts:** Disable User for FileVault 2 Delete Account: setupUser **Maintenance:** Update Inventory
Force Rotate jamfManage PW				**Trigger:** None (Self Service) **Management Accounts:** Rotate Account Password

Remediation Workflows

"Apple is my sword. Jamf is my shield. Remediation workflows are my armor." – Stephen Strange

github.com/nverselab/JNUC-2024

	Extension Attribute	Smart Group	Config Profile	Policy Payload
Wait for Bootstrap Escrow before FileVault		**Computers with Escrowed Bootstrap:** Boostrap Token Escrowed – is - Yes	Enable and Escrow FileVault with PRK	
Force Bootstrap Generation and Escrow		**Computers without Escrowed Bootstrap:** Bootstrap Token Allowed – is – Yes And - Bootstrap Token Escrowed – is – No		**Trigger:** Recurring Check-in **Script:** Jamf-EscrowBootstrap-StandardUser.sh **Maintenance:** Update Inventory
Validate and Reissue PRK when Invalid		**Computers with Invalid PRK:** Bootstrapt Token is Escrowed – is – Yes And – (FileVault 2 Status – is – All Partitions Encrypted Or – FileVault 2 Status – is – Boot Partitions Encrypted) And – FileVault Individual Key Validation – is - Invalid		**Trigger:** Recurring Check-in **Script:** reissueKey.sh **Maintenance:** Update Inventory
Clean up Setup User after another Secure Token Account is Detected	Jamf-ExtensionAttribute-SecureToken_Users.sh	Computers with setupUser and at least 1 other Account: Bootstrap Token Escrowed – is – Yes And – EA: Secure Token Users – is not – setupUser And – EA: Secure Token Users – like - setupUser		**Trigger:** Recurring Check-in **Local Accounts:** Disable User for FileVault 2 Delete Account: setupUser **Maintenance:** Update Inventory
Force Rotate jamfManage PW				**Trigger:** None (Self Service) **Management Accounts:** Rotate Account Password

Remediation Workflows

"Apple is my sword. Jamf is my shield. Remediation workflows are my armor." – Stephen Strange

github.com/nverselab/JNUC-2024

	Extension Attribute	Smart Group	Config Profile	Policy Payload
Wait for Bootstrap Escrow before FileVault		**Computers with Escrowed Bootstrap:** Boostrap Token Escrowed – is - Yes	Enable and Escrow FileVault with PRK	
Force Bootstrap Generation and Escrow		**Computers without Escrowed Bootstrap:** Bootstrap Token Allowed – is – Yes And - Bootstrap Token Escrowed – is – No		**Trigger:** Recurring Check-in **Script:** Jamf-EscrowBootstrap-StandardUser.sh **Maintenance:** Update Inventory
Validate and Reissue PRK when Invalid		**Computers with Invalid PRK:** Bootstrapt Token is Escrowed – is – Yes And – (FileVault 2 Status – is – All Partitions Encrypted Or – FileVault 2 Status – is – Boot Partitions Encrypted) And – FileVault Individual Key Validation – is - Invalid		**Trigger:** Recurring Check-in **Script:** reissueKey.sh **Maintenance:** Update Inventory
Clean up Setup User after another Secure Token Account is Detected	Jamf-ExtensionAttribute-SecureToken_Users.sh	Computers with setupUser and at least 1 other Account: Bootstrap Token Escrowed – is – Yes And – EA: Secure Token Users – is not – setupUser And – EA: Secure Token Users – like - setupUser		**Trigger:** Recurring Check-in **Local Accounts:** Disable User for FileVault 2 Delete Account: setupUser **Maintenance:** Update Inventory
Force Rotate jamfManage PW				**Trigger:** None (Self Service) **Management Accounts:** Rotate Account Password

Remediation Workflows

"Apple is my sword. Jamf is my shield. Remediation workflows are my armor." – Stephen Strange

github.com/nverselab/JNUC-2024

	Extension Attribute	Smart Group	Config Profile	Policy Payload
Wait for Bootstrap Escrow before FileVault		**Computers with Escrowed Bootstrap:** Boostrap Token Escrowed – is - Yes	Enable and Escrow FileVault with PRK	
Force Bootstrap Generation and Escrow		**Computers without Escrowed Bootstrap:** Bootstrap Token Allowed – is – Yes And - Bootstrap Token Escrowed – is – No		**Trigger:** Recurring Check-in **Script:** Jamf-EscrowBootstrap-StandardUser.sh **Maintenance:** Update Inventory
Validate and Reissue PRK when Invalid		**Computers with Invalid PRK:** Bootstrapt Token is Escrowed – is – Yes And – (FileVault 2 Status – is – All Partitions Encrypted Or – FileVault 2 Status – is – Boot Partitions Encrypted) And – FileVault Individual Key Validation – is - Invalid		**Trigger:** Recurring Check-in **Script:** reissueKey.sh **Maintenance:** Update Inventory
Clean up Setup User after another Secure Token Account is Detected	Jamf-ExtensionAttribute-SecureToken_Users.sh	Computers with setupUser and at least 1 other Account: Bootstrap Token Escrowed – is – Yes And – EA: Secure Token Users – is not – setupUser And – EA: Secure Token Users – like - setupUser		**Trigger:** Recurring Check-in **Local Accounts:** Disable User for FileVault 2 Delete Account: setupUser **Maintenance:** Update Inventory
Force Rotate jamfManage PW				**Trigger:** None (Self Service) **Management Accounts:** Rotate Account Password

Remediation Workflows

"Apple is my sword. Jamf is my shield. Remediation workflows are my armor." – Stephen Strange

github.com/nverselab/JNUC-2024

	Extension Attribute	Smart Group	Config Profile	Policy Payload
Wait for Bootstrap Escrow before FileVault		**Computers with Escrowed Bootstrap:** Boostrap Token Escrowed – is - Yes	Enable and Escrow FileVault with PRK	
Force Bootstrap Generation and Escrow		**Computers without Escrowed Bootstrap:** Bootstrap Token Allowed – is – Yes And - Bootstrap Token Escrowed – is – No		**Trigger:** Recurring Check-in **Script:** Jamf-EscrowBootstrap-StandardUser.sh **Maintenance:** Update Inventory
Validate and Reissue PRK when Invalid		**Computers with Invalid PRK:** Bootstrapt Token is Escrowed – is – Yes And – (FileVault 2 Status – is – All Partitions Encrypted Or – FileVault 2 Status – is – Boot Partitions Encrypted) And – FileVault Individual Key Validation – is - Invalid		**Trigger:** Recurring Check-in **Script:** reissueKey.sh **Maintenance:** Update Inventory
Clean up Setup User after another Secure Token Account is Detected	Jamf-ExtensionAttribute-SecureToken_Users.sh	Computers with setupUser and at least 1 other Account: Bootstrap Token Escrowed – is – Yes And – EA: Secure Token Users – is not – setupUser And – EA: Secure Token Users – like - setupUser		**Trigger:** Recurring Check-in **Local Accounts:** Disable User for FileVault 2 Delete Account: setupUser **Maintenance:** Update Inventory
Force Rotate jamfManage PW				**Trigger:** None (Self Service) **Management Accounts:** Rotate Account Password

github.com/nverselab/JNUC-2024

1. Why is my PreStage LAPS password out of sync with FileVault?

   A: The SetAutoAdminPassword Command cannot change FV Passwords

2. Why does a hidden admin appear on the FV lock screen?

   A: Any user with a Secure Token will appear to unlock the disk

3. Why wouldn’t Software Updates work using MDM Commands?

   A: The Bootstrap Token must be escrowed to the MDM to send Software Updates

4. Why can only one user unlock a shared workstation?

   A: Unless the Bootstrap Token is escrowed, only the first created or logged in user gets a Secure Token

5. Why isn’t the Bootstrap Token escrowing to Jamf Pro

   A: User-Initiated Enrollments do not escrow the Bootstrap automatically.
   A script/command is required to be run as an Admin a with Secure Token

github.com/nverselab/JNUC-2024